BEWARE: BLUETOOTH AHEAD

The Civil Rights & Privacy Dangers of Deploying Bluetooth to Track COVID-19 Exposure

ALBERT FOX CAHN, ESQ. &
JOHN YANY VEISZLEMLEIN

MAY 7, 2020

STOP
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

As the world grapples with the unprecedented impact of COVID-19, some governments and companies are turning to new forms of electronic surveillance that have no proven public health benefit, but which pose a clear threat to privacy and civil rights. Though the effectiveness of these surveillance programs is unclear, their capacity to eviscerate users' privacy has been well demonstrated.[1] In the United States, many political and business leaders are calling for the implementation of Bluetooth beacon tracking,[2] and Apple and Google have jointly developed an Application programming interface or "API" for that purpose. However, this system has the potential to violate the fundamental privacy of billions of people and deserves greater skepticism.

Current Electronic COVID-19 Surveillance Systems, Generally

The Bluetooth API developed by Apple and Google, is an attempt to automate contact tracing—a system of identification, testing, and quarantining of those infected with COVID-19. Traditional, manual contact tracing requires a disease detective to ask a patient for a list of people they've interacted with during the disease incubation period. This model has been relied on for decades to mitigate transmissible diseases.[3] It enables public health authorities to identify and quarantine infected individuals, especially during the incipiency of a potential epidemic or pandemic. This manual system has its benefits, allowing interviewers to develop trust with patients who might be fearful of an automated system.

Manual contact tracing is proven to work, but it is also quite resource intensive, making it costly to scale. Additionally, manual contact tracing is only as effective as patients' memories, though many patients are able to refresh their recollection by examining their credit card transactions, schedule, and other records. Also, while patients likely won't know the name of every person on the surrounding rows of an airplane, contact tracers can use flight manifests to supplement patient data.

In contrast, technology-assisted contact tracing (TACT) relies directly on electronic contact and location data, reducing reliance on person-to-person interviews. Countries are

---

[1] *See, e.g.*, Saheli Roy Choudhury, *Singapore Says It Will Make Its Contact Tracing Tech Freely Available to Developers*, CNBC (Mar. 25, 2020), https://www.cnbc.com/2020/03/25/coronavirus-singapore-to-make-contact-tracing-tech-open-source.html; Williams, *supra* note 18; Zak Doffman, *Coronavirus Spy Apps: Israel Joins Iran and China Tracking Citizens' Smartphones to Fight COVID-19*, FORBES (Mar. 14, 2020), https://www.forbes.com/sites/zakdoffman/2020/03/14/coronavirus-spy-apps-israel-joins-iran-and-china-tracking-citizens-smartphones-to-fight-covid-19/#4b9423d2781b; Nemo Kim, *'More Scary than Coronavirus': South Korea's Health Alerts Expose Private Lives*, GUARDIAN (Mar. 5, 2020), https://www.theguardian.com/world/2020/mar/06/more-scary-than-coronavirus-south-koreas-health-alerts-expose-private-lives; Paul Mozer, Raymond Zhong & Aaron Krolik, *In Coronavirus Fight, China Gives Citizens a Color Code, with Red Flags*, N.Y. TIMES (Mar. 1, 2020), https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html;

[2] Tony Room, Elizabeth Dwoskin & Craig Timberg, *U.S. Government, Tech Industry Discussing Ways to Use Smartphone Location Data to Combat Coronavirus*, WASH. POST (Mar. 17, 2020), https://www.washingtonpost.com/technology/2020/03/17/white-house-location-data-coronavirus.

[3] *See* Karen Landman, *How the Painstaking Work of Contact Tracing Can Slow the Spread of an Outbreak*, NAT'L PUB. RADIO (Mar. 10, 2020), https://www.npr.org/sections/health-shots/2020/03/10/814129534/how-the-painstaking-work-of-contact-tracing-can-slow-the-spread-of-an-outbreak.

increasingly experimenting with various forms of TACT, developing systems that differ both in the type of data used and how that data is acquired.

In some countries, such as Austria and Italy, governments are requesting higher-level anonymized data from telecommunications companies to identify general trends about the movements of citizens.[4] This has limited usefulness as a contact-tracing tool, since it does not link individual phones with people who have tested positive for COVID-19. (at least, not without some amount of additional information or effort by the government to de-anonymize the data).

