# COVID-19 Technology and Privacy:

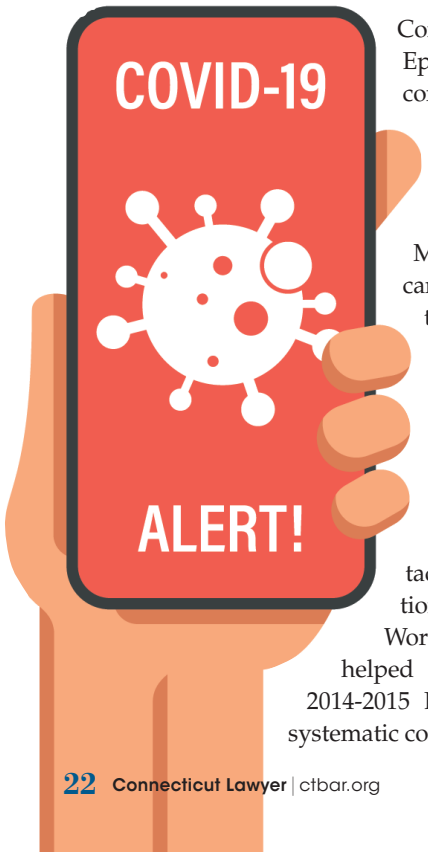
# Contact Tracing Technology and its Implications for U.S. Privacy Law

## Part 1: Contact Tracing: The Apple | Google API

By DAYLE A. DURAN

### What is contact tracing?

Contact tracing is a manual method that state and local public health agencies (PHAs) use to track suspected or confirmed infections and notify individuals who may have had exposure to an infected person.[1] PHAs are tasked with optimizing public health and safety and contact tracing is an important tool to achieve that end. While there are privacy concerns surrounding the general concept of contact tracing, legislatures and PHAs tend prioritize the public good of infectious disease management over the attendant privacy risks.




Contact tracing is not new. Epidemiologists have used contact tracing to battle the spread of infectious disease for at least a hundred years. During World War I, the U.S. Military screened American troops to track and halt the spread of syphilis and gonorrhea.[2] In the latter half of the 20th century, the World Health Organization led a global effort to eradicate smallpox and tuberculosis, relying heavily on contact tracing and vaccination.[3] More recently, the World Health Organization helped countries suppress the 2014-2015 Ebola outbreak through systematic contact tracing.[4]

PHAs conduct contact tracing by drawing on the infected person's memory of places they went and people they saw while they were infectious but undiagnosed. Manual contact tracing relies on the accuracy of an infected person's memory and the ability of PHAs to deploy a large enough workforce to quickly interview infected people and notify exposed contacts. To be effective for COVID-19 mitigation purposes, manual contact tracing relies on the infected person's *accurate* recollection of the prior two weeks and knowledge about all of those with whom they had close contact.

### What did Apple and Google build to help with contact tracing?

As COVID-19 spread in the U.S. and across the world in the spring of 2020, contact tracing technology dominated headlines as nations scrambled to find effective ways to manage the pandemic.[5] In response, Apple and Google developed a new technology to address the inefficiency and inaccuracy of manual contact tracing.[6] Their application programming interface (API) is essentially a courier that software developers can use as a foundation for contact tracing apps.

Mechanically, APIs function like the server at a restaurant. The server takes, executes, and delivers the customer's food order. An app is the restaurant itself: the knives, forks, tables, walls, menu, décor, dining style—*the experience*. Suffice it to say, a restaurant needs the server to take, relay, and deliver the dine-in order to the restaurant customer. Much the same, apps leverage APIs to deliver an experience to the end-user.

