APRIL 10, 2020

eff.org

The Challenge of Proximity Apps For COVID-19 Contact Tracing

ESPAÑOL

Around the world, a diverse and growing chorus is calling for the use of smartphone proximity technology to fight COVID-19. In particular, public health experts and others argue that smartphones could provide a solution to an urgent need for rapid, widespread contact tracing—that is, tracking who infected people come in contact with as they move through the world. Proponents of this approach point out that many people already own smartphones, which are frequently used to track users' movements and interactions in the physical world.

But it is not a given that smartphone tracking will solve this problem, and the risks it poses to individual privacy and civil liberties are considerable. *Location tracking*—using GPS and cell site information, for example—is not suited to contact tracing because it will not reliably reveal the close physical interactions that experts say are likely to spread the disease. Instead, developers are rapidly coalescing around applications for *proximity tracing*, which measures Bluetooth signal strength to determine whether two smartphones were close enough together for their users to transmit the virus. In this approach, if one of the users becomes infected, others whose proximity has been logged by the app could find out, self-quarantine, and seek testing. Just today, Apple and Google announced joint application programming interfaces (APIs)

using these principles that will be rolled out in iOS and Android in May. A number of similarly designed applications are now available or will launch soon.

As part of the nearly unprecedented societal response to COVID-19, such apps raise difficult questions about privacy, efficacy, and responsible engineering of technology to advance public health. Above all, we should not trust any application—no matter how well-designed—to solve this crisis or answer all of these questions. Contact tracing applications cannot make up for shortages of effective treatment, personal protective equipment, and rapid testing, among other challenges.

COVID-19 is a worldwide crisis, one which threatens to kill millions and upend society, but history has shown that exceptions to civil liberties protections made in a time of crisis often persist much longer than the crisis itself. With technological safeguards, sophisticated proximity tracking apps may avoid the common privacy pitfalls of location tracking. Developers and governments should also consider legal and policy limits on the use of these apps. Above all, the choice to use them should lie with individual users, who should inform themselves of the risks and limitations, and insist on necessary safeguards. Some of these safeguards are discussed below.

How Do Proximity Apps Work?

There are many different proposals for Bluetooth-based proximity tracking apps, but at a high level, they begin with a similar approach. The app broadcasts a unique identifier over Bluetooth that other, nearby phones can detect. To protect privacy, many proposals, including the Apple and Google APIs, have each phone's identifier rotated frequently to limit the risk of third-party tracking.

When two users of the app come near each other, both apps estimate the distance between each other using Bluetooth signal strength. If the apps estimate that they are less than approximately six feet (or two meters) apart for a sufficient period of time, the apps exchange identifiers. Each app logs an encounter with the other's identifier. The users' location is not necessary, as the application need only know if the users are sufficiently close together to create a risk of infection.

When a user of the app learns that they are infected with COVID-19, other users can be notified of their own infection risk. This is where different designs for the app significantly diverge.

Some apps rely on one or more central authorities that have privileged access to information about users' devices. For example, TraceTogether, developed for the government of Singapore, requires all users to share their contact information with the app's administrators. In this model, the authority keeps a database that maps app identifiers to contact information. When a user tests positive, their app uploads a list of all the identifiers it has come into contact with over the past two weeks. The central authority looks up those identifiers in its database, and uses phone numbers or email addresses to reach out to other users who may have been exposed. This places a lot of user information out of their own control, and in the hands of the government. This model creates unacceptable risks of pervasive tracking of individuals' associations and should not be employed by other public health entities.

Other models rely on a database that doesn't store as much information about the app's users. For example, it's not actually necessary for an authority to store real contact information. Instead, infected users can upload their contact logs to a central database, which stores anonymous identifiers for everyone who may have been exposed. Then, the devices of users who are not infected can regularly ping the authority with their own identifiers. The authority responds to each ping with whether the user has been exposed. With basic safeguards in place, this model could be more protective of user privacy. Unfortunately, it may still allow the authority to learn the real identities of infected users. With more sophisticated safeguards, like cryptographic mixing, the system could offer slightly stronger privacy guarantees.

Some proposals go further, publishing the entire database publicly. For example, Apple and Google's proposal, published April 10, would broadcast a list of keys associated with infected individuals to nearby people with the app. This model places less trust in a central authority, but it creates new risks to users who share their infection status that must be mitigated or accepted.

Some apps require authorities, like health officials, to certify that an individual is infected before they may alert other app users. Other models could allow users to self-report infection status or symptoms, but those may result in significant numbers of false positives, which could undermine the usefulness of the app.

In short, while there is early promise in some of the ideas for engineering proximity tracking apps, there are many open questions.

Would Proximity Apps Be Effective?

Traditional contact tracing is fairly labor intensive, but can be quite detailed. Public health workers interview the person with the disease to learn about their movements and people with whom they have been in close contact. This may include interviews with family members and others who may know more details. The public health workers then contact these people to offer help and treatment as needed, and sometimes interview them to trace the chain of contacts further. It is difficult to do this at scale during a pandemic. In addition, human memory is fallible, so even the most detailed picture obtained through interviews may have significant gaps or mistakes.

Any proximity app contact tracing is not a substitute for public health workers' direct intervention. It is also doubtful that a proximity app could substantially help conduct COVID-19 contact tracing during a time like the present, when community transmission is so high that much of the general population is sheltering in place, and when there is not sufficient testing to track the virus. When there are so many undiagnosed infectious people in the population, a large portion of whom are asymptomatic, a proximity app will be unable to warn of most infection risks. Moreover, without rapid and widely available testing, even someone with symptoms cannot confirm to begin the notification process. And everyone is already being asked to avoid proximity to people outside their household.

However, such an app might be helpful with contact tracing in a time we hope is coming soon, when community transmission is low enough that the population can stop sheltering in place, and when there is sufficient testing to quickly and efficiently diagnose COVID-19 at scale.

Traditional contact tracing is only useful for contacts that the subject can identify. COVID-19 is exceptionally contagious and may be spread from person to person during even short encounters. A brief exchange between a grocery clerk and a customer, or between two passengers on public transportation, may be enough

for one individual to infect the other. Most people don't collect contact information for everyone they encounter, but apps can do so automatically. This might make them useful complements to traditional contact tracing.

But an app will treat the contact between two people passing on the sidewalk the same as the contact between roommates or romantic partners, though the latter carry much greater risks of transmission. Without testing an app in the real world—which entails privacy and security risks—we can't be sure that an app won't also log connections between people separated by walls or in two adjacent cars stopped at a light. Apps also don't take into account whether their users are wearing protective equipment, and may serially over-report exposure to users like hospital staff or grocery store workers, despite their extra precautions against infection. It is not clear how the technological constraints of Bluetooth proximity calculations will inform public health decisions to notify potentially infected individuals. Is it better for these applications to be slightly oversensitive and risk over-notifying individuals who may not have actually been standing within six feet of an infected user for the requisite amount of time? Or should the application have higher thresholds so that a notified user may have more confidence they were truly exposed?

Furthermore, these apps can only log contacts between two people who each have a phone on their person that is Bluetooth enabled and has the app installed. This highlights another necessary condition for a proximity app to be effective: its adoption by a sufficiently large number of people. The Apple and Google APIs attempt to address this problem by offering a common platform for health authorities and developers to build applications that offer common features and protections. These companies also aspire to build their own applications that will interoperate more directly and speed adoption. But even then, a sizable percentage of the world's population—including a good part of the population of the United States—may not have access to a smartphone running the latest version of iOS or Android. This highlights the need to continue to employ tried-and-true public health measures such as testing and traditional contact tracing, to ensure that already-marginalized populations are not missed.

We cannot solve a pandemic by coding the perfect app. Hard societal problems are not solved by magical technology, among other reasons because not everyone will have access to the necessary smartphones and infrastructure to make this work.

Finally, we should not excessively rely on the promise of an unproven app to make critical decisions, like deciding who should stop sheltering in place and when. Reliable applications of this sort typically go through many rounds of development and layers of testing and quality assurance, all of which takes time. And even then, new apps often have bugs. A faulty proximity tracing app could lead to false positives, false negatives, or maybe both.

Would Proximity Apps Do Too Much Harm to Our Freedoms?

Any proximity app creates new risks for technology users. A log of a user's proximity to other users could be used to show who they associate with and infer what they were doing. Fear of disclosure of such proximity information might chill users from participating in expressive activity in public places. Vulnerable groups are often disparately burdened by surveillance technology, and proximity tracking may be no different. And proximity data or medical diagnoses might be stolen by adversaries like foreign governments or identity thieves.

To be sure, some commonly used technologies create similar risks. Many track and report your location, from Fitbit to Pokemon Go. Just carrying a mobile phone brings the risk of tracking through cell tower triangulation. Stores try to mine customer foot traffic through Bluetooth. Many users are "opted in" to services like Google's location services, which keep a detailed log of everywhere they have gone. Facebook attempts to quantify associations between people through myriad signals, including using face recognition to extract data from photographs, linking accounts to contact data, and mining digital interactions. Even privacy-preserving services like Signal can expose associations through metadata.

So the proposed addition of proximity tracking to these other extant forms of tracking would not be an entirely new threat vector. But the potentially global scale of contact tracing APIs and apps, and their collection of sensitive health and associational information, presents new risks for more users.

Context matters, of course. We face an unprecedented pandemic. Tens of thousands of people have died, and hundreds of millions of people have been instructed to shelter in place. A vaccine is expected in 12 to 18 months. While this gives urgency to proximity app projects, we must also remember that this crisis will end,

but new tracking technologies tend to stick around. Thus proximity app developers must be sure they are developing a technology that will preserve the privacy and liberty we all cherish, so we do not sacrifice fundamental rights in an emergency. Providing sufficient safeguards will help mitigate this risk. Full transparency about how the apps and the APIs operate, including open source code, is necessary for people to understand, and give their informed consent to, the risks.

Does a Proximity App Have Sufficient Safeguards?

We urge app developers to provide, and users to require, the following necessary safeguards:

Consent

Informed, voluntary, and opt-in consent is the fundamental requirement for any application that tracks a user's interactions with others in the physical world. Moreover, people who choose to use the app and then learn they are ill must also have the choice of whether to share a log of their contacts. Governments must not require the use of any proximity application. Nor should there be informal pressure to use the app in exchange for access to government services. Similarly, private parties must not require the app's use in order to access physical spaces or obtain other benefits.

Individuals should also have the opportunity to turn off the proximity tracing app. Users who consent to some proximity tracking might not consent to other proximity tracking, for example, when they engage in particularly sensitive activities like visiting a medical provider, or engaging in political organizing. People can withhold this information from traditional contact tracing interviews with health workers, and digital contact tracing must not be more intrusive. People are more likely to turn on proximity apps in the first place (which may be good for public health) if they know they have the prerogative to turn it off and back on when they choose.

While it may be tempting to mandate use of a contact tracing app, the interference with personal autonomy is unacceptable. Public health requires trust between public health officials and the public, and fear of surveillance may cause individuals to avoid testing and treatment. This is a particularly acute concern in marginalized communities that have historical reasons to be wary of coerced participation in the name of

public health. While some governments may disregard the consent of their citizens, we urge developers not to work with such governments.

Minimization

Any proximity tracking application for contact tracing should collect the least possible information. This is probably just a record of two users being near each other, measured through Bluetooth signal strength plus device types, and a unique, rotating marker for the other person's phone. The application should *not* collect location information. Nor should it collect time stamp information, except maybe the date (if public health officials think this is important to contact tracing).

The system should retain the information for the least possible amount of time, which likely is measured in days and weeks and not months. Public health officials should define the increment of time for which proximity data might be relevant to contact tracing. All data that is no longer relevant must be automatically deleted.

Any central authority that maintains or publishes databases of anonymous identifiers must not collect or store metadata (like IP addresses) that may link anonymous identifiers to real people.

The application should collect information *solely* for the purpose of contact tracing. Furthermore, there should be hard barriers between (a) the proximity tracking app and (b) anything else an app maker is collecting, such as aggregate location data or individual health records.

Finally, to the greatest extent possible, information collected should reside on a user's own device, rather than on servers run by the application developer or a public health entity. This presents engineering challenges. But lists of devices with which the user has been in proximity should stay on the user's own device, so that checking whether a user has encountered someone who is infected happens locally.

Information security

An application running in the background on a phone and logging a user's proximity to other users presents considerable information security risks. As always, limiting the attack surface and the amount of information collected will lower these risks. Developers should open-source their code and subject it to third-party audits and penetration testing. They should also publish details about their security practices.

Further engineering may be necessary to ensure that adversaries cannot compromise a proximity tracing system's effectiveness or derive revealing information about the users of the application. This would include preventing individuals from falsely reporting infections as a form of trolling or denial of service, as well ensuring that well-resourced adversaries who monitor metadata cannot identify individuals using the app or log their connections with others.

"Anonymous" identifiers must not be linkable. Regularly rotating identifiers used by the phone is a start, but if an adversary can learn that multiple identifiers belong to the same user, it greatly increases the risk that they can tie that activity to a real person. As we understand Apple and Google's proposal, users who test positive are asked to upload keys that tie together all their identifiers for a 24-hour period. (We have asked Apple and Google for clarification.) This could allow trackers to collect rotating identifiers if they had access to a widespread network of bluetooth readers, then track the movements of infected users over time. This breaks the safeguards created by using rotating identifiers in the first place. For that reason, rotating identifiers must be uploaded to any central authority or database in a way that doesn't reveal the fact that many identifiers belong to the same person. This may require that the upload of a single user's tokens are batched with other user data or spread out over time.

Finally, governments might try to force tech developers to subvert the limits they set, such as changing the application to report contact lists to a central authority. Transparency will mitigate these risks, but they remain inherent in building and deploying such an application. This is one of the reasons we call on developers to draw clear lines about the uses of their products and to pledge to resist government efforts to meddle in the design, as we've seen companies like Apple do in the San Bernardino case.

Transparency

Entities that develop these apps must publish reports about what they are doing, how they are doing it, and why they are doing it. They must also publish open source code, as well as policies that address the above privacy and information security issues. These should include commitments to avoid other uses of information collected by the app and a pledge to avoid government interference to the extent allowed by law. Stated as application policy, this should also allow enforcement of violations through consumer protection laws.

Addressing Bias

As discussed above, contact tracing applications will leave out individuals without access to the latest technology. They will also favor those predisposed to count on technology companies and the government to address their needs. We must ensure that developers and the government do not directly or indirectly leave out marginalized groups by relying on these applications to the exclusion of other interventions.

On the other side, these apps may lead to many more false positives for certain kinds of users, such as workers in the health or service sectors. This is another reason that contact-tracing apps must not be used as a basis to exclude people from work, public gatherings, or government benefits.

Expiration

When the COVID-19 crisis ends, any application built to fight the disease should end as well. Defining the end of the crisis will be a difficult question, so developers should ensure that users can opt out at any point. They should also consider building time limits into their applications themselves, along with regular check-ins with the users as to whether they want to continue broadcasting. Furthermore, as major providers like Apple and Google throw their weight behind these applications, they should articulate the circumstances under which they will and will not build similar products in the future.