In other systems, such as those being used by China and Israel, the government has warrantless access to individual location records, tracking users' every move through cell-phone geolocation data.[5] Cell phones generally track their users' position using either cell-site location information (CSLI)—which relies on the phone's connection to nearby cell towers to triangulate its location—or the Global Positioning System (GPS), which uses satellites. CSLI provides only a rough approximation of location,[6] making it ineffective for contact tracing. While GPS is far more accurate (to within 16 feet),[7] it still cannot accurately identify whether two phones are within six feet of one another, which is generally cited as the maximum distance of person-to-person COVID-19 transmission. This hasn't stopped some countries from relying on GPS location data for contact tracing. If you are found to have been in the same place as someone who later tested positive for COVID-19, you are then quarantined. In addition to their dubious efficacy, these uses of technology raise obvious privacy concerns: in order for the system to work, the government must track where most of its citizens are at all times.

The resulting data is ripe for exploitation by other government agencies. For example, it could be used by law enforcement to circumvent the ordinary requirement to get a warrant before engaging in electronic surveillance. It could be used to track and harass political adversaries. It could even be used to identify and persecute religious minorities, communities of color, and undocumented immigrants.

---

[4] Dave Gershgorn, *We Mapped How the Coronavirus Is Driving New Surveillance Programs Around the World*, MEDIUM: ONEZERO (Apr. 9, 2020), https://onezero.medium.com/the-pandemic-is-a-trojan-horse-for-surveillance-programs-around-the-world-887fa6f12ec9; Isobel Asher Hamilton, *Compulsory Selfies and Contact-Tracing: Authorities Everywhere Are Using Smartphones to Track the Coronavirus, and It's Part of a Massive Increase in Global Surveillance*, BUS. INSIDER (Apr. 14, 2020), https://www.businessinsider.com/countries-tracking-citizens-phones-coronavirus-2020-3.

[5] David B. Halbfinger, Isabel Kershner & Ronen Bergman, *To Track Coronavirus, Israel Moves to Tap Secret Trove of Cellphone Data*, N.Y. TIMES (Mar. 16, 2020), https://www.nytimes.com/2020/03/16/world/middleeast/israel-coronavirus-cellphone-tracking.html; Paul Mozer, Raymond Zhong & Aaron Krolik, *In Coronavirus Fight, China Gives Citizens a Color Code, with Red Flags*, N.Y. TIMES (Mar. 1, 2020), https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html.

[6] Robinson Meyer, *This Very Common Cellphone Surveillance Still Doesn't Require a Warrant*, ATLANTIC (Apr. 14, 2016), https://www.theatlantic.com/technology/archive/2016/04/sixth-circuit-cellphone-tracking-csli-warrant/478197 ("This data, CSLI, isn't as precise as a GPS coordinate, but in urban or suburban areas it can narrow someone's location down to less than two miles and give their angular relationship to the nearest cell tower.").

[7] Krista Merry, Pete Bettinger, *Smartphone GPS Accuracy Study in an Urban Environment*, PLOS ONE (July 18, 2019).

In an attempt to avoid these privacy pitfalls, Singapore introduced a partially-decentralized system in March that relies on Bluetooth signals to detect proximity between devices.[8] Google and Apple's system is in many ways an attempt to scale up and further decentralize this system, enabling its use worldwide.

How Google/Apple's Exposure Notification System Works

Bluetooth is a global standard for low-powered, short-range wireless data transfer. The technology is used for everything from streaming music to home stereo speakers to peer-to-peer data transfers from cellphones and tablets.[9] Modern cellphones and other electronic devices come equipped with Bluetooth, and thus are able to link with nearby devices.[10]

In April, Apple and Google announced their partnership on the Exposure Notification System, adding software to their mobile operating systems (iOS and Android, respectively) to enable compatible devices to operate Bluetooth beacons. These beacons broadcast to, and listen for broadcasts from, all nearby Bluetooth devices.[11] Devices use signal to estimate the physical proximity of the other Bluetooth device, [12] and if the two devices are close enough for long enough, they exchange a cryptographic code. Which interactions are "close enough" and "long enough" to count as a contact for epidemiological purposes will be design choices made by the public health officials who roll out individual applications built upon the Exposure Notification System.[13] Unfortunately, a variety of factors can alter Bluetooth signal strength, making it a potentially unreliable indicator of distance.[14]

The peer-to-peer exchange creates a partially decentralized model of contact tracing. Under the Exposure Notification System, each device would generate a unique, daily

---

[8] Aaron Holmes, *Singapore is Using a High-Tech Surveillance App to Track the Coronavirus, Keeping Schools and Businesses Open. Here's How It Works*, BUS. INSIDER (Mar. 24, 2020), https://www.businessinsider.com/singapore-coronavirus-app-tracking-testing-no-shutdown-how-it-works-2020-3.