Because APIs require an app to conduct contact tracing, many PHAs are commissioning compatible apps and technical specifications. For example, MIT developed a technical standard/specification called PACT: Private Automated

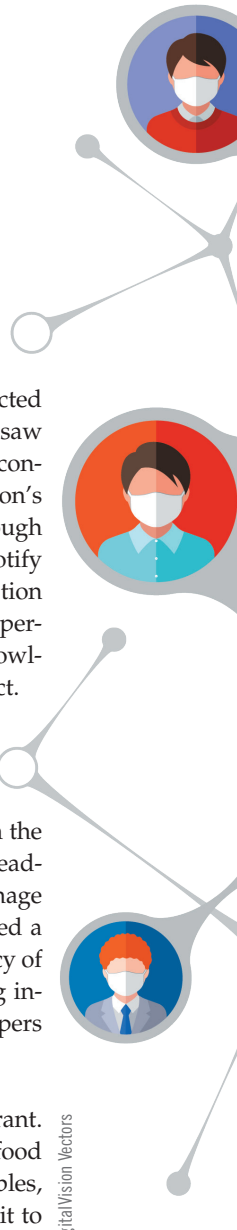


Image credit: PeterPencil/ Ani_Ka/ DigitalVision Vectors

Contact Tracing to aid in U.S.-based contact tracing efforts.[7] At the close of 2020, twenty U.S. states and the District of Columbia had either deployed an app leveraging the API or committed to developing one.[8] Meanwhile, most of the European Union along with the United Kingdom, Brazil, Ecuador, Canada, Japan, Kazakhstan, New Zealand, Russia, Saudi Arabia, and a number of other countries have also released Apple/Google API-compatible contact tracing apps.[9]

## Can this technology boost the efficacy of contact tracing without getting creepy?

Apple and Google's API functions using Bluetooth beacons. Bluetooth beacons are a string of random numbers, or "chirps," broadcasted and received by a Bluetooth-enabled device. The strength and duration of the chirp tells the receiving device the proximity and duration of exposure to the chirp's source. Chirps do not carry any personally identifiable information (PII) and they operate without any connection to the internet. Most importantly, the user must affirmatively turn on the chirp functionality and voluntarily download an API-compatible contact tracing app. Simply downloading a software update like iOS 13.5 will not automatically activate contact tracing.[10] Only after the app is downloaded and the chirp is enabled will the device broadcast chirps and capture the ones it encounters. As a result, the device owner must consent to sending and receiving the chirps. Privacy professionals call this "opt-in" consent.

The API adds a layer of complexity to the resulting data sets by changing the emitting device's chirp every ten to 20 minutes.[11] This variance makes it difficult to identify and track the chirper because no name, location data, or other PII is associated with the chirp. Next, the system stores the list of chirps the device has sent and received on each individual device. The device does not share that list *at all* unless its owner opts-in to sharing their COVID-19 diagnosis with the relevant PHA via the app.

Once the list is shared with the PHA, the agency will make those anonymous lists accessible through the app. Users can then direct the system to periodically cross reference the updated PHA list. This allows the system to determine whether the user came into contact with an infected person. If the system detects a matching chirp it will prompt the user to take additional steps, like consulting with the PHA, self-quarantining, or seeking medical attention.

Randomized chirps, siloed data, and decentralized databases add an important layer of complexity that makes de-anonymization more difficult, especially because the resulting datasets are only accessible to the PHA behind each app—*not Apple and not Google*.

## Is this technology anonymous?

For all practical purposes, yes—or at least it is more anonymous than traditional contact tracing. The CARES Act requires COVID-19 testing sites to report all diagnostic and screening results to a PHA anyway.[12] It is standard practice for PHAs to use this information to track and mitigate the spread of COVID-19 and other diseases that significantly impact community health. Whether officials undertake that process manually or with the use of technology, PHAs will receive data on designated communicable diseases and contact tracing will continue. Technology-assisted contact tracing creates an opportunity for PHAs to efficiently recommend follow-up testing, medical care, and quarantine in a manner that is anonymous enough not to require any personally identifying information.

If used as intended, the technology described above increases the accuracy and efficiency of contact tracing without sacrificing an impactful amount of privacy. The API demonstrates the real-life application of several core privacy principles like privacy by design, data minimization, and privacy by default.[13] As a result, connecting the Bluetooth beacons back to the originating device and then to a specific individual would require a chain of convoluted events. Because of the API's design, the resulting data sets will likely be of limited utility even if they are used in ways that deviate from the original intent of collection.

However, no aggregated data set can be irreversibly private since hackers, private businesses, nosey people, and ne'er-do-wells will always exploit cracks to access valuable data. But even governments operating in the name of the public good are cause for concern. As noted in a recent IAPP article,[14] in 2017 private data aggregators like 23andMe and AncestryDNA made a database of genetic information available to California law enforcement. While the data sharing resulted in the capture of a serial killer, it also drew ire for what may well have been a massive warrantless search in violation of the Fourth Amendment.

Because all contact tracing methods, whether manual or technology-assisted, are imperfect and raise privacy concerns we need more than strong privacy design to protect against nefarious data use and functionality creep. American lawmakers must pass legislation addressing the use of COVID-19 contact tracing data to ensure the information cannot be exploited for uses outside of the intended purpose.

# Part 2: A Proposed Bills Provide Insight on Potential Solutions in Protecting Privacy in Contract Tracing and Beyond

By DENA M. CASTRICONE

In this country, we have only a patchwork of sectoral and state-specific privacy laws. None of those laws provide a nationwide solution or a foundation from which guidance or regulations could emerge to protect data collected in connection with a public health emergency (PHE). The lack of a federal privacy law has left Congress scrambling to propose needed legislation.

Over a three-week period in the Spring of 2020, U.S. Senators proposed three different privacy bills related to the PHE and emerging technologies designed to track the spread of disease. On May 7, 2020, a group of Republican senators introduced the *COVID-19 Consumer Data Protection Act*.[15] One week later, led by Connecticut's Senator Richard Blumenthal, 12 Democrats and one Independent introduced the *Public Health Emergency Privacy Act*.[16] Then, on June 1, a bipartisan group of senators introduced the *Exposure Notification Privacy Act*[17] (ENPA). Unlike the partisan bills, which both sought to regulate the collection and processing of COVID-19-related health information more broadly, the ENPA focused solely on contact tracing technologies called "automated exposure notification services" designed to trace any infectious disease. The ENPA would permit only entities working with a public health authority (PHA) to collect data for purposes of offering an automated notification service.

Before discussing the proposed legislation any further, it is important to note that none of the three proposed bills made it out of committee. There were a couple of important factors at play: (1) we were (and currently are) in the middle of a pandemic and the legislators were likely more focused on access to care, stimulus, and emergency aid than privacy; and (2) we were just months away from a contentious presidential election. While none of the three proposed privacy bills received material attention from Congress, they highlight some of the challenges in passing any consequential federal privacy legislation. As a result, these three bills provide useful insight on what to expect in imminent federal privacy legislation proposals as well as how future legislation might protect data during PHEs.

Generally, the ENPA sought to dramatically limit the collection, use, and transfer of any data in automated exposure notification systems, specifically prohibit commercial use, and require confirmation of a diagnosis from a PHA or licensed healthcare provider. Further, it would not preempt state law or provide for a private right of action (two areas where Democrats and Republicans rarely agree) and it requires breach notification. These key provisions, along with others discussed below, made the ENPA the best proposal.

## Commonalities Among the Proposed Bills

All three bills contained the following requirements:

- Affirmative express consent from the individual prior to collecting, using, or transferring data, and such consent cannot be inferred from inaction;
- Limitation on the collection, use, and transfer of data to the least amount necessary to carry out the permitted purpose;
- Reasonable security practices (the ENPA provided the most robust requirements, including a risk assessment and defined reasonable security practices as those accepted by information security experts);
- Deletion of data when it is no longer being used (the ENPA requires deletion at least every 30 days, on a rolling basis, or as directed by a public health authority);
- A privacy policy providing transparency on collection, use, and transfer (the ENPA offered the most detail on required policy contents); and
- Enforcement by the Federal Trade Commission under the unfair and deceptive acts provision of the Federal Trade Commission Act, while granting authority to state attorneys general to enforce locally.

## The ENPA's Key Differences

### Scope

Both partisan bills sought to apply broadly to information collected and used that relates to the COVID-19 PHE. The ENPA, on the other hand, was written to apply solely to automated exposure notification services (AENS) (like those built with the Apple/Google API) and would require that AENS can only be provided in collaboration with a PHA. The ENPA would apply to AENS for any infectious disease, not just COVID-19, which would be useful if there is another pandemic in the future.

Generally, technology-specific legislation designed to address a particular issue, such as contact tracing apps, has diminishing utility because such legislation is often outdated as soon as it is passed, which may not have been an issue with the ENPA. Its focus on AENS and meaningful rules within the bill itself makes it functional without the need to create regulations, which is a time-consuming and cumbersome process (the other bills required rulemaking).

### Authorized Diagnosis

The ENPA sought to prohibit AENS operators from collecting diagnosis information unless a PHA or a licensed health care provider confirms the diagnosis. This promotes public trust by mitigating the risk of honest or malicious false positive reports. Further, only an individual with such an authorized diagnosis could permit the AENS to process that information. Neither partisan bill addressed diagnosis information.

### Health Insurance Portability and Accountability Act (HIPAA) Exemption

Both partisan bills specifically would exempt HIPAA covered entities and business associates from compliance. Conversely, the ENPA does not mention HIPAA at all. Due to its limited applicability to AENS, the ENPA does not seek to regulate health information in the same way as the partisan bills. Under the ENPA, if a health care provider, that is also a covered entity under HIPAA, wants to operate an AENS, that provider must comply with the new rules, regardless of HIPAA. This is beneficial because the same rules will apply to all AENS operators.

### Nondiscrimination

The ENPA seeks to make it unlawful for anyone to discriminate against an individual based on data in an AENS or based on an

individual's decision not to use such a service. The Democratic bill shares a similar provision, but more broadly prohibits housing, employment, and other discrimination as well as governmental interference with voting rights based on collected data. Given the narrow purpose for which the AENS operators can collect, use, or transfer covered data, the broader provisions in the Democratic proposal may not be warranted.

## Tech Industry Influence on the ENPA

Some believe that Google and Apple have had too much influence on the ENPA as several of Google/Apple's policies for their contact tracing API overlap with ENPA provisions (e.g., voluntary individual use and required collaboration with a PHA). While industry influence on legislation has the potential to be problematic, it is not unduly concerning here. This is an unprecedented collaborative effort between competitors of all kinds. Because nothing happens expeditiously in Congress and because we needed a speedy legislative solution, it made sense to follow the lead of two tech giants that have set aside competition and financial gain to tackle the PHE.

## Recommendations for an Improved ENPA

Should members of Congress decide to re-introduce the ENPA, there are a couple of additional privacy protection measures that would improve the proposed bill. First, the ENPA needs a sunset provision that accounts for enactment of federal privacy legislation that covers the data at issue. Second, under the ENPA, aggregate data is not regulated. It may be worth requiring an affirmative act to prove that aggregate data is not reasonably linkable to a person, such as requiring a documented expert determination.[18] Finally, law enforcement use of raw or aggregate data should be clearly limited or prohibited. As noted in Part I above, law enforcement has seized on the availability of genetic data held by companies like 23and Me and AncestryDNA in a way that consumers never imagined.

## Conclusion

The ENPA's proposed language would have adequately addressed the privacy risks related to unintended use and function creep. Most importantly, it would have avoided creating a new set of health privacy rules that would serve only to further complicate the already complex and confusing privacy ecosystem in this country. If Congress decides to enact the ENPA or a similar bill, hopefully, it will inspire a collaborative effort to create comprehensive federal data privacy legislation, so that there is applicable law in place in the event of a future crisis. ■

***Dayle A. Duran*** CIPP/US *is a privacy attorney based in Massachusetts. She works in the legal department at Wellframe, a digital health management platform, where she advises on compliance with U.S. privacy laws as well as implementation of privacy-by-design throughout the software development lifecycle.*

***Dena M. Castricone*** CIPP/US, CIPM, *managing member of DMC Law, LLC, is a privacy and healthcare attorney with substantial experience helping healthcare providers navigate privacy challenges and counseling clients on compliance with privacy laws. Attorney Castricone also advises healthcare providers on a broad range of regulatory compliance, risk management, and day-to-day operational issues.*

■ This article originally appeared on the DMC Law LLC Blog (dmclawllc.com/blog), and updates have been made for this publication.

### NOTES

1. *Principles of Contact Tracing*, CDC, www.cdc.gov/coronavirus/2019-ncov/php/principles-contact-tracing.html.
2. Frederick Holmes, MD, *Medicine in the First World War*, University of Kansas Medical Center, www.kumc.edu/wwi/index-of-essays/venereal-disease.html.
3. *Frequently asked questions and answers on smallpox*, World Health Organization, www.who.int/csr/disease/smallpox/faq/en/; Matt Begun, *et al., Contact Tracing of Tuberculosis: A Systematic Review of Transmission Modeling Studies*, www.ncbi.nlm.nih.gov/pmc/articles/PMC3762785/.
4. *Ebola publications: surveillance contact tracing, laboratory*, WHO, www.who.int/csr/resources/publications/ebola/surveillance/en/.
5. TraceTogether, safer together (Singapore), www.tracetogether.gov.sg/; COVIDSafe (Australia), www.health.gov.au/resources/apps-and-tools/covidsafe-app#get-the-app; NHS COVID-19 App (United Kingdom), www.nhsx.nhs.uk/covid-19-response/nhs-covid-19-app/ Stopp Corona (Austria), participate.roteskreuz.at/stopp-corona/; TraceCovid (United Arab Emirates), https://tracecovid.ae/; ProteGO (Poland), www.gov.pl/web/cyfryzacja/zycie-po-kwarantannie–przetestuj-protego.
6. *Privacy-Preserving Contact Tracing*, www.apple.com/covid19/contact-tracing.
7. *PACT: Private Automated Contact Tracing*, pact.mit.edu/.
8. Zac Hall, *Which U.S. states are using Apple's Exposure Notification API for COVID-19 contact tracing?*, 9to5 Mac (Dec. 7, 2020), https://9to5mac.com/2020/12/07/covid-19-exposure-notification-api-states/.
9. Mishaal Rahman, *Here are the countries using Google and Apple's COVID-19 Contact Tracing API*, XDA Developers (Dec. 28, 2020), www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries/.
10. *Fact check: Apple's iOS 13.5 update does not automatically activate contact tracing or allow the government to "track" users*, Reuters (May 26, 2020), www.reuters.com/article/uk-factcheck-apple-update/fact-check-apples-ios-135-update-does-not-automatically-activate-contact-tracing-or-allow-the-government-to-track-users-idUSKBN2322TF.
11. *Exposure Notification Frequently Asked Questions* (May 2020 v1.1), Apple | Google, https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-BluetoothSpecificationv1.2.pdf.
12. *Reporting Lab Data*, CDC, www.cdc.gov/coronavirus/2019-ncov/lab/reporting-lab-data.html.
13. Ann Cavoukian, Ph.D., *Privacy by Design The 7 Foundational Principles*, https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf.
14. Evelina Manukyan, Joseph Guzzetta, *How function creep my cripple app-based contact tracing*, IAPP Privacy Advisor, tinyurl.com/y9k4kjg8.
15. www.commerce.senate.gov/services/files/A377AEEB-464E-4D5E-BFB8-11003149B6E0.
16. iapp.org/media/pdf/resource_center/Public_Health_Emergency_Privacy_Act.pdf
17. www.cantwell.senate.gov/imo/media/doc/Exposure%20Notification%20Privacy%20Bill%20Text.pdf