May 13th, 2020

TLP White

This week, Hacking Healthcare takes an extended look at digital contact tracing. We begin with an overview of contact tracing and its digital development. Next, we briefly outline some of the political, technical, logistical and legal impediments and considerations of digital contact tracing efforts. We then provide an update on where the United States (U.S.) and other countries are in their efforts to implement digital contact tracing programs. Finally, we wrap-up with some thoughts on what it all means. Welcome back to *Hacking Healthcare*.

Overview

Contact Tracing Explained*:* Contact tracing has existed as a fundamental disease control measure for decades.[1] Simply put, contact tracing is a means to help prevent the spread of disease by assessing who may be infected, and who may have come into contact with infected individuals. By advising those who may have been exposed to isolate or seek medical attention, further infections may be inhibited.

Analog and Digital: Traditionally, contact tracing has been carried out in person by groups of specially trained individuals who possess strong interpersonal communication skills, detailed knowledge of medical science, and a deep understanding of the ethical and privacy issues involved.[2] However, advances in technology and the near ubiquity of smartphones have created an environment able to support the implementation of digital contact tracing, often in the form of a smartphone application.

Digital Development: Unfortunately, the rapid spread of COVID-19 and the infancy of digital contact tracing efforts has left little time for governments, healthcare sectors, and citizens to debate and agree on what implementing large scale digital contact tracing efforts should look like. In the wake of the current global pandemic, digital contact tracing efforts are varied and often appear to reflect the characteristics of their societies and governing leadership. However, all of them are grappling with legal, logistic, political, and technical issues at an international, national, and even sub-national level.

May 13th, 2020

Deployment Impediments and Considerations

***Legal*:** Contact tracing could potentially implicate many different areas of the law. Privacy and security, employment and labor, and healthcare law to name a few. Organizations are thinking about how digital contact tracing can be used or accessed by an employer, and what legal challenges could arise from this new application of technology. As contact tracing develops further, more regulations will potentially emerge at the state and federal level, as well in international regimes, adding further clarity to possible legal liability. To help understand some of the current issues, we have outlined a few high-level legal privacy considerations for selecting and using contact tracing technology. We will follow legal developments in this area to provide updated guidance and analysis when possible.

What are some of the legal privacy considerations when selecting and using contact tracing technology?

Unlike other areas of the world, the U.S does not currently have a universal privacy law. As a result, contact tracing technologies in the U.S are instead subject to a variety of laws that come from sources like states, industry sectors, or even common law. This type of piecemeal regulation can make it difficult for employers to know what privacy standards to look for when examining new technologies. Below are a few privacy questions healthcare organizations should consider regarding contact tracing:

What information is the application collecting and how is it being used?

The practices involved in gathering consumer information through an application (notice, permissions, etc.) have been on the market for more than a decade. The difference now with contact tracing is that the information is being used and shared for public health purposes. This new use potentially raises questions around common law and civil liberty privacy protections. The applications under development may or may not have considered the privacy and security implications when developing the technology. It is essential that organizations understand the product they are using, what information is being collected, the purpose of such collection, and how the information will be stored.

Some apps may ask basic health questions while others ask for more detailed personal information, or even track employee movements on an automated basis. Depending on the type of information being collected, a number of privacy laws could be triggered. For example, some states, like Illinois, have biometric laws in place. The Illinois Biometric Information Privacy Act ("BIPA")[3] requires that informed consent be obtained prior to collecting biometric information, including facial scans. BIPA includes a private right of action for violations which as the name implies, means that individuals who believe they have been harmed by the collection of their biometric information can bring legal action.

There is also the California Consumer Privacy Act (CCPA)[4] that went into effect January 1, 2020, and has an enforcement date set for July 1, 2020. While there is an exemption for employee information under the CCPA until 2021, employers are still required to provide California

residents with a notice of collection of personal information, and the purpose for such collection. The employee information exemption does not cover the CCPA's private right of action. This means that businesses could face liability for unauthorized access or disclosure stemming from failure to implement and maintain reasonable security procedures around contact tracing.