[9] *How Does Bluetooth Work?*, SCI. AM. (Nov. 5, 2007), https://www.scientificamerican.com/article/experts-how-does-bluetooth-work.

[10] BLUETOOTH, BLUETOOTH MARKET UPDATE 2018 21 (2018), https://www.bluetooth.com/wp-content/uploads/2019/03/Bluetooth_Market_Update_2018.pdf ("100% of smarthphones, tablets, and laptops shipped in 2018 will include Bluetooth.").

[11] EXPOSURE NOTIFICATION: FREQUENTLY ASKED QUESTIONS (Apr. 2020), https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.0.pdf.

[12] Darrel Etherington & Natasha Lomas, *Apple and Google Update Joint Coronavirus Tracing Tech to Improve User Privacy and Developer Flexibility*, TECHCRUNCH (Apr. 24, 2020), https://techcrunch.com/2020/04/24/apple-and-google-update-joint-coronavirus-tracing-tech-to-improve-user-privacy-and-developer-flexibility.

[13] Khari Johnson, *Apple and Google Build More Privacy and Flexibility into Bluetooth Contact Tracing Tech*, VENTURE BEAT (Apr. 24, 2020), https://venturebeat.com/2020/04/27/pixel-buds-with-hands-free-google-assistant-go-on-sale-for-179.

[14] Chaim Gartenberg, *Here's How Apple and Google Will Track the Coronavirus with Bluetooth*, VERGE (Apr. 14, 2020), https://www.theverge.com/2020/4/14/21220644/apple-googles-bluetooth-low-energy-le-coronavirus-tracking-contact-tracing (The more obstacles and obstructions between devices — like backpacks, pockets, walls, or windows — the worse Bluetooth LE is at accurately tracking something since those obstructions will degrade the radio signal strength used to measure distance.").

"Temporary Exposure Key," which it would uses, in turn, to generate a new "Rolling Proximity Identifier" for the phone every 10–20 minutes.[15] When devices come into contact with one another, they exchange these short-lived Rolling Proximity Identifiers. If the duration and signal strength reach the minimums set by the public health authority, each device then stores the identifier they received from the other phone, along with some metadata about the interaction that is transmitted along with the identifier (*i.e.*, how strong the signal between the two devices was, the length of the interaction, and the time at which it occurred).[16]

If a person tests positive for COVID-19, they send their Temporary Exposure Keys from the past two weeks will be transmitted to a "diagnosis server" operated by the public health authority, which then makes available aggregated lists of COVID-19-positive Temporary Exposure Keys to all of its users.[17] Users' phones can then use the daily Temporary Exposure Keys to calculate all of the Rolling Proximity Identifiers for each infected person over the past two weeks.[18] If one of the codes calculated from the key matches a code stored in the user's contact log, the user is told that they have been exposed to COVID-19. The Temporary Exposure Key also enables their phone to decrypt the metadata associated with the interaction that exposed them. Depending on the design choices made by the public health agencies instituting the technology, this may permit the user to see how many days ago the interaction occurred.[19]

Privacy Impact

The Exposure Notification System provides some privacy protections compared to centralized tracking systems (such as GPS phone data or cellphone tower data), but it will potentially arm governments and companies with expanded ability to track private individuals' movements. One concern is that institutional actors will be able to use their networks of Bluetooth beacons to deanonymize Bluetooth data.

In the case of someone reporting a positive diagnosis, institutional actors potentially will see dozens or even hundreds of locations associated with an individual's movements. Take, for

---

[15] EXPOSURE NOTIFICATION: CRYPTOGRAPHY SPECIFICATION (Apr. 2020), https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-CryptographySpecificationv1.1.pdf; EXPOSURE NOTIFICATION: FREQUENTLY ASKED QUESTIONS, SUPRA NOTE 11.

[16] EXPOSURE NOTIFICATION: CRYPTOGRAPHY SPECIFICATION, SUPRA NOTE 15; EXPOSURE NOTIFICATION: FREQUENTLY ASKED QUESTIONS, SUPRA NOTE 11; Clifford Colby, *How Apple and Google Will Fight the Spread of Coronavirus with Contact Tracing*, CNET (Apr. 26, 2020), https://www.cnet.com/how-to/how-apple-and-google-will-fight-the-spread-of-coronavirus-with-contact-tracing.

[17] EXPOSURE NOTIFICATION: CRYPTOGRAPHY SPECIFICATION, SUPRA NOTE 15; EXPOSURE NOTIFICATION: FREQUENTLY ASKED QUESTIONS, SUPRA NOTE 11; Zack Whittaker, Darrell Etherington, *Q&A: Apple and Google Discuss Their Coronavirus Tracing Efforts*, TECHCRUNCH (Apr. 13, 2020), https://techcrunch.com/2020/04/13/apple-google-coronavirus-tracing (saying that the data will be "'relayed' through servers run by the health organizations across the world, and will not be centralized").