Technology has the power to amplify society's efforts to tackle complex problems, and this pandemic has already inspired many of the best and brightest. But we're also all too familiar with the ability of governments and private entities to deploy harmful tracking technologies. Above all, even as we fight

COVID-19, we must ensure that the word "crisis" does not become a magic talisman that can be invoked to build new and ever more clever means of limiting people's freedoms through surveillance.

RELATED UPDATES

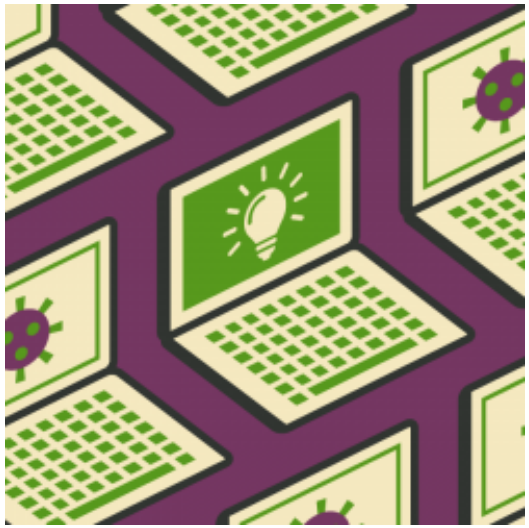
Copyright and Crisis: Filters Are Not the Answer

DEEPLINKS BLOG BY KATHARINE TRENDACOSTA, CORYNNE MCSHERRY | APRIL 21, 2020

DEEPLINKS BLOG BY JASON KELLEY | APRIL 20, 2020

ICYMI: Watch "At Home With EFF," A Virtual Discussion of COVID-19 and Digital Rights

Open Innovation in Medical Technology Will Save Lives



DEEPLINKS BLOG BY KIT WALSH, SOPHIA COPE, ELLIOT HARMON | APRIL 15, 2020

DEEPLINKS BLOG BY MATTHEW GUARIGLIA | APRIL 15, 2020

Telling Police Where People With COVID-19 Live Erodes Public Health

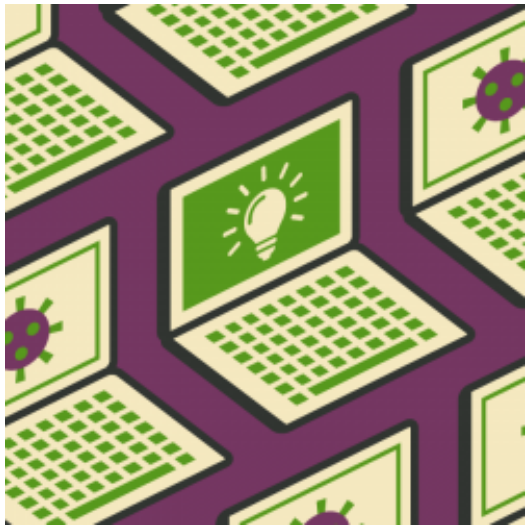
EFF Seeks Public Comment About Expanding and Improving Santa Clara Principles

PRESS RELEASE | APRIL 14, 2020

DEEPLINKS BLOG BY CORYNNE MCSHERRY, KATHARINE TRENDACOSTA | APRIL 10, 2020

Sharing Our Common Culture in Uncommon Times

Lengthening Patent Terms by 10 Years is Exactly the Wrong Response to COVID-19



DEEPLINKS BLOG BY JOE MULLIN | APRIL 8, 2020

DEEPLINKS BLOG BY MATTHEW GUARIGLIA, COOPER QUINTIN | APRIL 7, 2020

Thermal Imaging Cameras are Still Dangerous Dragnet Surveillance Cameras

How to Protect Privacy When Aggregating Location Data to Fight COVID-19

DEEPLINKS BLOG BY JACOB HOFFMAN-ANDREWS, ANDREW CROCKER | APRIL 6, 2020

DEEPLINKS BLOG BY ERNESTO FALCON | APRIL 6, 2020

California Legislator Introduces Fiber Broadband for All Bill