THE CYBER PROJECT / THE DEFENDING DIGITAL DEMOCRACY PROJECT

Considerations for Digital Contact Tracing Tools for COVID-19 Mitigation

Recommendations for Stakeholders and Policymakers

Maria Barsallo Lynch

Lauren Zabierek

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
JUNE 2020

The Cyber Project
The Defending Digital Democracy Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org

Design and layout by Andrew Facini

THE CYBER PROJECT / THE DEFENDING DIGITAL DEMOCRACY PROJECT

Considerations for Digital Contact Tracing Tools for COVID-19 Mitigation

Recommendations for Stakeholders and Policymakers

Maria Barsallo Lynch

Lauren Zabierek

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
JUNE 2020

Acknowledgments

The Cyber Project and Defending Digital Democracy Project would like to thank members of the **Special Working Group on the Government-Tech Partnership to Track COVID-19** for their time and expertise:

- Dr. **Margaret Bourdeaux**, global health policy expert and current Research Director of the Security and Global Health Project at the Belfer Center
- The Honorable **Sue Gordon**, former Principal Deputy Director of National Intelligence and Senior Fellow at the Belfer Center
- **Juliette Kayyem**, former Assistant Secretary for Intergovernmental Affairs at DHS and Senior Belfer Lecturer in International Security and frequent CNN contributor
- **Andrew McLaughlin**, J.D., Former Deputy Chief Technology Officer of the United States, former VP of ICANN, and current President and COO of [NewCo]
- **Robby Mook**, President, House Majority PAC, Co-Founder D3P, Adjunct Lecturer at HKS, former campaign manager for Hillary Clinton
- **Kathy Pham**, founding product and engineering member of the White House's US Digital Service, founder The Ethical Tech Collective and current Adjunct Lecturer in Public Policy at HKS
- **Eric Rosenbach**, former Pentagon Chief of Staff and current co-director of the Belfer Center for Science and International Affairs at HKS, Director, D3P and a Lecturer in Public Policy at HKS
- **Bruce Schneier**, internationally renowned security technologist, author, and Adjunct Lecturer at HKS
- **Alex Stamos**, Adjunct Professor at Stanford University's Center for International Security and Cooperation, former CSO at Facebook and senior advisor to D3P at the Belfer Center
- **Jim Waldo**, Chief Technology Officer of Harvard University and Computer Science Professor at HKS and SEAS
- Dr. **Marc Zissman**, Associate Head of the Cyber Security and Information Sciences Division at MIT Lincoln Laboratory
- **Jonathan Zittrain**, Professor of International Law at Harvard Law School, Professor of Computer Science at the Harvard School of Engineering and Applied Sciences, and Faculty Director at the Berkman Klein Center

The varied perspectives of the Working Group members greatly informed this paper; however, the statements and recommendations are solely those of the authors.

We would also like to thank members of the Belfer Center's International Council for their advice and support in launching a working group on forefront data, technology, and cyber issues, which helped pave the way for this inaugural working group.

—

We would especially like to thank our colleagues, fellows, and students for their expertise and support in bringing this report to fruition:

- **Karen Harris**, Managing Director of Bain & Company's Macro Trends Group
- **Julia Voo**, Research Director for the China Cyber Policy Initiative (CCPI) at Harvard Kennedy School's Belfer Center for Science and International Affairs
- **Maya Nandakumar**, Program Coordinator for the Cyber Project, CCPI, and D3P at Harvard Kennedy School's Belfer Center for Science and International Affairs
- **Utsav Sohoni**, Non Resident Fellow for the Cyber Project at Harvard Kennedy School's Belfer Center for Science and International Affairs
- **Christie Lawrence**, Harvard Kennedy School graduate student
- **Vandinika Shukla**, Harvard Kennedy School graduate student

—

*We'd also like to thank **Josh Burek**, Belfer Center Director of Global Communications and Strategy, and Adjunct Lecturer in Public Policy at HKS, for his support and teamwork from realizing the working group concept to sharing this report, **Sharon Wilke**, Belfer Center Associate Director of Communications, for her expert eye, and the entire Belfer Center Communications team, including **Julie Balise**, **Benn Craig** and **Andrew Facini**, for their collaboration in making sure these recommendations reach decisionmakers at a vital time.*

About the Authors

Lauren Zabierek is the Executive Director of the Cyber Project at the Belfer Center. The Cyber Project is a multidisciplinary effort to examine and recommend cybersecurity policy to further national security.

Maria Barsallo Lynch is the Executive Director of the Defending Digital Democracy Project (D3P). D3P identifies and recommends strategies and tools to protect democratic processes and systems from cyber and information attacks.

The Belfer Center for Science and International Affairs is the hub of Harvard Kennedy School's research, teaching, and training in international security and diplomacy, environmental and resource issues, and science and technology policy.

Table of Contents

In this April 22, 2020 photo, Gerard Bakulikira, right, and captain Tim Daghelet, left, both wear a Romware *COVID Radius* digital bracelet, which flashes red when people are too close to each other and creates a log of contacts.

AP Photo/Virginia Mayo

Executive Summary

From the time we began writing this report to its publication date, COVID-19-related deaths in the United States had skyrocketed from just over 40,000 (on April 20) to more than 100,000 (on May 28, 2020).[1] Unemployment claims in the U.S. in late May exceeded 40 million.[2] Businesses have shuttered, international trade has plummeted, and the global economy is in shock.[3] In the U.S., all 50 states are cautiously working to reopen without imposing significant risk on public health facilities or causing surges in deaths.

Many are looking to digital contact tracing to assist these efforts, especially in light of reports that the U.S. could expect as many as 100,000 more deaths due to the virus by this Fall.[4] This report focuses on how the U.S. might consider various proposed solutions. We believe there are real benefits, challenges, and even potential harms in using digital solutions in the fight against COVID-19, but we must also acknowledge that the promise of any technology and associated systems to assist manual contact tracing efforts is largely hypothetical in the United States. There is not one catch-all answer; the truth is that technology is not a panacea, but it may be able to assist official efforts at an unprecedented time. However, no technological solution can succeed without two specific factors: public trust and buy-in, and rapid, widespread testing for everyone living in the U.S. To achieve the first, a number of factors must be addressed by officials in the states looking to implement digital solutions, and by technology developers.

A number of tech solutions are currently in discussion or in development at the federal and state levels, and some are being offered

1 Max Roser, et al., "Coronavirus (COVID-19) Deaths," *Our World in Data*, Oxford Martin Programme on Global Development, last modified May 12, 2020, https://ourworldindata.org/covid-deaths.

2 Rebecca Rainey, "2.1 million new unemployment claims filed last week, as workers still struggle to get benefits," *Politico*, May 28, 2020, https://www.politico.com/news/2020/05/28/coronavirus-weekly-jobless-claims-286911

3 "Trade set to plunge as COVID-19 pandemic upends global economy," *World Trade Organization,* April 8, 2020, https://www.wto.org/english/news_e/pres20_e/pr855_e.htm.

4 NPR Morning Edition with David Greene and Dr. Ashish Jha, "As U.S. Nears 100,000 COVID-19 Deaths, Where Is The Country Headed?" May 26, 2020 https://www.npr.org/2020/05/26/862012540/as-u-s-nears-100-000-covid-19-deaths-where-is-the-country-headed

directly to the public. In the weeks since our *Special Working Group on the Government-Tech Partnership to Track COVID-19* convened at the Belfer Center to discuss proposed methods, the landscape of solutions has shifted. Of the proposed solutions, two digital contact tracing methods are at the forefront of proposals to assist manual contact tracing; both use one of two smartphone-driven methods—(1) Bluetooth proximity signaling via low energy beacon protocol, and (2) applications utilizing location servicess.

In this report we highlight two digital contact tracing systems. The first is Google and Apple's COVID-19 Exposure Notification Application Programming Interface (API), which would allow Bluetooth "chirps" from Google and Apple smartphone users to be accessible to public health authorities via third party applications and decentralized public health servers. This would ultimately allow the phone of a patient who has tested positive for COVID-19 to anonymously make users aware they have been in close proximity to that patient. The second is the use of location services in contact tracing software applications; here we discuss Utah's Healthy Together App developed by the social media company Twenty, and MIT-led Safe Paths, a software kit (currently in beta) that collects location trails from participating users' smartphones and allows government public health officials to use their reported locations over time to identify overlaps with infected patients' locations.[56] As this report is released, the Bluetooth proximity method is widely considered the most privacy-preserving option.[7]

Digital contact tracing to supplement overall contact tracing presents opportunities to scale efforts and potential for effectiveness, but much needs to be considered and developed in order to execute either method. Some tools are being developed with the expectation of official state use and some are being directly marketed to individual consumers, which presents its own set of challenges. With either digital method, one part of the system will be handed to state officials by developers, but the rest of the

5 "Healthy Together Utah," *Twenty Labs,* accessed May 12, 2020, https://healthytogetherutah.com.

6 "Safe Paths Overview" Accessed May 15, 2020 https://www.media.mit.edu/projects/safepaths/overview/

7 Ronald L. Rivest, et al., "PACT: Private Automated Contact Tracing," *MIT Lincoln Laboratory* (Cambridge, MA: MIT University Press, 2020), https://pact.mit.edu/wp-content/uploads/2020/04/MIT-PACT-ONEPAGER-2020-04-07-B.pdf.

ecosystem—both technological and policy—must be developed and implemented by those states.

These digital contact tracing methods present either privacy or mobility issues. Both also present potential implementation challenges. The Bluetooth proximity method is the most privacy-preserving and the PACT: Private Automated Contact Tracing Team is working with Google and Apple to ensure their solution is as secure and reliable as possible, setting it apart in significant ways from other Bluetooth efforts. The overall architecture will utilize decentralized public health servers, which will allow states to use data derived from Google and Apple's architecture. It also means public health servers across states will likely not communicate with each other at the outset—a critical issue for when people travel, explored further in this report as the "airport problem," and one ripe for interstate collaboration. The location services method addresses the mobility issue and might be more accurate in identifying one's location in relation to another infected individual, but it does not address whether that infected individual was too close to another, or for how long. In using a location services app for digital contact tracing, the potential loss of privacy is a concern as well. Users consent to provide personal health and location data to either tech companies or to state government public health officials that show where that user has been over a certain period of time to compare with the location data from other users.

Beyond digital contact tracing, location services may also be used at a more anonymized, aggregate level to model the disease spread, providing officials with situational awareness. Officials may decide to augment digital contact tracing with disease spread modeling, or opt for one methodology over another. States must seriously consider these tradeoffs when choosing a technological solution to assist manual contact tracing efforts and to determine how such decisions are communicated to the public. Otherwise, loss of public trust and buy-in could result in real harm to overall efforts.

States grappling with such decisions and technological challenges could benefit from the ability to coordinate at a national level. Currently, a number of efforts are working to coordinate and provide insights on aspects of these challenges, such as the U.S. Digital Response (USDR) and the COVID-19 Technology Task Force (CTTF), both staffed with

technology experts. We recommend bringing together these efforts in an ongoing national-level coordinating body to scale information sharing quickly with state officials through the National Governors Association, and to include other key stakeholders, such as public health officials and technology companies, specifically PACT, and Google and Apple. Convening these specific groups–which have the ability to bring together experts from tech, public health, legal, and policy perspectives–will allow state officials to better assess technological and policy recommendations.

We hope this report helps stakeholders in their assessments of proposed technological solutions during this urgent and difficult time.

Summary of Recommendations

Coordinating Body	**National Coordinating and Convening Body:** We recommend the coordination and convening of at least the USDR, CCTF, NGA, Public Health Authorities, and the tech companies involved in developing digital contact tracing technologies. Convening these groups at a minimum to brief, provide expertise, exchange information, and introduce key decisions individual states should consider that may nationally scale digital tracing would do a great deal to assure its success.
	USDR and CTTF: The U.S. Digital Response (USDR) or the COVID-19 Technology Task Force (CTTF), are volunteer efforts that may be able to help in this cross-coordination. Currently both groups are working to facilitate communication between states, Google and Apple, and tech experts to advise and support.
	NGA: The National Governors Association plays an important role in coordinating state leadership at a national level, providing guidance and expertise on policy issues and uniting bipartisan members, and facilitating the distribution of vital information. At minimum, its existing convening capacity would allow for civil society groups of experts to connect with state leadership on digital contact tracing issues.
	Public Health Authorities: States' top public health authorities that also report to national level public health authorities must be a part of this stakeholder group. These officials within each state will be making key decisions around digital contact tracing. Their consistent reporting to the federal level is ongoing and their perspective on how digital contact tracing can help manual contact tracing efforts is central to the purpose of coordination.
	Tech Companies: Google's and Apple's solution and partnership with the PACT Protocol position them to be an important stakeholder, especially through the current interface with public health officials in states (and other countries). Whether they are represented through the civil society groups or have formal representatives that will field questions and provide some guidance for specification requests, mainly around server connectivity, their participation is also important.
For State and Local Government	**Recommendations for State and Local Governments:** As the states hold primary responsibility for public health, much rests on the decisions that governors, state public health authorities, and their leadership teams make together in this effort. Execution may be delegated to local governments; as such, we recommend strong coordination between state and local governments in policy, planning, and execution of anti-COVID-19 operations.
	State Task Force: States may already have special task forces created that are helping address and advise COVID-19 response. For mitigation efforts, a special committee within the existing task force should exist to explore digital contract tracing and other technology solutions to assist manual contact tracing.
	Preparing to use the GAEN Solution: States must consider or develop the following to use the GAEN: - A software application to utilize data derived from the API - A rollout, deployment, maintenance, and communication plan for the app - Potential interoperability with other state health systems as part of the app's functionality - How to address user travel across state lines - Define the Too Close for Too Long (TC4TL) Parameters for its Bluetooth data - Determine how users will obtain and report certification of infection - Define any additional security protocols for public health servers to interface with the data derived from the API"
	Preparing to use Location Services: States must consider or develop the following to use a Location Services Software App: - Define how users will obtain and report certification of infection - Develop policies and processes for handling and redacting sensitive PII and location data - Develop redress procedures for potential abuse of information - Consider never collecting or storing PII if this data is not required for contact tracing - Include the CISO or CIO in decisions surrounding the use of the app and associated data and software"
	Integrating with Manual Contact Tracing: As any digital contact tracing effort is meant to assist manual tracing, states should determine how the two will be integrated as well as the following: - Consider establishing a virtual command center - Manual contact tracers should be trained to operate using cybersecurity practices to ensure user data privacy and security - Working closely with public health officials, determine how digital and manual tracing data are combined and assessed - Connect technologists with manual contact tracers to better understand the challenges - Consider how to include the population without smartphones in overall tracing efforts
	Cybersecurity: Each state is responsible for securing any location, health, and personal data. Given increased cyberattacks and overall vulnerability of health system during the pandemic, the following should be considered: - States should prioritize the security of their digital health systems - States should determine interoperability of systems across their state and review accreditation process of organizations that feed into the system - States should work to increase broadband access and cybersecurity to remote municipalities - Municipalities could consider forming regional coalitions to scale efforts.
	Public Interface: Getting the public to participate in the contact tracing system, especially the digital aspect, will require trust and buy-in. As such, states should conduct transparent and coordinated communications with the public across a range of media to include radio and television broadcast, print, social media.
For Tech Companies	**Recommendations for Tech Companies:** To further develop technological solutions during this effort, companies should coordinate with public health officials to maintain awareness of the issues. Long-term, the digital public health system may need a large-scale security upgrade. Secure cloud providers may be able to help in this regard.
	Google, Apple, PACT: - Continue efforts to coordinate with public health officials to prepare them to use the solution and to maintain awareness of the issues - Continue testing and improving data collection and usage and work with states to address mobility and server issues - Should develop an onboarding network and criteria for states to have a clear understanding of how its public health server(s) will need to be set up to receive data from the API and from individual downloads. System specific recommendations should be communicated.
	Location Services App Developers: - Should seek to have transparent data privacy and security standards that can be communicated easily to state and local governments and to the general public - Should be transparent about which personal data will be collected and make redacting information easy for the user, rather than giving responsibility to the government official - Consider not storing any PII - Should clearly articulate how data will be processed and will flow through the system, and should describe security at each layer of the solution - Work to understand how to integrate technology with existing public health infrastructure by working with state officials - Should integrate with public health officials and manual contact tracers to understand the problems they are working to address - Ensure the user interface is simple and easy to use
For Congress	**Recommendations for Congress:** Congress should pass legislation for necessary funding for manual and digital contact tracing and other technical solutions as a part of any further funding for COVID-19 response. Any proposed legislation to increase the manual tracing work force should also provide funding to states and public health officials to put toward assistive technology that also addresses data privacy and security as manual tracing progresses and states' response efforts evolve.
	National Data Privacy and Security Legislation: Congress should continue to address the lack of national laws to govern data privacy and security and create legislation that safeguards any individual health data reported through application vendors to public health officials.
	Sunsetting Data Collection and/or Destruction of Data: For location data being used to track COVID-19 spread, Congress should also create at a minimum legislation that requires a sunset of such tracking measures. Legislation should also seek to address the complexity and the responsibility of data use and storage.

Introduction

As the novel Coronavirus, or COVID-19, spread throughout the United States in February and March 2020, several media outlets including *Politico* and the *Washington Post* reported that the federal government sought to work with tech companies and academia to explore possibilities for using smartphone data to to track and mitigate the spread of the virus. The decision to implement such strategies would advance technical, legal, and policy questions into adoption given these unprecedented circumstances. This announcement came as other countries reported use of smartphone data with varying levels of success; however, experts were quick to point out the foundational differences between the U.S. government and others, especially regarding privacy.

The quickly evolving environment and our outstanding questions prompted us to pull together a group of experts from government, tech, law, and public health to discuss the opportunities and issues in order to find some clarity and to provide recommendations to the myriad stakeholders who are grappling with how best to utilize technology solutions to help stop the spread of COVID-19. This Inaugural Working Group was convened to assess the pressing need for tracing solutions in response to COVID-19 and was held on Friday, April 17 in a special online format. These recommendations stem from the working group's discussion and from additional research and conversations with experts. During the working group discussions, the audience submitted a number of questions surrounding the topic of privacy and security needs during the COVID-19 pandemic and potential uses of individual user data, giving a glimpse of the significance of these issues to the public.

The goal of the working group at the Belfer Center was to assess these issues as they relate to COVID-19 and beyond. Given the novelty of the situation, the questions surrounding the various efforts, and uncertainties about the technical offerings, it is important to gather facts and present them and our recommendations to the public and stakeholders in a clear and transparent manner. While this report focuses on digital contact tracing efforts, we must acknowledge there are other tech initiatives in

development, discussion, or application by a range of companies, but for brevity we chose to exclude those options for now.

In releasing this report, we continue to have more questions as the situation on the ground evolves, but determined that it is important to publish these recommendations in a timely manner.

We aim to help stakeholders assess their options as companies race to develop solutions and outreach to states by vendors begins to increase. What is clear is the need for a holistic, coordinated effort to fight the spread of the Coronavirus and maintain public trust while preserving lives. The following concepts were highlighted throughout the course of the working group's discussion and various sub-discussions. This report seeks to analyze and highlight considerations for how a number of stakeholders—state governments, technology companies, Congress, health providers and researchers—might weigh options for digital contact tracing solutions.

We must emphasize that automated contact tracing supported by technology is only one piece of the puzzle. Any tracing efforts, manual and automated, must be supported by comprehensive, rapid, and easily accessible testing nationwide and we simply are not there yet, despite some progress on local fronts. Writing this report has given us a first-hand view of the many hard-working people who are moving forward efforts to mitigate COVID-19. Their efforts and our collective societal contributions are a hopeful sign of the progress we will make during this uncertain time.

Digital Contact Tracing Solutions

Digital contact tracing is a forefront solution being pursued by many governments, and its promise is further elevated by the recently-released software upgrade to Apple and Android smartphone users.[8] Digital contact tracing as a means to lighten the overall load of contact tracing on the personnel charged with this mission remains an assumption in the U.S., but how it is implemented will determine its efficacy in contributing to COVID-19 mitigation efforts in the short term.

Digital Contact Tracing with Bluetooth

Digital contact tracing using the Bluetooth Low Energy beacon protocol is a specially-developed methodology by Google, Apple, and the Private Automated Contact Tracing (PACT) Team in which a user can upload random identifiers from one's smartphone that represent instances of close proximity with other users to a public health database in the event that person is diagnosed with COVID-19. A Bluetooth-enabled device "chirps" when in proximity to another enabled device and can exchange their respective IDs—saving them locally on both enabled devices in an encrypted form." [9] These Bluetooth "chirps" are constantly anonymized and do not use location data. Using this method, a patient who has tested positive for COVID-19 would give consent for their Bluetooth data to be uploaded to a database of anonymized contacts within decentralized public health servers (likely by state), and individuals who will have come into contact with this individual would then be notified by a manual contact tracer or possibly by a software application.[10]

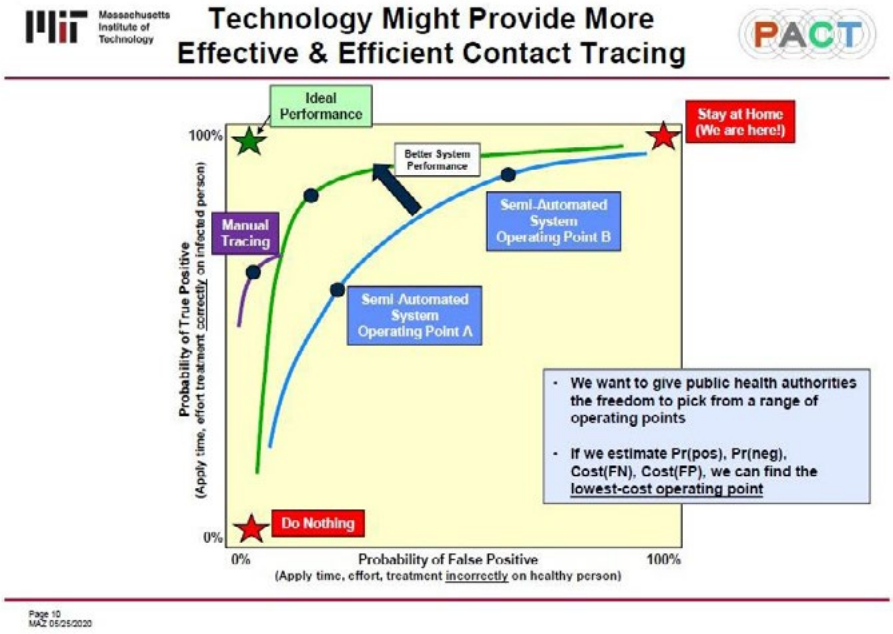
The Google and Apple Exposure Notifications (heretofore referred to as the GAEN) Application Programming Interface (API) was released on May 20, 2020 by both companies with research and development support by

8 Joint Statement from Apple and Google, "Exposure Notification API launches to support public health agencies," May 20, 2020https://blog.google/inside-google/company-announcements/apple-google-exposure-notification-api-launches/

9 Angiuli, "How to De-Identify," https://queue.acm.org/detail.cfm?id=2838930, (2015).

10 Edward Felten, COVID-19 Technology Task Force (CTTF), Digital Tracing Task Force Briefing Briefing on Digital Contact Tracing & Proximity Alerts, April 24, 2020.

PACT.[11, 12] Apple and Google have developed and integrated an opt-in automated contact tracing protocol, rules that facilitate communication between electronic devices, into their Apple and Android operating systems that uses the anonymized Bluetooth technology to help assess person-to-person transmission of COVID-19.[13] One strong benefit of this methodology is that it can determine close proximity—known as "too close for too long" based on signaling.[14] The PACT team continues to work with the companies to address the proximity signaling protocol, which defines proximity detection for Bluetooth (to include the phenomenology, data modeling, systems operability, and battery constraints) as well as the cryptographic layer (privacy, chirp ID rollover frequency, and server issues) and is working to advise states on the requirements for user and public health interfaces to operationalize the system.[15] The resulting system promises trustworthiness and reliability, backed by some of the world's foremost electrical engineers.



11 Ronald L. Rivest, et al., "PACT: Private Automated Contact Tracing Mission and Approach," May 19, 2020, https://pact.mit.edu/wp-content/uploads/2020/05/PACT-Mission-and-Approach-2020-05-19-.pdf

12 Joint Statement from Apple and Google, "Exposure Notification API launches to support public health agencies," May 20, 2020 https://blog.google/inside-google/company-announcements/apple-google-exposure-notification-api-launches

13 Ibid.

14 Ronald L. Rivest, et al.,"The PACT Protocol Specification," April 8, 2020, https://pact.mit.edu/wp-content/uploads/2020/04/The-PACT-protocol-specification-ver-0.1.pdf

15 Ibid.

The work that PACT is conducting in collaboration with Google and Apple is a critical element of improving the accuracy and therefore trust in utilizing this method as a tracing tool. If states choose to forgo the GAEN system, but still seek to use Bluetooth as a proximity tool, officials would have to expend precious time and resources to develop a system paling in comparison to one already created and tested by leading experts. The proximity signaling protocol PACT is developing is an innovation in and of itself—it's replication would require specific capabilities and resources that are unlikely to be easily replicated, especially in the timeframe in which these solutions are seeking to be implemented. The tradeoff between both methods is perhaps resolved by what type of data is most beneficial to manual tracing efforts and states' overall COVID-19 response strategies.

The Bluetooth chirp data can be transmitted to any number of decentralized public health servers around the country and pulled via the Google and Apple-developed-and-managed API only by authorized state public health authorities with a specially-developed software application.[16] The companies maintain they will discontinue the use of the API when it is no longer needed, but that threshold is yet undetermined.[17] The GAEN solution is the first step in a series of technical and policy decisions that will need to be made in order to assist contact tracing. Successful implementation will require coordination between the companies, states, software application (app) developers and public health officials along with stakeholders who oversee server systems in public health offices, localities and states.

A mobile app must be developed in order to access the data provided by the GAEN solution. Apps that will be granted access to the Bluetooth chirp data must be approved by public health officials. In developing such apps, stakeholders may decide that additional data (e.g symptom tracking) is needed to augment manual tracing and public health efforts. Importantly, the protections afforded by the GAEN system do not extend beyond the

16 Zack Whittaker and Darrell Etherington, "Q&A: Apple Google discuss their coronavirus tracing efforts," *TechCrunch,* April 13, 2020, https://techcrunch.com/2020/04/13/apple-google-coronavirus-tracing.

17 James Pero, "Apple and Google promise to discontinue COVID-19 tracking program when the pandemic is over and outline plan for stronger encryption of user data," *DailyMail UK,* April 24, 2020, https://www.dailymail.co.uk/sciencetech/article-8255441/Apple-Google-promise-discontinue-COVID-19-tracking-following-pandemic.html.

API. Once the app utilizes this data, additional privacy considerations will need to be assessed by public health officials and states.

Digital Contact Tracing Using Location Services Applications

Digital contact tracing using location services uses a combination of WiFi, cell tower, and GPS data to provide public health officials a way to compare user locations with infected individuals.[18] This method helps to identify potential transmission areas. Location data may also use Bluetooth, when available, along with stated data sources to approximate a device's location.[19] Using this methodology, a user with a smartphone device creates a log of time-stamped locations traveled over a period of time; upon notification of positive diagnosis of COVID-19 or of potential exposure to an infected person, those logs are compared to users who have been in the same area during the same timeframe based on this location data.[20] Notionally, if this solution is utilized by a state government, this data is collected by the app and provided to state public health officials to assist manual contact tracing.[21],[22] While this method allows for mobility and historical location records, using this particular methodology for digital contact tracing yields increased privacy concerns.[23]

Individual users must consent to providing location and in some cases personal health data to government officials.[24] Location data collected by tech companies is often quite accurate—identifying frequently or infrequently visited locations—which many living in the U.S. might find

18 "Location Services & Privacy," *Apple Support Page*, accessed May 21 2020, https://support.apple.com/en-us/HT207056

19 Ibid.

20 Raskar Ramesh, et al, "Apps Gone Rogue: Maintaining Personal Privacy in an Epidemic," March 19, 2020, https://arxiv.org/pdf/2003.08567.pdf

21 Ibid.

22 "Healthy Together Utah," *Twenty Labs,* accessed May 12, 2020, https://healthytogetherutah.com.

23 Jim Waldo, "Remarks on Contact Tracing," Special Online Session: Expert Working Group on Government-Tech Partnership to Track COVID-19 (working group session, Harvard Kennedy School Belfer Center for Science and International Affairs, Cambridge, MA, April 17, 2020).

24 "Healthy Together App Frequently Asked Questions," accessed May 11, 2020 https://coronavirus.utah.gov/healthy-together-app/

discomforting.[25] Although location data can be aggregated and anonymized, as the European Commission is currently using toward its mitigation efforts, data collected on location can also be individually specific as China has used in their mitigation efforts or as South Korea has also used. Location data methods can lead to surveillance questions.[26],[27],[28]

Some states, such as Utah and North Dakota, have developed their own apps using location data; Healthy Together was developed for the state of Utah by the social media company Twenty and Care19 was developed for North Dakota by ProudCrowd.[29],[30] Healthy Together uses smartphone location data to track users who test positive, and offers an interface for users to input symptoms and receive directions to the nearest testing center.[31] Public health officials then receive test results and share them through the app and reach out to the user and work with him or her to go through recent contacts. From there, the public health official reaches out to those contacts to notify them of potential exposure.[32] The Healthy Together Utah and Utah Coronavirus websites go to great lengths to explain how the app uses personal data and to explain privacy considerations which is critically important in the user interface layer. The success of the app within the larger manual contact tracing effort remains to be seen, but initial downloads of the app were considered strong.[33] However, even initial download momentum may not be sufficient for the level of user engagement needed to make digitally collected data helpful for officials, reinforcing the need for a focus on public education, transparency and trust in selecting and implementing a digital solution.

25 Stuart A. Thompson and Charlie Warzel, "Twelve Million Phones, One Dataset, Zero Privacy," The New York Times, December 19, 2019. https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html

26 Natasha Lomas, "An EU coalition of techies is backing a 'privacy-preserving' standard for COVID-19 contacts tracing," *TechCrunch,* April 1, 2020, https://techcrunch.com/2020/04/01/an-eu-coalition-of-techies-is-backing-a-privacy-preserving-standard-for-covid-19-contacts-tracing.

27 Ibid.

28 Natasha Singer and Choe Sang-Hun, "As Coronavirus Surveillance Escalates, Personal Privacy Plummets," *New York Times,* last modified April 17, 2020, https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html.

29 Jennifer Valentino-DeVries, et al., "A Scramble for Virus Apps That Do No Harm," *New York Times,* April 29, 2020, https://www.nytimes.com/2020/04/29/business/coronavirus-cellphone-apps-contact-tracing.html?action=click&module=Top%20Stories&pgtype=Homepage.

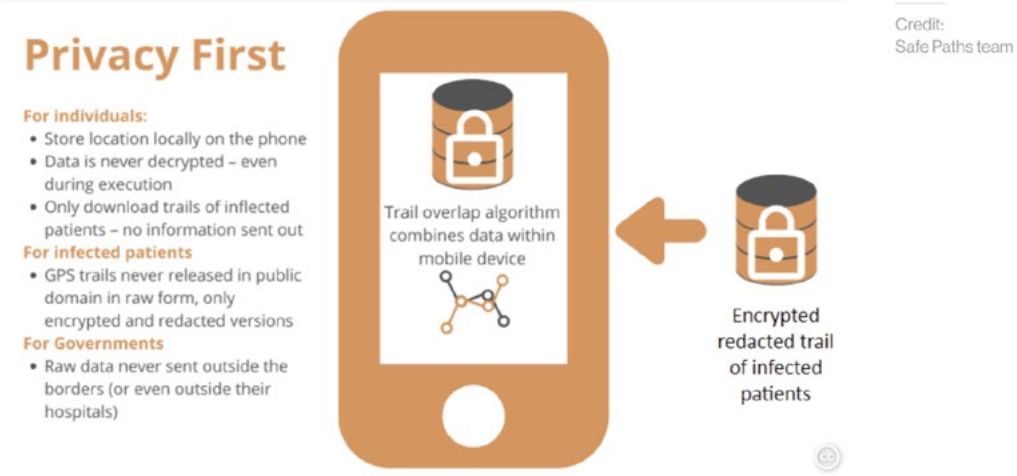
30 "Care19," accessed May 20, 2020, https://ndresponse.gov/covid-19-resources/care19

31 "Healthy Together Utah," *Twenty Labs,* accessed May 12, 2020, https://healthytogetherutah.com.

32 Ibid.

33 Informal discussion with National Governors Association on April 30, 2020

Safe Paths is a large-scale solution in development using location data collected from smartphones by developers associated with MIT and reportedly in use by various governments across the globe and within the United States. Safe Paths is a free and open-source, web-based software (Safe Places) for use by public health officials and smartphone application (Private Kit) for use by consumers.[34] Safe Places will be used by public health officials to collect time-stamped location data from one of the three sources, via the Private Kit: Safe Paths app data, location history, and patient interviews.[35] Private Kit will allow location history, will match personal location history with infected patient anonymous redacted trace files provided by public health officials, and will match personal location history with encrypted anonymous redacted infected patient trace files provided by officials.[36] Safe Paths offers the ability to anonymize location data, and also goes to great lengths to address privacy concerns and provide documentation detailing the protocol and any tradeoffs in privacy and efficacy. However, making the government authority responsible for redacting personally identifiable information data collected from users raises concerns, addressed later in this report.



34 "Safe Paths Overview" Accessed May 15, 2020 https://www.media.mit.edu/projects/safepaths/overview/

35 Ibid.

36 Ibid.

Location data may also be used in an anonymized and non-user specific way. Following the lead of countries like Denmark, location data use should hold questions central to public trust at the core of its app and policy development decisions. Denmark developed its Bluetooth and location application with a focus on gaining a user's trust.[37] The location data the app uses is utilized in an aggregated and pseudonymised manner.[38] The data collected helps officials understand the disease spread.[39] For users, the insight gained in using the app is intended to increase and understand social-distancing efforts, not to warn of a confirmed proximity of infection.[40] This app works in conjunction with a symptom tracker that allows users to submit how they are feeling.[41] Although in an initial download, the user must confirm their identity to register, the identifiable information does not get passed to the app.[42]

Officials must determine what type of data is most useful to their COVID-19 response efforts. In not holding responsibility for personally-identifiable information (PII), or in using anonymized data, officials will mostly rely on a user to initiate contact with health authorities for potential or confirmed infection, underscoring the integrated focus of public trust in designing a solution for how data might help existing public health and manual tracing efforts. Officials should also seriously consider never collecting or storing any PII. Storing the data, even with the promise that it will be quickly and completely destroyed at some future point in time, invites a host of privacy and cybersecurity issues and exposes the state to added risks. Securing PII versus anonymized data will require specific security measures. At a minimum, states should have an explicit goal to stop collecting and to destroy data, echoing the "right to be forgotten" in the European Union's General Data Protection Regulation.[43]

37 *MedTech Innovation,* "How two digital solutions are helping Denmark lift its COVID-19 lockdown," April 22, 2020 https://www.med-technews.com/news/how-two-digital-solutions-will-help-denmark-lift-its-covid-1/

38 Ibid.

39 *Public Technology*, "How Denmark aims to 'create trust' in contact-tracing tech," May 7, 2020. https://www.publictechnology.net/articles/features/how-denmark-aims-%E2%80%98create-trust%E2%80%99-contact-tracing-tech

40 Ibid.

41 MedTech Innovation, Ibid.

42 Public Technology, Ibid.

43 "Right to Erasure," Information Commissioner's Office, accessed May 27, 2020. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/

Digital Tracing Bluetooth and Location Services Combined

The GAEN system will not allow integration with apps that use location data from smartphone devices.[44] As such, while the two methodologies may complement each other and yield a more effective solution for contact tracing, at this time, that is not an option. What may result is that states opt for one solution over another, in an effort to speed the process. We urge careful consideration of either option if a state is to incorporate digital contact tracing into its COVID-19 mitigation operations. This is one example of an issue where states could benefit from working with each other and tech experts to understand these issues, scale resources, and make coordinated policy decisions through a national coordinating body.

44 Khari Johnson, "Apple and Google prohibit location tracking in new contact tracing guidelines," May 4, 2020https://venturebeat.com/2020/05/04/apple-and-google-prohibit-location-tracking-in-new-contact-tracing-guidelines/

Considerations

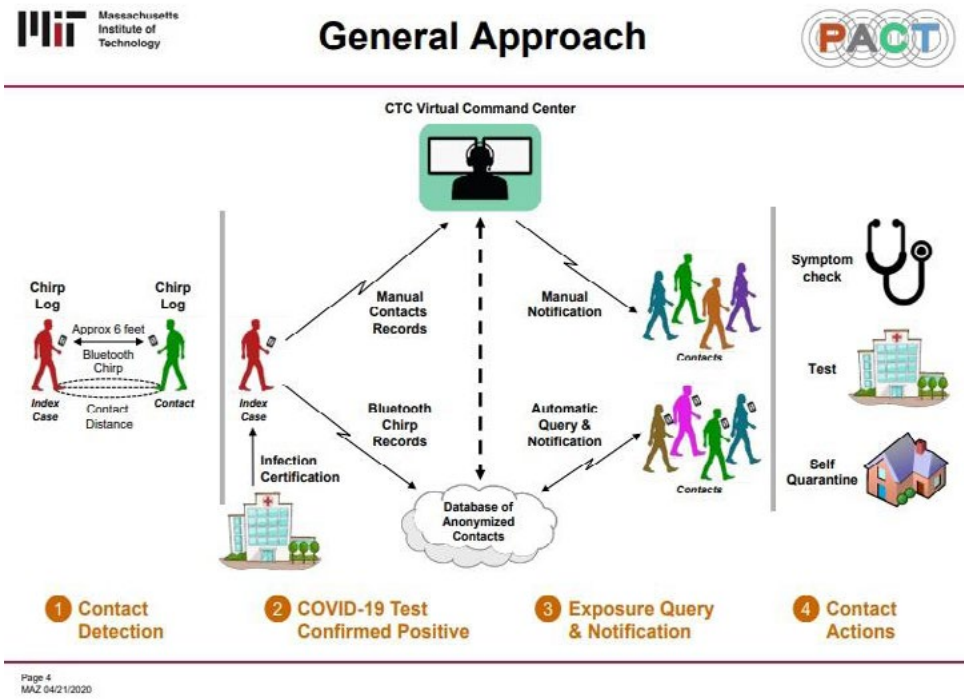
Testing. The United States needs better, faster, and wider testing capabilities for any digital contact tracing to be truly effective in the fight against COVID-19.

Public health is state-run. Because public health is state-run and sometimes locally-executed, digital contact tracing solutions will be coordinated at the state level. This decentralized model makes implementation difficult for a number of reasons. With both digital contact tracing methodologies, state and local governments will be provided with partial solutions; it is up to officials to build out the rest of the ecosystem. Therefore, much work at the state level must be done to prepare for any tech-assisted or digital tracing effort.

What States Must Develop with the GAEN System and Associated Challenges

Think of the GAEN solution as the foundational first and second layer of a three-layer cake.[45] One ingredient in the top layer of the cake is the software app development which will utilize Bluetooth data from the GAEN to make it possible for smartphone users to receive exposure notifications. Other elements of that layer include states and public health authorities working in coordination to vet app vendors, to set the parameters of what such apps can collect from users, to determine what distance and amount of time qualify proximity indicators to notify users, and to assure servers across local and state jurisdictions are properly configured to interface with the GAEN-derived Bluetooth identifier data and transmit information back to users. Skilled development teams will be needed to quickly achieve scale and lessen the window of error for how applications interface with data from the API. Finally, the top layer is the public user interface, and a chief concern here is communication with the public to gain public trust and buy-in for a solution—all while state and public health leaders continue to coordinate critical response efforts.

45 Ronald L. Rivest, et al., "The PACT protocol specification," *MIT Lincoln Laboratory* (Cambridge, MA: MIT University Press, 2020), https://pact.mit.edu/wp-content/uploads/2020/04/The-PACT-protocol-specification-ver-0.1.pdf.



The GAEN solution and PACT protocol describe a system of decentralized public health servers that only public health departments can access.[46] This assumption means that states will need to plan a process for how their public health servers are secured and interact with each other. If states choose an app that will integrate the GAEN solution, they will need to make decisions to address this issue as the country begins to reopen and becomes more mobile because as users cross state lines, their data would not be captured by their point of origin state public health server. Users may have to download apps for the states they intend to visit in order to reconcile partial data in the way that decentralized state public health servers will be set up to utilize data derived from the GAEN solution.

Experts point to the distributed servers as one of the hardest issues to reconcile at a systems level.[47] States may not be able to do this within the time-frame necessary to enact solutions for a rapid return to normalcy. At the top stack layer state and local governments will be coordinating to approve, challenges exist—from the software application to the development and execution of the overall process. Implementation issues can

46 Ibid.

47 Jim Waldo, "Remarks on Contact Tracing," Special Online Session: Expert Working Group on Government-Tech Partnership to Track COVID-19 (working group session, Harvard Kennedy School Belfer Center for Science and International Affairs, Cambridge, MA, April 17, 2020).

also pose an impediment to vital buy-in for manual tracing efforts. One example is a case in which a person is contacted several times over a period of time and told to self-quarantine successively. Critics argue that all of these factors combined could result in the loss of trust and buy-in from the public, rendering any technical solution ineffective at best and, at worst, damaging to the public's relationship with these innovative solutions, harming COVID-19 mitigation efforts.

It is critically important not only for users making the decision to use an app, but for states making decisions on what data is most helpful and in designing new processes and policies, to analyze questions about trust and liability to address tradeoffs between privacy and mobility in a national emergency.

What States Must Develop with a Location Data Solutions App and Associated Challenges

With location services apps (such as Safe Paths and Healthy Together) a user must consent to providing location and in some cases personal health data to government public health officials for manual contact tracing.[48] Documentation on both solutions' websites does provide transparency on how data is collected and used but even with such transparency, additional public education will be needed to help users understand data collection and privacy guidelines. With the Safe Paths app, governments across the globe can white-label Safe Paths and handle user-provided personal data as they see fit. The government is also responsible for redacting personal information.[49] From the outset, this presents a public trust challenge.

Traditionally, people living in the United States have been extremely wary of government surveillance and so adoption of this app could suffer. Vulnerable populations, such as victims of domestic abuse, those in witness protection, and undocumented immigrants might be reluctant to use such

48 "Healthy Together App Frequently Asked Questions," accessed May 11, 2020 https://coronavirus.utah.gov/healthy-together-app/

49 Ramesh Raskar, et al. "Apps Gone Rogue: Maintaining Personal Privacy in an Epidemic," March 19, 2020, Private Kit: MIT White Paper https://arxiv.org/pdf/2003.08567.pdf

systems if the responsibility for removing personally identifiable information rests on the government. While Safe Paths describes the data it collects as encrypted and/or redacted, it is unclear how this data will be handled at the state or local level and what policies and protections will be created to ensure that no nefarious actor abuses access to such data. Every state differs in its cybersecurity practices. Given 2019's continued uptick in ransomware attacks on state and local governments, it's easy to conclude that personal user data will be a prime target for cyber criminals and nation state actors, and states tasked with protecting this data must be prepared to deal with these attacks.[50]

In addition to implementing security policies and procedures surrounding personal data, public health officials will need to work with state and local governments to determine how anonymized or non-anonymized location data will integrate with manual contact tracing and aid overall COVID-19 mitigation efforts. States will need to generate a communications and rollout plan for the public to include transparent and easy-to-understand guidelines on the use and retention of personal data, opt-out procedures, and options for redress or reporting of abuse. State and local governments should not overlook these issues in the urgency to implement technological solutions to aid reopening.

Public trust will be paramount if for example, users are going to report symptoms, receive test results, and be tracked. How users will be informed about potential loss of privacy or how companies, state and local governments, or app developers may handle their data should be addressed in a transparent manner. States must also consider their liability and security based on what type of data is collected.

Integrating with Manual Contact Tracing

Any official technological solution must assist the personnel doing manual contact tracing; as such, it's imperative that technologists work with these and other public health personnel to better understand the problems they

50 Allan Liska, "State and Local Government Ransomware Attacks Surpass 100 for 2019," December 20, 2019. https://www.recordedfuture.com/state-local-government-ransomware-attacks-2019/

are working to overcome as COVID-19 response efforts evolve and collaboratively determine how they can best help. Several opportunities exist for such integration along the chain of development and use, and such a united approach will help officials determine the best digital tracing method for their state.

Estimates suggest the United States will need more than 200,000 people to help with manual contact tracing in all 50 states.[51] It is important that any volunteers be vetted and trained on any digital solutions, including digital tracing systems as well as ones to assist outreach beyond identification of COVID-19-positive patients. Such technologies include software to help organize contacts, use of encrypted messaging apps to contact people, and use of Virtual Private Networks (VPNs) to protect sensitive data.[52]

Public Education: Trust, Buy-In, and Privacy Are Key to Success

The Bluetooth methodology requires high acquisition for maximum benefit. A 1/N adoption rate sees 1/N^2 exposure events, so if there is a 50% adoption rate of an app, 25% of exposure events are identified.[53] This also means that the use of multiple, non-compatible apps will lessen the effectiveness of this method.[54] State officials will need to determine procedures for notifying users found to have been in close proximity with infected individuals, and how those they should respond and communicate with medical or public health providers.

Transparency, trust, and acquisition will be necessary for both the utilization of this technology and how it drives digital tracing, highlighting the need to integrate seamlessly with manual contact tracing. States and public

51 Scott Gottlieb, "Call For Public Health Investment in Next Congressional COVID-19 Aid Package," Interview by Steve Inskeep, *Morning Edition on National Public Radio,* April 27, 2020, https://www.npr.org/2020/04/27/845322490/call-for-public-health-investment-in-next-congressional-covid-19-aid-package.

52 Associated Press, "Contact tracing apps are off to a slow start in the U.S.," May 19, 2020 https://www.nbcnews.com/tech/tech-news/contact-tracing-apps-are-slow-start-u-s-n1210191

53 Edward Felten, COVID-19 Technology Task Force (CTTF), Digital Tracing Task Force Briefing Briefing on Digital Contact Tracing & Proximity Alerts, April 24, 2020.

54 Ibid.

health officials will need to be transparent about how they are assessing data voluntarily collected through an approved app and other mechanisms. The app itself will not be able to make a person self-quarantine if they have potentially been in proximity with someone who tested positive. Disinformation around COVID-19 continues world-wide, and such efforts may continue to be used to confuse or create distrust in institutions. Therefore consistent public education will need to be an element of any manual or digital tracing solutions.

It is worth noting that not everyone in the United States owns a smartphone.[55] Experts estimate that 80% of the U.S. population has access to a smartphone and from this population, there is potential to track 65% of potential exposures. This may not account for use by children or multiple family members, or even older generation smartphones that are not equipped to use this technology.[56] This is not only an efficacy issue—but also one of equity. Solutions like wearable Bluetooth pendants are in development, but creating policies and procedures for sharing information from these devices will also need to be developed.

New apps are appearing daily on the market; some are malicious, using disinformation to promise users important information and presenting potentially harmful cybersecurity risks—including ransomware attacks on users phones.[57] These threats underscore the need to work with or download apps from trusted vendors and sources. Officials must provide clear and understandable messaging about their approved app vendors and tracing process.[58] Further, apps may appear on the market from any developer in any country that ask for personal information, health data, or track user location. As we warn elsewhere in this report, minimal safeguards exist to protect consumers from such companies collecting, using, selling, or not securing that data. This also presents potential counterintelligence, foreign

55 S. O'Dea, "Smartphone penetration rate as share of the population in the United States from 2010 to 2021," *Statista,* April 8, 2020 https://www.statista.com/statistics/201183/forecast-of-smartphone-penetration-in-the-us.

56 Edward Felten, COVID-19 Technology Task Force (CTTF), Digital Tracing Task Force Briefing Briefing on Digital Contact Tracing & Proximity Alerts, April 24, 2020

57 Zeljka Zorz, "Fake Covid-19 tracker app delivers ransomware, disinformation abounds," March 16, 2020.https://www.helpnetsecurity.com/2020/03/16/fake-covid-19-tracker/

58 Cornell, "The Best COVID-19 Tracking," https://www.howtogeek.com/668325/the-best-covid-19-tracking-apps-and-websites, (2020).

surveillance, and disinformation risks for users in the United States—and continued risks to public trust and overall COVID-19 mitigation efforts.

As companies race to develop solutions for contact tracing or exposure notification, whether due to altruistic, financial, or even nefarious motivations, the market is likely to be saturated with technology options offered to the public and governments. This could lead to a diffusion in uptake for official or state-developed apps which could harm the state's larger contact tracing efforts. Some recent epidemiological estimates say that at least 60% uptake for a digital tracing solution is needed for effectiveness.[59] The more options there are, the higher the possibility for diffusion, confusion, or app fatigue, unless they are made interoperable. Moreover, if users decide to use solutions that are not privacy-preserving or at least transparent in their usage of personal data, public trust in technology and the official COVID tracing efforts could be harmed.

Legal and Liability Issues

There are no national privacy and data security laws to guide technology development. While the federal government is limited in the type and amount of data it can collect on U.S. soil through the Intelligence Oversight and the Foreign Intelligence Surveillance Act, the private sector faces no such restriction in the collection, management, use, and sale of user data.[60] Six states have enacted laws, which give varying levels of control over user data.[61] The Health Insurance Portability and Accountability Act (HIPAA) does not apply to tech companies acquiring data directly from its consumers which may be especially applicable for officials in selecting vendors to provide an app for digital contract tracing.[62] Under the Consumer Privacy Act companies must follow their own privacy policies and if they break

59 Valentino-DeVries, et al., "A Scramble," https://www.nytimes.com/2020/04/29/business/coronavirus-cellphone-apps-contact-tracing.html?action=click&module=Top%20Stories&pgtype=Homepage, (2020).

60 Executive Order 12333—United States intelligence activities, https://www.archives.gov/federal-register/codification/executive-order/12333.html

61 "Complete Guide to Privacy Laws in the US," Varonis. Accessed May 29, 2020. https://www.varonis.com/blog/us-privacy-laws/

62 Andrew McLaughlin, "Remarks on Contact Tracing," Special Online Session: Expert Working Group on Government-Tech Partnership to Track COVID-19 (Working group session, Harvard Kennedy School Belfer Center for Science and International Affairs, Cambridge, MA, April 17, 2020).

them they can be tried for deceptive practices.[63] While large tech companies may decide to follow European Union's General Data Protection Regulation (GDPR) or California Consumer Privacy Act (CCPA) guidelines to account for their global presence, smaller companies or those operating outside of these geographic boundaries are not subject to these regulations .[64],[65] As part of the GAEN solution, Google and Apple will only allow apps that are designated by public health authorities, who will also determine and approve the privacy guidelines of such vendors.[66] Google and Apple have included policies that developers must adhere to in using the exposure notification API which helps prioritize the privacy principles important to both companies in providing the solution.[67]

Big tech may companies may want to help, but are cognizant of the liability and criticism they may incur, this concern could also hinder a holistic solution.[68] The GAEN solution is a prime example of this; the joint-venture delivers mass data at a scale other technology companies would not be able to provide, however it passes on potential liability on issues of privacy to jurisdictions who use the solution.

The Airport Problem

The "airport problem" refers to the concern that a person using Bluetooth proximity tracing method (such as the GAEN solution) might travel across state lines, but the decentralized servers cannot reconcile that travel. Internationally, GAEN policy allows for one approved app per country, but the companies are willing to work with countries if they indicate a regional

63 Ibid.

64 Ibid.

65 Ibid.

66 Edward Felten, COVID-19 Technology Task Force (CTTF), Digital Tracing Task Force Briefing Briefing on Digital Contact Tracing & Proximity Alerts, April 24, 2020

67 Tech Crunch, "Apple and Google release sample code, UI and detailed policies for COVID-19 exposure-notification apps" https://techcrunch.com/2020/05/04/apple-and-google-release-sample-code-and-detailed-policies-for-covid-19-exposure-notification-apps/, May 4, 2020.

68 Alex Stamos, "Remarks on Contact Tracing," Special Online Session: Expert Working Group on Government-Tech Partnership to Track COVID-19 (working group session, Harvard Kennedy School Belfer Center for Science and International Affairs, Cambridge, MA, April 17, 2020).

or state-based approach to the solution.[69] In the U.S., unless a coordinated national approach is taken by states, the GAEN solution will work with individual state public health servers. The state-developed app will likely be configured to transmit chirp data to specific decentralized public health servers, and those servers are likely not configured to not communicate with other servers across state lines at this time.

To achieve such connectivity would likely require additional resources, navigating a host of hardware, software, and/or system design questions, and time. It is unclear whether the benefits would outweigh the challenges. Moreover, a person must consent to uploading anonymous data from one's phone to such a server and agree that it could be shared across state servers should that option exist down the road. Currently, if a person comes into contact with infected persons during interstate travel, those Bluetooth chirps cannot be transmitted or downloaded during that period.

As mass interstate transit resumes, the mobility question must be addressed. Options to do so include collection of some location data at airports, in which unique Bluetooth chirps would communicate with an airport-based server, or downloading an approved state app once a user arrives in a particular state. This would allow the users chirps to synchronize with a local server while present in the state but not while in transit. Where location-based apps like Safe Paths do not use the same decentralized public health server infrastructure, the airport problem is not a concern, but the tradeoffs are privacy and proximity. Such decisions could benefit from discussion at a national level with trusted experts via the proposed coordinating body.

69 Tech Crunch, "Apple and Google release sample code, UI and detailed policies for COVID-19 exposure-notification apps" https://techcrunch.com/2020/05/04/apple-and-google-release-sample-code-and-detailed-policies-for-covid-19-exposure-notification-apps/, May 4, 2020.

Recommendations

A National Coordinating Body: To Convene, Coordinate, and Support Digital Contact Tracing Efforts

Although Singapore's Bluetooth app is often cited for its efficacy, the U.S. replication of such an effort will have different requirements to success given the population (300 million) and decentralized governance in the U.S. The European Union's Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) project tackles the digital contact tracing issue for a large population (500 million). This effort aims to develop a coordinated response to COVID-19 contact tracing between countries that are part of the European Union by uniting a multinational European team, creating recommendations that comply with GDPR, and can account for multi-country data exchange. The PEPP-PT is a working group of scientists, technologists, and expert institutions and companies that is creating the protocol for apps to interface with national health services. It is a non-profit and provides open technical and security standards.[70]

A similar model should be adapted for an American context. If a national coordinating effort can unite experts to assure and recommend development and security standards, coordinate individual application developers, and create clear standards for inter-state server data exchange, the likelihood of successful digital tracing implementation will be more easily scaled within the timeframe where such data may be helpful for mitigation efforts—within the coming months. Volunteer efforts that have recently formed like the COVID-19 Data and Research Tech Task Force, or the U.S. Digital Response, which are both coordinating with Google, Apple and states, could be linked and expanded within the government to quickly coordinate at a national level.[71]

70 Lomas, "An EU coalition of techies," https://techcrunch.com/2020/04/01/an-eu-coalition-of-techies-is-backing-a-privacy-Preserving-standard-for-covid-19-contacts-tracing, (2020).

71 COVID Tech. About the Task Force. https://www.crttf.org/covid19/ May 2020.

As efforts get quickly underway in the U.S., we recommend the coordination and convening of at least these four stakeholders mentioned above and detailed below. At a minimum, convening these groups to (1) brief, (2) provide expertise, (3) exchange information, and (4) introduce key decisions individual states should consider that may nationally scale digital tracing, would do a great deal to ensure its success. Beyond this, their continued coordination could ensure that communication, resources, and expertise are readily available for states as COVID-19 response efforts continue.

Recommended Experts and Key Members

The U.S. Digital Response (USDR) or the COVID-19 Technology Task Force (CTTF), are volunteer efforts that may be able to help in this cross-coordination. Currently both groups are working to facilitate communication between states, Google and Apple, and tech experts to advise and support. The *"USDR embeds volunteers to partner directly with governments and understand their needs, implementing effective technology for COVID-19 response."* Each state has a different culture and different technical and legal requirements but the USDR might offer some replicability and trusted developers across states.[72] The CTTF "*serves simultaneously as the contact point among tech companies producing solutions to respond and recover from the COVID-19 pandemic and between the tech industry and the public sector to identify and fulfill public needs*".[73] Both groups have brought together highly talented experts who are assessing the needs for the implementation of technology solutions to support COVID-19 mitigation efforts, including, but not limited to, exposure notification. Their assessment of policy considerations, implementation realities of how tech may support future efforts is also a needed resource. Both groups have been growing quickly and are actively trying to make inroads with individual states.

72 "What We're Working On," U.S. Digital Response, accessed May 12, 2020, https://www.usdigitalresponse.org/projects.

73 COVID Tech. About the Task Force. https://www.crttf.org/covid19/ May 2020.

The National Governors Association (NGA)

The NGA brings together governors from the U.S.' 55 states and territories. "*Through NGA, governors identify priority issues and deal with matters of public policy and governance at the state, national and global levels. Our research arm, NGA Solutions, helps in developing and implementing innovative solutions to public policy challenges.*"[74]

NGA's role in convening state leadership nationally, providing guidance and expertise on policy issues and uniting bipartisan members, facilitating vital information should not be understated. At minimum, its existing convening capacity would allow for civil society groups of experts to connect with state leadership on digital contact tracing issues. Importantly, some of the decisions states need to make with their own implementation plans that could have national significance for digital tracing solutions—such as multi-server communication, the airport problem solution, or public education around approved state apps—could occur as part of NGA's current working structure.

Public Health Authorities

States' top public health authorities that also report to national level public health authorities must be a part of this stakeholder group. Public health officials within each state will make key decisions around digital contact tracing. Their consistent reporting to the federal level is ongoing and their perspective on how digital contact tracing can help manual contact tracing efforts is central to the purpose of coordination. Their insights will help determine what data is most useful. State public health officials can help to map out the numbers and status of public health servers, answering a key question among technologists. Recently, the Centers for Disease Control (CDC), put out resources for Health Departments on digital contact tracing tools.[75] As further guidance will be recommendation-focused, public health authorities who will decide on and implement strategies should also be represented.

74 National Governors Association. About Us. https://www.nga.org/about/

75 Centers for Disease Control. Preliminary Criteria for the Evaluation of Digital Contact Tracing Tools for COVID-19. https://www.cdc.gov/coronavirus/2019-ncov/downloads/php/prelim-eval-criteria-digital-contact-tracing.pdf

Technology Companies

Google's and Apple's solution and partnership with PACT Protocol position them to be an important stakeholder, especially through the current interface with public health officials in states (and other countries). Whether they are represented through the civil society groups or have formal representatives that will field questions and provide some guidance for specification requests, mainly around server connectivity, their participation is also important. In this type of convening a regional, state or national approach could be discussed for best coordination with the GAEN solution. Organizations like Safe Paths, or other app developers, may also eventually be represented, however the functionality of this coordinating group may be to set recommendations for app development and may not be contingent on their engagement in initial coordinating and convening sessions.

—

The coordinating and convening council would not only address the scale of technical solutions and decisions by states, but would also provide a forum for discussing policy and process decisions, especially around privacy and liability. For instance, to take advantage of the benefits of both the Bluetooth proximity and location methods in digital contact tracing, states could consider forming a consortium to present Apple and Google with a comprehensive plan to address privacy concerns associated with location data, accept liability for privacy, and appeal for the use of the API in conjunction with location data. Or states would convene to coordinate solutions for the airport problem or joint education around state app downloads. Even a series of digital convenings planned to address core topics for the implementation of digital contact tracing, recommendations on development or security standards, and other insights to additional technology integration with COVID-19 manual tracing effort with these stakeholders in attendance would allow for digital contact tracing efforts to get underway at the speed and with the national coordination that will be needed for its success.

Recommendations for State and Local Governments

As the states hold primary responsibility for public health, much rests on the decisions that governors, state public health authorities, and their leadership teams make together in this effort. Execution may be delegated to local governments; as such, we recommend strong coordination between state and local governments in policy, planning, and execution of anti-COVID-19 operations.

State Task Force Representatives

- States may already have special task forces created that are helping address and advise COVID-19 response. For mitigation efforts, a special committee within the existing task force should exist to explore digital contract tracing and other technology solutions to assist manual contact tracing. The function of this task force is to unite people to think through decisions and ease the ability to cross-collaborate and give recommendations for implementation:

    - *The state CIO*, responsible for securing systems and advising on any server interface considerations.
    - *The tech innovator role*, helping create technology or advise on assessing potential technologies such as apps the state may approve. Importantly, this role can work both to better understand the hurdles public health officials are trying to overcome and to suggest alternate technologies or development processes closely attuned to evolving needs. The USDR may help imbed tech experts with states for evolving considerations.
    - *Public health officials and researchers,* who can advise on what they need from manual and digital tracing. Public health officials, in the GAEN solution, will need to approve app vendors and may also oversee the state department of health's collection of individual public health servers. In

the location data solution, officials may need to advise on best use for the data. In either solution, they should advise around the data that is needed and helpful to collect via apps using either tracing tool and set important privacy measures.

- *A public communicator role*, who can understand processes and can advise and lead public advisory efforts.
- *Senior aides*, who are also involved in the state's overall strategic response, the public health department's continued data collection and reporting, who can be a connecting element with other parts of an existing task force, governor and health department leadership.

Preparing for Digital Contact Tracing

- States should determine if and how digital contact tracing will be incorporated into the overall public health plan. The integration into manual contact tracing operations and development of a technical ecosystem described below will take some time to accomplish.
- While we recommend a national coordinating body as described above to address and scale solutions, in the meantime or at a minimum, officials should work with the PACT team members and/or Apple and Google if using the Bluetooth proximity method, and with vendors such as Safe Paths if using the location data method to further understand the technology, protocol, requirements, and privacy considerations. USDR and CTTF may also be additional resources for specific implementation considerations.

- To Use the GAEN Solution:
    - States must develop or approve a software application (app) in order for its public health departments to utilize data derived from the API. The Defending Digital Democracy Project's Appendix for Vendor Selection and Management offers a starting point for security considerations when hiring a vendor.[76] In addition to adapting considerations like these, vendors will need to have a commitment to collaboration with public health authorities, Google and Apple, and among other stakeholders determined by the state. Only approved apps can leverage the API by accessing data locally stored on phones for its purposes.
    - As this is being considered, the development, rollout, deployment, maintenance, and communication of the app is paramount. Pressing needs for potential solutions to be activated quickly means that usual development and testing timelines may get condensed, increasing the possibility for issues with acquisition and scaling. With any solution public education and transparency are vital.
    - States should consider potential interoperability with other state health systems as part of the app's functionality.
    - Through the proposed coordinating body that must include Google and Apple, states should discuss how to address user travel, whether through server interoperability, multiple app downloads or other methods. Ensuring technologists and engineers are at the table of this body are paramount to resolving this issue.
    - States must define the Too Close for Too Long (TC4TL) parameters it wishes to apply to the Bluetooth Chirp data. This means that parameters within the app will define if Bluetooth Chirps warrant concern based on the proximity

76 Harvard Kennedy School Defending Digital Democracy Project, "Election Cybersecurity Playbook for State and Local Election Officials," *Belfer Center for Science and International Affairs,* February 2018, https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook#app1.

and the length of time when in contact with an infected person.

- States must define how users will obtain and report certification of infection.
- States will need to define any additional security protocols for public health servers to interface with data derived from the Google and Apple API and individual patient data reporting.

- To Use Location Services (i.e. the Safe Paths app):

    - States must define how users will obtain and report certification of infection
    - States will need to develop policies and processes for handling and redacting sensitive personally identifiable, health, and location data, as well as consider redress procedures for abuse of information. Handling any personally identifiable information, opens states to additional security concerns with such data, it may also raise additional privacy concerns. States should consider their needs and goals with location data:

        » As an example, whether to use a Denmark model of assessing location data at an aggregated and pseudonymized level to track the spread of the infection, versus location data that traces individual movement without anonymization providing efficient tracing but raising privacy concerns.

        » Further in line with the Denmark model, states should seriously consider never collecting or storing any personally-identifiable information if this data is not needed for contact tracing efforts. At a minimum, states should have an explicit goal to stop collecting and destroy data, echoing the "right to be forgotten" in the European Union's General Data Protection Regulation.

- States should consider how this data can help mitigation efforts without the likelihood of integrating with proximity tracing data interaction.
- States should consider the security of this data and include CISO or CIO in decisions made for using the app and operationalizing the data.

Integrating with Manual Contract Tracing Efforts

- As any digital contact tracing effort is meant to assist manual tracing, states should determine how the two will be integrated.
- States might consider establishing a virtual command center, possibly in line with the fusion cell concept, resource-and-time-permitting. This decision should carry considerations for overall security and risk.
- Manual contact tracers should be trained to operate using safe cybersecurity practices to ensure user data privacy and security. This might include use of a VPN, encrypted communications like Signal, and use of secure contact databases. States should consider the cost for these services in their plan.
- States will need to work closely with public health officials to determine how data utilized by manual tracing and data collected through digital means are combined and assessed for response.
- Connect technologists with manual contact tracers to better understand the challenges and opportunities as tracing teams build relationships with patients, communicate with them and adapt as mitigation efforts continue.
- States should consider how to include the population without smartphones in the overall tracing efforts and how this population also receives important information.

Cybersecurity

- While the Bluetooth Chirp data stored in decentralized public health servers is anonymous, other data might be identifiable. Each state is responsible for securing any location, health, and personal data. Given the increased cyberattacks and overall vulnerability of the health system during this pandemic, states should prioritize the security of their digital health systems.
- States should determine interoperability of systems across their state and review the accreditation process of organizations that feed into the system.
- Where some municipalities might lack broadband access, states should work to increase access and security. To assist in this effort, municipalities should consider forming regional coalitions to gain economies of scale when faced with resource constraints.

Public Interface

- Getting the public to participate in the contact tracing system, especially the digital aspect, will require trust and buy-in. As such, states should conduct transparent and coordinated communications with the public across a range of media to include radio and television broadcast, print, social media.

    - These communications should include public education and awareness on privacy, the ability to opt in or out, how the technology and associated software app will work, and reporting and notification procedures. Utah's website is one helpful model: https://coronavirus.utah.gov/healthy-together-app/

- Fighting disinformation around manual and digital tracing efforts will be vital. Rampant COVID-19 disinformation is being reported. States need to establish response processes to quickly identify and respond to incidents of disinformation and unintentional

misinformation. A Defending Digital Democracy Project Playbook on Influence Operations and Mis/Disinformation Incident Response Communications are forthcoming and can be shared by emailing connect@d3p.org.

Recommendations for Tech Companies

To further develop technological solutions during this effort, companies should coordinate with public health officials to maintain awareness of the issues. Long-term, the digital public health system may need a large-scale security upgrade. Secure cloud providers may be able to help in this regard.

Google and Apple

- Google, Apple, and PACT should develop an onboarding network and criteria for states to have a clear understanding of how its public health server(s) will need to be set up to receive data from the API and from individual downloads. System specific recommendations should be communicated.
- Continue testing and improving data collection and usage and work with states to address mobility and server issues
- Continue efforts to coordinate with public health officials to prepare them to use the solution and to maintain awareness of the issues

App Developers

- Developers should seek to have transparent data privacy and security standards that can be communicated to state governments and the general public.
- Developers should clearly articulate how data will be processed and flow through the system and should describe security at each layer of its solution.

- They should work to understand how to integrate technology with existing public health infrastructure by working closely with state officials to design app functionality.
- As much as possible, developers should integrate with public health officials and manual contact tracers in order to understand the problems they are working to address through technology.
- Developers should ensure the user interface is simple and easy to use.
- Location Services App Developers: Should be transparent about what personal data will be collected on the user and make redacting this data easy for the user, rather than giving responsibility to government officials. Depending on the goal of how location data will be used, consider not storing any personally identifiable information.

Recommendations for Congress

Congress should pass legislation with funding for manual and digital contact tracing and other technical solutions as a part of any further funding for COVID-19 response. Any proposed legislation to increase the manual tracing work force should also provide funding to states and public health officials to put toward assistive technology that also addresses data privacy and security as manual tracing progresses and states' response efforts evolve.

- Congress should continue to address the lack of national laws to govern data privacy and security and create legislation that safeguards any individual health data reported through application vendors to public health officials, especially for COVID-19-specific applications.
- For location data being used to track COVID spread, Congress should also create at a minimum legislation that requires a sunset of such tracking measures. Legislation should also seek to address the complexity and the responsibility of data use and storage. Guidance around when to and who will destroy data should be considered. The responsibility of who stores data and for what length of time may also necessitate security guidance. Given the uncertain path ahead with COVID-19, and unknown timelines for when this data may no longer be needed, legislation should seek to safeguard users from surveillance measures beyond understanding the spread of the virus.

Conclusion

After approximately twelve weeks of physical distancing and quarantine, Americans are eager to get back to work and resume social interaction. All potential solutions should be considered as states look to reopen their operations and economies. Given the near-total immersion of technology in our daily lives, it is natural to look to a tech solution to help us; however, there are several factors that should be considered. Technology must be assistive in the overall effort; it is not the only solution and in this context it must augment manual operations. States must hammer out policy and technical decisions if they choose to employ digital contact tracing. For digital contact tracing to be effective public trust is a must. Any technology solution deployed should offer transparency and security to gain the public trust.

In order to utilize and scale digital contact tracing, focused coordination and support within a state will be required to prepare the systems, processes, and design approval needed to implement either Bluetooth or location data digital tracing solutions. How officials plan to use the data collected for COVID-19 mitigation, as well as specific requirements to utilize either solution, may determine how states choose to pursue. A national coordinating body that convenes to brief officials, provide recommendations, and facilitate contact with experts will help make short-term implementation efforts of digital contact tracing solutions more successful.

We must emphasize that fighting the spread of COVID-19 rests on expanded, widely available, rapid testing for all Americans. Without testing, no manual or digital contact tracing effort will be effective. Federal government efforts must be channeled into making this a reality.

Once this pandemic is largely extinguished, it is imperative that the United States engage in long-term planning for the next pandemic or disaster, because there will be one. On a technology front, this involves reviewing, building, and securing digital infrastructure needed to deliver information and services to governments and the public. Comprehensive cybersecurity and information integrity within states is vital to good governance, both during peacetime and during various types of crises. Congress should

consider how it may update or create legislation dealing with privacy and technology to meet future challenges.

This is an unprecedented situation within our lifetime which calls for decisive action in the face of uncertainty. We hope this report provides some clarity to leaders weighing the decision to use digital contact tracing and other technology solutions in their COVID-19 battle plans.

Resources

Apple Documentation:
https://www.apple.com/covid19/contacttracing

CDC Contact Tracing Guidelines:
https://www.cdc.gov/coronavirus/2019-ncov/php/open-america/contact-tracing.html

COVID-19 Technology Task Force:
https://www.crttf.org/covid19/

Google Documentation:
https://blog.google/documents/57/Overview_of_COVID-19_Contact_Tracing_Using_BLE.pdf

Private Automated Contact Tracing (PACT):
https://pact.mit.edu/

MIT Safe Paths:
http://safepaths.mit.edu/ and
https://www.media.mit.edu/projects/safepaths/overview/

National Governors Association:
https://www.nga.org/

Partners in Health:
https://www.pih.org/coronavirus-response

U.S. Digital Response:
https://www.usdigitalresponse.org/

The Cyber Project
The Defending Digital Democracy Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org

Printed in the United States of America