[18] EXPOSURE NOTIFICATION: CRYPTOGRAPHY SPECIFICATION, SUPRA NOTE 15.

[19] Stephen Nellis, *Apple, Google Update Coronavirus Contact Tracing Tech Ahead of Launch*, REUTERS (Apr. 24, 2020), https://www.reuters.com/article/us-apple-google-contact-tracing/apple-google-update-coronavirus-contact-tracing-tech-ahead-of-launch-idUSKCN2262NT.

example, a commercial landlord who installs Bluetooth beacons in the building's elevator banks. Such beacons would allow the landlord to monitor the infection rate in each building and floor, and better deploy cleaning resources. But such data could also be paired with closed-circuit TV cameras to monitor for unwanted subleases, large gatherings, and other infringements of building rules.

Alternatively, an advertising agency could repurpose existing Bluetooth beacons in stores and, combined with credit-card data or facial recognition, identify someone with a positive test. Commercial entities could then use that data to do anything from notifying employers of employees' positive tests, to marketing medical services to potential patients. Similarly, employers could use the same types of beacons to directly monitor their workers' health.

Regardless of the intent behind the Exposure Notification System, others will harness the API in ways Apple and Google can neither control nor predict. The companies are creating a foundational technology,[20] but others can easily build on that foundation. No matter how many privacy safeguards the technology companies bake into the software, they can't control how governments and companies use that technology, including how it's paired with other tracking tools. Utah, and North and South Dakota, are already working to pair Bluetooth data with GPS location data.[21]

The Illusion of Consent

Google, Apple, and their partners have frequently highlighted the fact that users will need to "opt in" to the Exposure Notification Service. This means that while millions of devices will be updated automatically to add the Bluetooth tracking capability, the software will not be enabled on a user's device without their consent. But simply requiring users to click "I agree" falls short of ensuring that users actually consent to Bluetooth tracking.

As an initial matter, simply saying "I consent" is not enough to prove users gave *informed* consent. Will the update clearly explain to the user the system's functionality and potential privacy pitfalls so that they can make an informed decision of whether to opt in? Or will it give overly technical descriptions in the middle of a pages-long operating system update log? This concern is especially pronounced if users are promised that Bluetooth data will remain anonymous when it can actually be deanonymized.

Apart from the software terms of services, many users may not get to decide for themselves if they agree to new tracking. Most states and localities have no restrictions to block employers from forcing employees to agree to Bluetooth tracking as a condition of employment. Similarly, schools—especially private and parochial institutions—may require students to accept tracking

[20] EXPOSURE NOTIFICATION: FREQUENTLY ASKED QUESTIONS, SUPRA NOTE 11 at 3 ("[B]oth companies will release application programming interfaces (APIs) that allow contact tracing apps from public health authorities to work across Android and iOS devices . . . .").

[21] Stephen Nellis, Paresh Dave, *Showdown Looms Between Silicon Valley, U.S. States over Contact Tracing Apps*, REUTERS (Apr. 24, 2020), https://www.reuters.com/article/us-health-coronavirus-usa-apps/showdown-looms-between-silicon-valley-u-s-states-over-contact-tracing-apps-idUSKCN22702F.

as a condition of attendance, or transit providers could require use to board buses or trains. While a government mandate to use a tracking app would like face scrutiny in the courts, those who opt out of tracking might find themselves effectively forced to opt out of public life.

Uncertain Benefits

Despite the obvious privacy risks, it remains unclear if the Bluetooth API will be effective in combatting COVID-19. As previously discussed, the system's goal would be to contact trace—to identify people who have been in contact with an infected individual. However, in order to be effective, we need to be able to actually test people who receive an exposure notification for COVID-19. The unvarnished truth is that we simply don't have the testing capacity to make this a reality.

In the months since the COVID-19 pandemic began, the United States has only tested 5.8 million people[22]—only 17 tests for every 1,000 Americans.[23] But with each COVID-19 carrier potentially interacting with dozens of individuals, we would need millions of new tests, not every month, but every *day*, to track potential exposure. We don't have a fraction of that testing capacity, and we're unlikely to anytime in the foreseeable future. Until the U.S.'s testing capacity drastically increases, the Exposure Notification System will be more of a distraction than a plausible way of controlling COVID's spread.