These laws are just a few of the possible regulations that could be implicated around contact tracing apps. Given the potential privacy implications, organizations should at the very least understand the basics of what information the contact tracing app is collecting and how that information is being used. Some questions to ask may include:

- ✓ Is proximity data collected through Bluetooth or geolocation data;
- ✓ If proximity data is collected, how and where is it stored;
- ✓ How long will the application keep the personal information;
- ✓ Will the personal information be shared with others, if so, is it in its native form or at an aggregated or de-identified level?
- ✓ Will any biometric data be collected?

How is this application securing the personal information?

Another important aspect to consider is how the application will keep the personal information secure. Understanding what type of encryption is used, if it's used at all, or if the app uses anonymization or de-identification are important parts of the vetting process.

Ensuring an app uses proper security measures also helps protect against employer liability. Employers could be at risk through state breach law or through its own representations made in privacy policies or other internal documents if an employer uses technology that does not adequately safeguard employee information.

For employees, how will information about the program be communicated?

Clear notice of information collection is an important privacy principle. Companies should consider reviewing their employee-facing privacy policies, confidentiality guidelines, and procedures for communicating information about contact tracing programs.

Are any of our users located in the EU or other international locations?

European governmental bodies have focused extensively on contact tracing apps. Recently, the European Commission issued guidance that "sets out features and requirements which apps should meet to ensure compliance with EU privacy and personal data protection legislation, in particular the General Data Protection Regulation (GDPR) and the ePrivacy Directive."[5] Failure to comply with the GDPR can result in serious fines. Companies should understand if any of its employees are subject to requirements imposed in the EU or elsewhere.

Logistic: The primary logistic impediment to digital contact tracing relates to adoption. Ideally, digital contact tracing efforts are most effective when the entirety of a population is actively participating as instructed. However, experts within the U.K. note that such efforts can be beneficial even when less than half of a population is participating.[6] Impediments to reaching this goal include a population's lack of trust that such efforts are safe and private, a lack of awareness that such efforts exist, insufficient ease of use, a lack of devices with the appropriate hardware and software, and the voluntary nature of most digital contact tracing efforts.

Technical: Technical considerations include whether the digital contact tracing efforts are centralized or decentralized, as well as what type of technology is involved. The technical specifications of a contact tracing effort influence privacy, security, and legal considerations. Furthermore, the technical aspects of digital contact tracing can be affected by the preferences of private sector entities whose devices are being used.

Centralized vs Decentralized: One of the major technical rifts that exists between various digital contact tracing methods is deciding between centralization or decentralization. Centralized efforts have lost support lately, but the U.K. and France are prominent examples of countries who have opted for the added control and visibility centralized methods can offer. On the other side are decentralized efforts. This is most prominently exemplified by Google and Apple's effort which has won the support of Canada and many European countries.[7]

Centralized methods can take different forms, but they rely on a central computer server and database to determine which devices have been in contact with which other devices. This method requires a device to connect to and upload its unique identifier along with all identifiers that encountered it. Upon receiving this information, the centralized system determines who if anyone needs to receive an alert with relevant health information.[8] Centralized methods are generally operated or overseen by a government's health agency.

Centralized methods are most often criticized for their potential privacy abuses. Privacy advocates are wary that governments will not strictly define an appropriate scope for digital contact tracing and that sufficient oversight will not exist to ensure that all health, location, and personal data is protected and promptly deleted after use. Furthermore, critics are skeptical of how effective data anonymization in centralized efforts really are.

Advocates stress that privacy and security issues can be addressed, that national governments are often in the best position to secure such data, and that centralization allows aggregated data to provide visibility that can improve policy and healthcare responses.[9]

Decentralized methods can also take different forms, but the underlying concept is generally the same. In decentralized methods, a device will only provide its own unique identifier to a centralized system and will download an updated database of identifiers that includes those that have been reported as infected.[10] This allows for the processing of whether or not an

individual came into contact with an infected individual to be done locally without sharing with the centralized system who they have come into contact with.[11]

Decentralized methods are generally more difficult to intentionally misuse for the collection of personal information depending on the specifics of how they are implemented.[12] However, it is not impossible, and decentralized methods remain open to trolling or malicious actions[13, 14]

Location data: Another significant technical aspect is the decision to collect or not to collect location data. Location data can be collected in various ways including making use of a device's GPS sensor, Wi-Fi connections, and cellular data. This data can be used paint a picture of where infections are taking place at a more granular level, which in turn can help direct healthcare response efforts and policy. However, doing so can create privacy and security concerns.

Political: There are a few political considerations that will impact the effectiveness of digital contact tracing. First, it is important to note that differences of opinion between governments on how digital contact tracing should be implemented may negatively impact interoperability between them. This could impact both domestic and international travel and commerce. Secondly, there are some worries that nationalistic pride will incentivize the creation of homegrown digital contact tracing efforts, even when other solutions may be available.[15]

Contact Tracing in the United States

Federal: Within the U.S., a comprehensive and organized nation-wide strategy for contact tracing is lacking. In the absence of a strong federal response, states have forged ahead with their own in-person and digital contact tracing approaches.[16, 17] The lack of federal guidance and collaboration between states has led to some lawmakers citing privacy, efficiency, and interoperability concerns.[18]

State: As of this writing, digital contact tracing efforts have already been launched in at least three states: North Dakota, South Dakota, and Utah.

Both North and South Dakota began using an application in early April called Care19, the product of a partnership between the North Dakota Department of Health and private sector company ProudCrowd.[19] The exact details of the application's implementation are vague, but it appears to track and log a user's movements using WiFi, cell data, and GPS location data.[20] Upon testing positive for COVID-19, a user may receive a request from their respective state's health department to receive that logged location data to potentially inform them of new COVID-19 hotspots.[21] It is unclear if the two states systems are interoperable, or if it would be possible to integrate other contact tracing applications with Care19.[22]

In late April, Utah partnered with social network Twenty to launch the application Healthy Together. Healthy Together is billed as an app that allows Utahns to "track their symptoms and find their nearest testing center," but it also uses Bluetooth, location, and GPS data to track contacts and movement.[23] Concerning to some is the admission that "Public health officials and

a limited number of development employees with Twenty Holdings, Inc. will have access to your name, phone number, and location data."[24]

Contact Tracing Internationally

U.K.: The U.K. is currently in the midst of rolling out its self-developed centralized contact tracing application that is available on both Apple and Google's app stores.[25] Developed by their National Health Service (NHS) in partnership with outside experts and the National Cyber Security Centre (NCSC), their contact tracing application has been deployed on the Isle of Wight prior to a national release.[26] [27] As of Monday evening, the application had been downloaded approximately 55,000 times. However, because the app does not track location data there is no way of knowing if all of those downloads come from the island's roughly 140,000 residents.[28]

As noted above in the logistical challenges, widespread adoption is key for the U.K.'s program to be successful, with experts suggesting that "80% of smartphone users - 60% of the population - would have to actively use it" for the best results.[29] There is skepticism over how realistic that target is considering the popular messaging application WhatsApp is only installed on roughly 67% of UK smartphones, and that only 52% of respondents of a recent poll indicated they were likely to download the application.[30, 31] The U.K. has allegedly not removed the possibility of ditching its own effort in favor of Google and Apple's decentralized model which has gained popularity recently.

E.U.: There is no unanimous consensus within the E.U., however it appears that most countries, including Germany, Italy, Estonia, and Ireland favor the decentralized approach outlined by Apple and Google.[32] Notably absent are the recently Brexited U.K. and France. Between the improved privacy and the almost assured interoperability of the Apple and Google effort, there are strong incentives for that decentralized approach to become the norm.

South Korea: South Korea has been described as a major success story, reporting fewer than 300 deaths, in part because of their use of digital contact tracing. However, their methods are likely to appear extreme in many western countries. The Guardian reports that "People who tested positive were asked to describe their recent movements, aided by GPS phone tracking, surveillance camera records and credit card transactions."[33] While many would find some of these measures uncomfortable, the appear to have helped the Korea Centres for Disease Control and Prevention take decisive steps to limit COVID-19's spread.[34]

Conclusion and Analysis

Fundamentally, digital contact tracing as a technical embodiment of a long-established medical practice is not controversial. Furthermore, it is generally accepted that digital methods are not a standalone silver bullet that will return society to normal. However, when used as one tool of a larger holistic strategy to prevent and contain infectious diseases, digital contact tracing can be incredibly powerful.

May 13th, 2020

As with the introduction of most new technologies, digital contact tracing is going through a normal process of legal, regulatory, and political pushback as it challenges the status quo. The security, privacy, and legal considerations, as well as the technical and logistical impediments that are hotly contested are not unique. Unfortunately, the circumstances resulting from COVID-19 have exacerbated the potential short-term benefits of the technology, while diminishing any chance to calmly debate its merits and drawbacks at length.

The uncertainty that surrounds how such measures will be implemented, what laws and regulations will ultimately end up applying, and how effective such measures can be, will only become clear as the weeks and months elapse. That may not be comforting now, but the lessons learned and the norms that evolve from COVID-19 will assuredly help prepare us to use such technologies to their maximum potential in the future.

Congress –

Tuesday, May 12th:
- Senate Committee on the Judiciary: "Examining Liability During the COVID-19 Pandemic"

Wednesday, May 13th:
- Senate Committee on Homeland Security and Governmental Affairs: "Evolving the U.S. Cybersecurity Strategy and Posture: Reviewing the Cyberspace Solarium Commission Report"

Thursday, May 14th:
- House Committee on Energy and Commerce - Subcommittee on Health: "Protecting Scientific Integrity in the COVID-19 Response"

International Hearings/Meetings –

EU –

Tuesday, May 12th:
-European Parliament - Environment, Public Health, and Food Safety meeting

Conferences, Webinars, and Summits –

-- MAZE Ransomware Webinar – Webinar (5/13/2020)
https://h-isac.org/hisacevents/maze-ransomware-webinar/
--Cybersecurity for the 21st Century by IronNet – Webinar (5/14/2020)
https://h-isac.org/hisacevents/byironnet/
--H-ISAC Monthly Member Threat Briefing – Webinar (5/26/2020)
https://h-isac.org/hisacevents/h-isac-monthly-member-threat-briefing-8/
-- H-ISAC Virtual Security Workshop – Webinar (5/27/2020)
https://h-isac.org/hisacevents/nz-virtual-workshop/
--Shared Solution Webinar: Managed Threat Detection for the Rest of Us – Webinar (5/28/2020)
https://h-isac.org/hisacevents/managed-threat-detection-for-the-rest-of-us/
--Identity for the CISO – Becoming 'Identity-Centric' – Webinar (6/3/2020)
https://h-isac.org/hisacevents/identity-for-the-ciso/

May 13th, 2020

--H-ISAC Security Workshop - Frederick, MD (6/9/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-frederick-md/
-- An H-ISAC Framework for CISOs to Manage Identity – Webinar (5/10/2020)
https://h-isac.org/hisacevents/framework-for-cisos-to-manage-identity/
--AAMI Exchange – New Orleans, LA (6/12/2020-6/15/2020)
https://h-isac.org/hisacevents/aami-exchange/
--H-ISAC Security Workshop - Lisbon, Portugal (6/17/2020) (POSTPONED)
https://h-isac.org/hisacevents/h-isac-security-workshop-lisbon-portugal/
--H-ISAC Security Workshop - Buffalo, NY (6/23/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-buffalo-ny-2/
H-ISAC Monthly Member Threat Briefing – Webinar (6/30/2020)
https://h-isac.org/hisacevents/h-isac-monthly-member-threat-briefing-9/
--Healthcare Cybersecurity Forum - Mid-Atlantic – Philadelphia, PA (7/17/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426497
--Healthcare Cybersecurity Forum - Rocky Mountain – Denver, CO (7/20/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426499
--Healthcare Cybersecurity Forum – Southeast – Nashville, TN (9/9/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426517
--H-ISAC Security Workshop - Greenwood Village, CO (9/16/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-greenwood-villiage-co/
--Healthcare Cybersecurity Forum – Northeast – Boston, MA (9/22/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/427126
--H-ISAC Cyber Threat Intel Training - Titusville, FL (9/22/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-titusville-fl/
--H-ISAC Security Workshop - Forchheim, Germany
https://h-isac.org/hisacevents/h-isac-security-workshop-forchheim-germany/
--Summit on Security & Third Party Risk – National Harbor, MD (9/28/2020-9/30/2020)
https://h-isac.org/hisacevents/summit-on-security-third-party-risk/
--Healthcare Cybersecurity Forum – Texas – Houston, TX (10/8/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428840
--CYSEC 2020 – Dubrovnik, Croatia (10/27/2020 – 10/28/2020)
https://h-isac.org/hisacevents/cysec-2020-croatia/
--H-ISAC Security Workshop - Mounds View, MN (10/27/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-buffalo-ny/
--Healthcare Cybersecurity Forum - Pacific Northwest – Seattle, WA (10/28/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428886
--H-ISAC Security Workshop - Seattle, WA – (10/29/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-seattle-wa-2/
--Healthcare Cybersecurity Forum – California – Los Angeles, CA (11/12/2020)
https://h-isac.org/hisacevents/healthcare-cybersecurity-forum-california-2/
--H-ISAC Security Workshop - Paris, France (11/18/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-paris-france/

May 13th, 2020

Sundries –

--ENISA: Cybersecurity in the healthcare sector during COVID-19 pandemic
https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-healthcare-sector-during-covid-19-pandemic
-- FBI, DHS to go public with suspected North Korean hacking tools
https://www.cyberscoop.com/north-korea-hacking-hidden-cobra-dhs-fbi/
-- OCR Shares COVID-19 Privacy and Security Threat Resources
https://healthitsecurity.com/news/ocr-shares-covid-19-privacy-and-security-threat-resources

Contact us: follow @HealthISAC, and email at contact@h-isac.org

---

[1] https://www.cdc.gov/coronavirus/2019-ncov/php/principles-contact-tracing.html
[2] https://www.cdc.gov/coronavirus/2019-ncov/php/principles-contact-tracing.html
[3] http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57
[4] https://www.oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf
[5] https://ec.europa.eu/info/sites/info/files/5_en_act_part1_v3.pdf
[6] https://www.theguardian.com/world/2020/may/10/only-50-of-britons-would-download-nhs-tracing-app-poll
[7] https://www.bbc.com/news/technology-52355028
[8] https://www.bbc.com/news/technology-52579547
[9] https://iapp.org/news/a/centralized-vs-decentralized-eus-contact-tracing-privacy-conundrum/
[10] https://www.bbc.com/news/technology-52355028
[11] https://techcrunch.com/2020/04/06/eu-privacy-experts-push-a-decentralized-approach-to-covid-19-contacts-tracing/
[12] https://iapp.org/news/a/centralized-vs-decentralized-eus-contact-tracing-privacy-conundrum/
[13] https://threatpost.com/google-apple-contact-tracing-system-cyberattacks/155287/
[14] https://www.eff.org/deeplinks/2020/04/apple-and-googles-covid-19-exposure-notification-api-questions-and-answers
[15] https://www.bbc.com/news/uk-england-hampshire-52558894
[16] https://thehill.com/policy/healthcare/496957-states-build-contact-tracing-armies-to-crush-coronavirus
[17] https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/HHS.2020.4.30.pdf
[18] https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/HHS.2020.4.30.pdf
[19] https://www.valleynewslive.com/content/news/North-Dakota-launches-Care19-app-to-combat-COVID-19-569448971.html?utm_campaign=wp_the_cybersecurity_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_cybersecurity202
[20] https://www.wsj.com/articles/apps-to-track-the-new-coronavirus-have-an-old-problem-getting-the-downloads-11588115728
[21] https://covid.sd.gov/care19app.aspx
[22] https://www.lawfareblog.com/contact-tracing-apps-united-states
[23] https://coronavirus.utah.gov/healthy-together-app/
[24] https://coronavirus.utah.gov/healthy-together-app/
[25] https://www.bbc.com/news/uk-england-hampshire-52617236
[26] https://www.bbc.com/news/uk-england-hampshire-52617236
[27] https://www.zdnet.com/article/the-uks-coronavirus-tracing-app-everything-you-need-to-know/
[28] https://www.zdnet.com/article/the-uks-coronavirus-tracing-app-everything-you-need-to-know/
[29] https://www.bbc.com/news/explainers-52442754
[30] https://www.theguardian.com/world/2020/may/10/only-50-of-britons-would-download-nhs-tracing-app-poll

---

[31] https://www.bbc.com/news/explainers-52442754
[32] https://www.bbc.com/news/technology-52355028
[33] https://www.theguardian.com/world/2020/apr/23/test-trace-contain-how-south-korea-flattened-its-coronavirus-curve
[34] https://www.theguardian.com/world/2020/apr/23/test-trace-contain-how-south-korea-flattened-its-coronavirus-curve