But even if testing were available, the Exposure Notification System would face another fundamental challenge: obtaining a critical mass. A contact-tracing system is only as effective as the number of users it's able to attract. While no contact tracing will detect every COVID-19 transmission, many experts believe a Bluetooth-based system would need to sign-up 60% of Americans. If only a small subset of the public signs up, most transmissions will go completely undetected, and tracing data will remain a dystopian novelty. In Singapore, a similar system has only a 12% usage rate,[24] and recent polling has indicated that the majority of Americans are uncomfortable using this application.

And what about the millions of Americans who don't have a smartphone capable of running the application? Apple and Google are limiting Exposure Notification System to phones made in recent year[25] that have sufficient battery life.[26] Alarmingly, that design excludes the exact same Americans who are most at risk. Nearly half of those over 60 lack any cell phone, let

---

[22] *COVID-19 Coronavirus Pandemic*, WORLDOMETER (last visited Apr. 28, 2020).
[23] *Id.*
[24] Alex Hern & Kari Paul, *Apple and Google Team Up in Bid to Use Smartphones to Track Coronavirus Spread*, GUARDIAN (Apr. 10, 2020), https://www.theguardian.com/world/2020/apr/10/apple-google-coronavirus-us-app-privacy.
[25] Jules Wang, *Apple and Google Add New Tech Specs for Coronavirus Tracking Tool to Boost User Privacy*, ANDROID POLICE (Apr. 24, 2020), https://www.androidpolice.com/2020/04/24/apple-and-google-are-working-together-to-fight-coronavirus-with-a-new-contact-tracing-tool.
[26] Stephen J. Vaughan-Nichols, *How Apple and Google Coronavirus Contact Tracing Will Work*, ZDNET (Apr. 14, 2020), https://www.zdnet.com/article/how-apple-and-google-coronavirus-contact-tracing-will-work.

alone a smartphone capable of ruling the Exposure Notification System.[27] Additionally, the low-income Americans who face the greatest economic pressure to continue at jobs with a high risk of exposure are also less likely to have a smartphone.[28]

Additionally, there are a number of engineering challenges that will undermine the reliability of Bluetooth tracking. What if someone with COVID-19 lives in the apartment above yours? Your phones may be less than six feet from one another without any risk of transmission. The public health authorities who create testing parameters might choose settings that are fairly effective in wealthy suburbs, but which lead to exponentially more errors in high-density urban housing.

This risk of inaccurate exposure notification is also acute for lower-income households where multiple users share access to a single device. Additionally, the choice to keep a phone in one's handbag versus their pants pocket could weaken Bluetooth signals and lead to higher error rates, introducing a significant risk of gender bias. While it is far from certain that these sorts of biases will manifest in practice, the onus should be on designers and public-health authorities to test for such discrimination in advance. Without proper safeguards, design assumptions could exacerbate the pronounced inequalities of the American healthcare system.

What Does This All Mean?

In a time of crisis, some national political leaders promote the motto "what do you have to lose?" But when it comes to flawed contact tracing, we may not just lose our privacy, we could lose even more lives to COVID-19. By relying on flawed and inaccurate data, we could misallocate health resources, and undermine our ability to respond. Indeed, Singapore, the one-time poster child for this technology, has seen cases spike in recent weeks; it now has nearly the same per capita rate of infection as the United States.[29]

But invasive and ineffective contact-tracing applications could not just threaten public healthy, they could threaten democracy itself. History teaches that privacy invasions often outlive the emergency they are intended to combat. To this day, the USA Patriot Act provisions that were supposed to expire in 2005 are being debated for renewal to 2024. Google and Apple pledged that their system will be phased out when the pandemic ends, but there is no clear definition of what that "end" will look like.[30] Moreover, the COVID-19 threat won't simply disappear in a day, but will fade over the course of years. Even if Apple and Google are willing to turn away from this tracking in a few months or years, the tech giants may find that the governments whose laws they are bound by are less willing to forsake the technology.

---

[27] *Mobile Fact Sheet*, PEW RES. CTR. (June 12, 2019), https://www.pewresearch.org/internet/fact-sheet/mobile.
[28] *Id.*
[29] *COVID-19 Coronavirus Pandemic*, WORLDOMETER (last visited Apr. 28, 2020).
[30] Russell Brandom, *Apple and Google Pledge to Shut Down Coronavirus Tracker When Pandemic Ends*, VERGE (Apr. 24, 2020), https://www.theverge.com/2020/4/24/21234457/apple-google-coronavirus-contact-tracing-tracker-exposure-notification-shut-down.

Surveillance Technology Oversight Project, Inc.

40 Rector Street
9th Floor
New York, NY, 10006

www.STOPSpying.org

STOP
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT