CoVista: A Unified View on Privacy Sensitive Mobile Contact Tracing

David Culler, Prabal Dutta, Gabe Fierro, Joseph E. Gonzalez, Nathan Pemberton,
Johann Schleier-Smith, K. Shankari, Alvin Wan, Thomas Zachariah
{culler, prabal, gt.fierro, jegonzal, nathanp}@berkeley.edu
{jssmith, shankari, alvinwan, tzachari}@berkeley.edu
UC Berkeley

Abstract

Governments around the world have become increasingly frustrated with tech giants dictating public health policy. The software created by Apple and Google enables individuals to track their own potential exposure through collated exposure notifications. However, the same software prohibits location tracking, denying key information needed by public health officials for robust contract tracing. This information is needed to treat and isolate COVID-19 positive people, identify transmission hotspots, and protect against continued spread of infection. In this article, we present two simple ideas: the ***lighthouse*** *and the* ***covid-commons*** *that address the needs of public health authorities while preserving the privacy-sensitive goals of the Apple and google exposure notification protocols.*

1 Introduction

Apple and Google have adopted a decentralized approach to mobile contact tracing that prioritizes individual privacy [1]. Under the Apple-Google Exposure Notification (AGEN) protocol (see Fig. 1), individual phones determine if the user has been exposed, without revealing *the identity of the infected individual* and *where the contact event took place* The AGEN protocol is related to contemporaneously proposed protocols including PACT and DP-3T [2, 3]. Like these other protocols, the AGEN protocol does not use location information. Instead, it relies on the Bluetooth radios present on all modern phones to detect proximity with others. Beyond not collecting Protected Health Information (PHI), the decentralized approach retains the non-PHI on the phone, allowing individuals to determine risk locally on their device.

Governments and public health authorities want to understand where and how the disease is spreading, so they can take preventative measures. They also want to be able to use mobile contact tracing to augment existing manual contact tracing efforts. With these goals in mind, governments advocate for a centralized approach, whether national or regional, where they maintain records of each person's locations and interactions. This allows governments to determine exposures and notify people directly, as timeliness reduces spread. While centralized contact tracing may offer utility critical to re-opening the world's economy, it raises profound concerns for civil

Bulletin of the IEEE Computer Society Technical Committee on Data Engineering

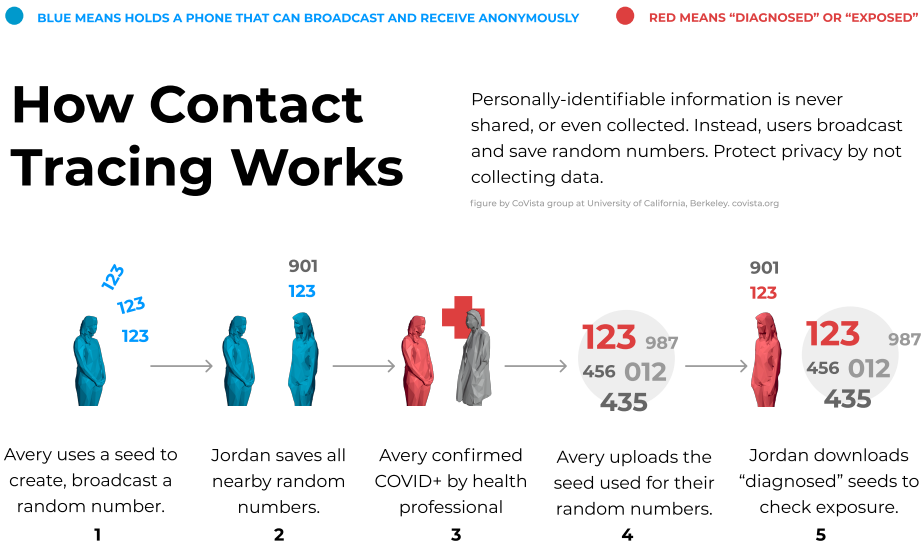

Figure 1: Apple-Google Exposure Notification (AGEN) Protocol Overview.

liberties and personal privacy. Government efforts that avoid reliance on the industrial Exposure Notification offerings have run into a host of failings, including reliability, power drain, interoperability, and participation.

Apple and Google have taken an unprecedented position – essentially dictating public policy, not just by requiring the decentralized approach, but also by prohibiting contact tracing apps from collecting location information. Further, they are restricting access to the new contact tracing APIs to national governments and permitting only one app per country or region. This decision circumvents the local governments, tribal organizations, and community health services that are often most aware of existing manual contact tracing efforts and the needs of their communities. Meanwhile, government contact tracing apps have failed due to restrictions imposed by AGEN.

In this article, we present two simple measures that enable the AGEN protocol to support manual contact tracing efforts, provide visibility into the spread of disease, and return authority to local communities all while preserving privacy within the Apple and Google framework.

1. **Treat places as people.** Endow public places with the same privacy-preserving technology used to monitor exposure for individuals.

2. **Nation-scale data, not apps and processes.** Build a common backend for the AGEN protocol that spans apps and governmental boundaries.

In the rest of this article, we describe these two simple measures and how they both improve contact tracing while also preserving individual privacy.

Lighthouse: Treat Places as People

If we treat public places as people, we can use the AGEN protocol to (a) understand COVID-19 exposures across space, (b) integrate with manual contact tracing, and (c) do so with the same privacy-sensitive protocol. To treat places as people in AGEN, simply attach mobile phones or specialized low-cost beacons to publicly accessible places (e.g., county services, stores, buses). Like a lighthouse, these devices help communicate risk associated with places. Well-positioned, they can offer robust proximity detection, can detect their exposure, and can convey aspects the risk that represents.

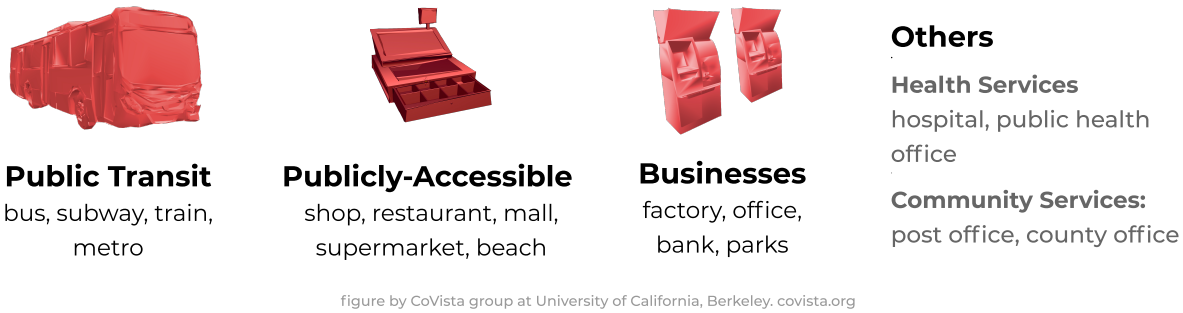

Figure 2: Lighthouses can extend the AGEN protocol to physical places

By choosing to share their locally computed exposure risk with public health authorities through the AGEN protocol, owners of publicly-accessible places can aid in mitigating virus spread. Alternatively, if a place is identified through traditional, manual contact tracing, the place can still anonymously participate in the AGEN protocol, notifying others without revealing where they were exposed. Treating places as people empowers stewards of public spaces to collaborate with public health authorities to help mitigate the spread of disease without jeopardizing the privacy of patrons or the reputation of the public spaces. This procedure can facilitate detection of exposure from a non-participating individual while improving anonymity over manual contact tracing methods. Going even further, such places could provide other means of beaconing that do not involve smartphones, such as QR code displays, codes on receipts and so on.

COVID Commons: A Nation-scale Data Backend

Rather than "one app per nation," a better solution would be to provide a common privacy-preserving data exchange across apps and administrative boundaries — a Commons. This would allow societal structures and innovation, rather than corporate policy, to determine how the app ecosystem should evolve. It is very likely that participation will be greatest if the apps are available through local organizations (e.g., tribal organization, university campus) that individuals trust. A common privacy-preserving data exchange is already compatible with the AGEN protocol.

When an individual tests positive and they engage in a conventional contact tracing interview with a public health professional. The professional obtains an authorization so the individual, on an opt-in basis, can share their anonymous exposure information. Public health professionals serve to protect the integrity of the information in the Commons without exposing any patient data or medical data.

Their actions are quite similar to publishing counts of cases, statistics and demographic information, as is done today. The Commons might be hosted by governmental or NGO structures, based on national or regional policy. A diverse and innovative app ecosystem can grow to meet the needs of individuals and agencies.

In the remainder of this article we describe both these technical solutions in greater detail. We have organized each section to be relatively self-contained.

2 Background on Privacy-Sensitive Mobile Contact Tracing

The key building block for Privacy-Sensitive Mobile Contact Tracing (PS-MCT) is a subtle combination of radio protocols, cryptography, and risk-calculation. Phones have a short-range radio, Bluetooth, used to connect to nearby devices. To make those connections it periodically broadcasts tiny bits of information. The PS-MCT protocols leverages this short-range background broadcast to resolve nearby individuals.

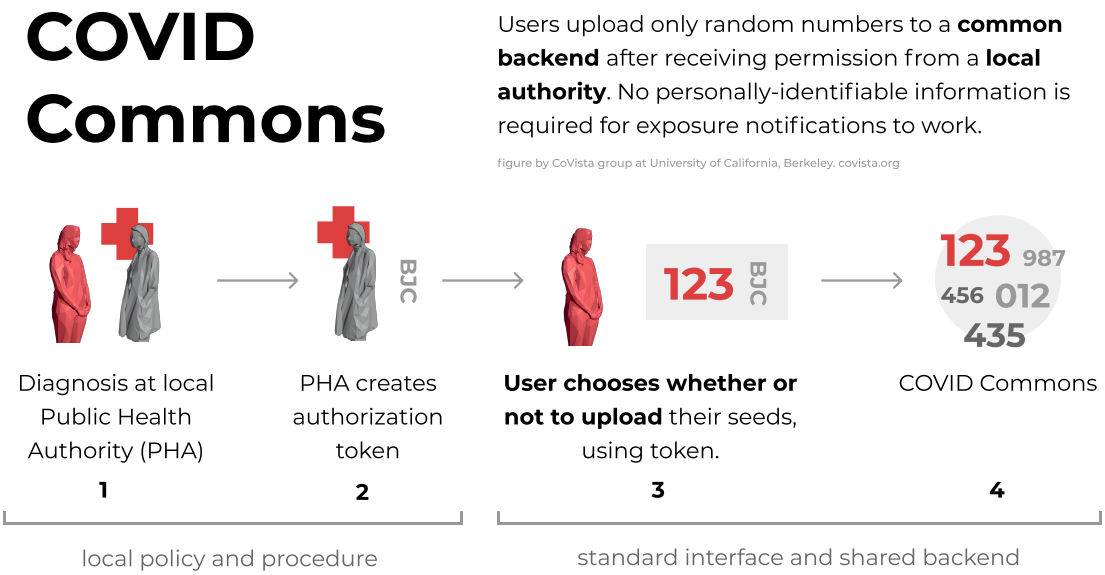

Figure 3: Covid Commons exposure notification process.

In the Apple-Google Exposure Notification (AGEN) protocol, each phone generates a daily secret key called a Temporary Exposure Key (TEK). Then every 15 minutes the phone uses the TEK to generate a new 16 byte Rolling Proximity Identifier (RPI). The RPI sequence is generated using a cryptographic hash function, so it does not carry any information about the source individual. The current RPI is then continuously broadcast every few hundred milliseconds. All phones log the RPIs they hear for future exposure analysis. Because the RPI is continuously changing, it also cannot be easily tracked.

When someone tests positive they can **anonymously** publish the daily keys (TEKs) from the days when they were contagious. The confirmed positive collection of TEKs is called a Diagnosis Key in the AGEN protocol. The Diagnois Keys are published by sharing them with a trusted server which publishes the TEKs for download. Others can obtain these keys and use the same cryptographic hash functions to recreate the sequence of RPIs. This sequence, combined with some region-specific weights, can determine if they encountered any infected individuals. This entire process is accomplished within the Android and iOS operating systems. Government sanctioned apps are only responsible for authenticating infected individuals and, with user permission, publishing the keys.

It is important to note the distinction between policy and mechanism. The AGEN protocol (and the extensions proposed in this paper) provide a mechanism to detect and notify users about exposure risk, but it is up to public health authorities to define what constitutes an exposure. This distinction is explored in more detail in section 4.

3 Lighthouses: Treating Places as People

Despite their promise, there remains significant concern around the efficacy of privacy-preserving contact tracing and exposure notification protocols. For one thing, not everyone has access to a mobile phone, and many that do may be unwilling to participate (even Singapore only achieved 20% adoption[4]). This is a serious concern as the probability of a successful detection grows quadratically with participation [2]. Of course, manual contact tracing does not have this issue and remains the gold standard. Will these two techniques exist in isolation or will they interact synergistically? Finally, bluetooth contact detection is limited in range and time; it cannot detect many

important forms of transmission like surfaces or HVAC systems[5].

3.1 Treating Places as People

There is a simple extension to mobile contact tracing that can help address these issues. The idea is rooted in centuries old maritime signaling. To navigate at night, ships use signal lights, much like our Bluetooth beacons, to identify and safely navigate around nearby ships. However, to safely sail at night, ships also rely on lighthouses, strategically placed beacons, to identify and safely navigate around key landmarks. It is this second form of beacon, the lighthouse, that is needed to address several of the key limitations in privacy-sensitive mobile contact tracing.

3.2 What is an Exposure Notification Lighthouse?

A privacy-sensitive exposure notification lighthouse is a device (e.g., a mobile phone or even a smart sticker) deployed in a public space following the same privacy sensitive mechanisms as individuals. Figure 4 gives a few examples of what lighthouses could look like. Much like the maritime lighthouse, contact tracing lighthouses can be used to inform others of potential exposures associated with public spaces discovered through manual contact tracing. A contact tracing lighthouse can also log passing beacons to inform owners and public health authorities of exposure risks. However, because the lighthouse follows the same privacy-sensitive protocols as individuals, it retains all of the privacy guarantees of the existing protocols. Moreover, by installing contact tracing lighthouses in participating public spaces ranging from stores and restaurants to schools and buses, we introduce a privacy sensitive mechanism to bridge manual contact tracing with mobile contact tracing. Such a bridge gives public health authorities the ability to gain visibility into the spread of disease while preserving individual privacy.

(a) **Existing Devices:** Easily deployed immediately but expensive to deploy to new places. They can also be unreliable when unattended.

wikimedia commons © Travelarz CC-ASA 3.0

(b) **Dedicated Devices:** Cheap and reliable. They will require new development and can be tricky to place correctly.

(c) **No Device:** Allows those without the app or even a mobile device to participate. They may be easier to re-identify and require manual effort from users to check.

Figure 4: Lighthouses can be deployed using a number of different devices with varying trade-offs. Each of these examples is feasible to deploy in the near future.

3.3 What Do We Get From Lighthouses?

Figure 5 walks through an example of how lighthouses could work in a typical case. Let's explore some of these benefits in more detail.

3.3.1 Bridging Place and Mobile

The contact tracing lighthouse empowers stewards of public spaces (e.g., shop owners, school administrators) to collaborate with public health authorities to help mitigate the spread of disease without jeopardizing the privacy of patrons or the reputation of the public spaces. When an individual is tested and confirmed, the manual contact tracing interview process begins. One of the first questions asked is "Can you recall where you have been that might have exposed others?". A place, unlike an individual, has a large set of explicit relationships with its institutional environment - business license, health department approvals, chamber of commerce, etc. The interview process routinely seeks to gather information about places. But often there is little the place can do to help. With its lighthouse, it has a very simple way to provide assistance without undue impact on its reputation. Just like a person, it can check its own potential exposures. And, like a person, it can anonymously publish its own random numbers as COVID positive so that people can use them for detecting their exposure risk. This is especially useful if the individual who tested positive was not using an app that broadcasts their own sequence of random numbers. Unlike a person's phone, stationary lighthouses can be carefully positioned to avoid issues like weak or unreliable broadcast that mobile phones can face. Finally, the public place may also take other measures in assisting its local health authority in detecting hot spots, such as informing them of the exposure risk that it observes.

3.3.2 Indirect Transmission

The lighthouse can be used to address forms of indirect transmission that are not captured in the existing privacy-sensitive mobile contact tracing efforts. If a COVID-positive individual enters a bus and touches or sneezes on several surfaces they could potentially infect others over the next several hours, long after they have left the bus. Air conditioning systems have also been implicated in spreading the virus over large distances [5]. Existing wireless protocols will fail to capture these forms of transmission since they rely on close, contemporaneous radio proximity with the positive individual. However, with the introduction of the lighthouse, the bus or restaurant can automatically determine that it was exposed and choose to anonymously publish its own random number sequence.

3.3.3 Beyond Mobile Contact Tracing

Finally, the lighthouse can also extend the privacy-sensitive mobile contact tracing protocol beyond the smartphone. Places provide channels of communication to individuals that complement smartphones. Simple lighthouse codes might be included on printed receipts or handed to customers. A person without contact tracing on their phone might use such code to manually perform the exposure checks that are automated by the apps. For example, they could enter such codes that they have received into a public website to determine their exposure risk.

3.4 Lighthouse Privacy

There are legitimate privacy interests for places, as there are for people. Businesses may fear irrational boycotts or loss of reputation, and there are risks of perpetuating prejudice or stigma against neighborhoods or ethnic groups (already a growing problem [6]). The good news is that lighthouses inherit the privacy protecting characteristics of the AGEN protocol. In their simplest form, they are phones running ordinary apps, different only because they live in a fixed place rather than in purse or pocket.

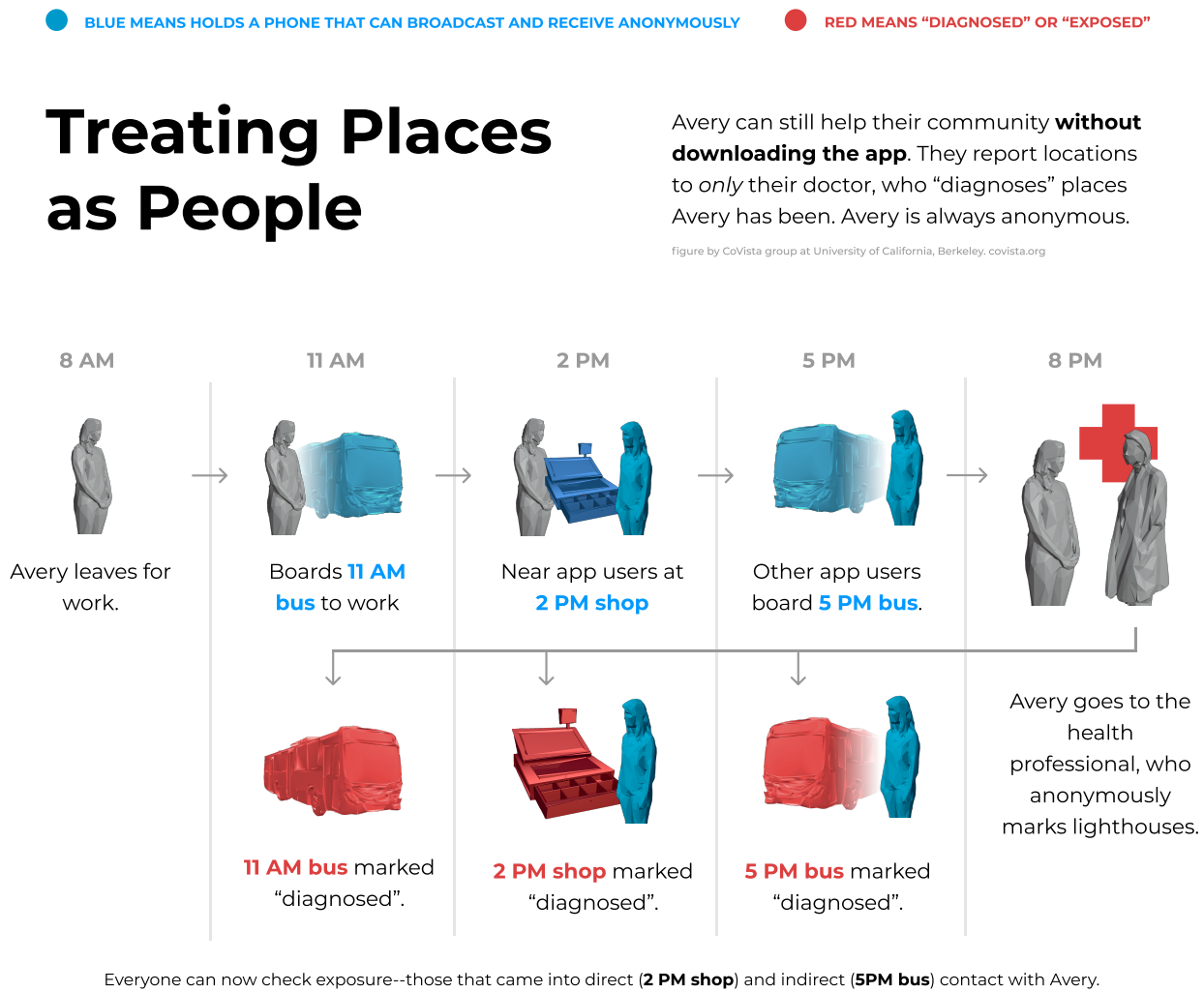

Figure 5: An example scenario of an affected individual (Avery) and a stranger (Bernie) that may have been exposed. Even if Avery is not an app user, the doctor can still notify the shop and bus of their exposure; lighthouses **connect manual and mobile contact tracing**. Lighthouses **bridge place and mobile** by allowing the bus and shop to notice their exposure and mark themselves as exposed, even if Avery did not remember visiting them. They also **enabled less direct forms of exposure** by notifying Bernie of their potential exposure, even though they were not on the bus at the same time as Avery. Finally, lighthouses offer places benefits **beyond the standard mobile contact tracing**. They can now track how often they are exposed, at what times, and even in which section within them (if they have multiple lighthouses installed).

Lighthouses can complement manual contact tracing by offering greater confidentiality in situations where people cross paths in stigmatized locations. For example, investigators following up on a recent case cluster associated with nightclubs in Korea catering to the LGBTQ community have struggled to contact attendees who are afraid of being "outed" or facing discrimination [7]. Lighthouses can fill such gaps without requiring or relying on anyone, even an affected person, to disclose their location history.

A potential concern about lighthouses is that internal state, if combined and aggregated, could be used to undermine some of the privacy guarantees of AGEN. Indeed, with a sufficiently large deployment of lighthouses and centralized collection of recieved RPIs, it would be possible to resolve the locations of all the COVID positive individuals. We therefore stress that each lighthouse must follow the existing decentralized protocol for risk assessment in which only risk is aggregated and not the underlying RPIs.

To address some of these security concerns, it is possible to deploy **transmit only** (passive) lighthouses which could be used to anonymously notify others of exposure without listening for RPIs. This eliminates the risk of resolving COVID positive individuals locations but also limits visibility into where the disease is spreading.

4 Covid Commons: Unified Contact Tracing With Many Apps

Standardizing on an exposure notification protocol such as AGEN is crucial to achieving the critical mass of participation required to make such an approach effective (estimated to be at least 80% for a city of 1 million individuals [8]) and privacy preserving. Apple and Google, as producers of the two dominant smartphone OSes, are uniquely positioned to bring these capabilities to nearly every smartphone and have engineered the AGEN protocol to that end. Providing an implementation of the protocol through an OS upgrade would eliminate the fragmentation of the protocol preventing sufficient adoption. However, standardizing the proximity detection protocol is just part of the solution.

Due to concerns over potential misuse of the capabilities of the proximity detection protocol and location tracking features of modern smartphones, Apple and Google have announced that access to the SDK for AGEN to "public health agencies" [9]. The realization of this policy has evolved to essentially mean "one app per state." Centralizing the apps around state governments means that tracing efforts are not limited to local jurisdictional boundaries. However, the public health authorities responsible for testing and tracing often operate at a more local level [10, 11].

The fundamental issue with this policy is a failure to distinguish between ownership of the required repository of "diagnosis keys" and the applications that produce and utilize them. The repository contains keys that correspond to times when diagnosed individuals may have interacted with others and must therefore be public-facing so that individuals, via AGEN-compatible apps, can download the keys and determine their own exposure risk. The keys uploaded to the repository must be limited to those that have been authorized by a public health authority through some testing and interview process. In the U.S., public health measures such as contact tracing and case reporting are carried out at a county or city level through individually executed processes, in coordination with state and national law and policy. However, health authorities do not generally have the technical, human or financial resources to produce the required app and also stand up and maintain such a public-facing data service. This is even less tenable during a pandemic, when such resources are already strained. Who, then, manages the AGEN backend needed to share Report Keys?

The worst-case scenario is for the repositories to emerge as fragmented silos of diagnosis keys. In the midst of the custody battle over administration of the emerging technical approaches to the contact tracing problem, it is important to remember that exposure does not respect administrative boundaries. Regardless of how the repository is established, it is essential that exposure notification can be transmitted across backends and across apps. Indeed, there are already efforts to combine contact tracing efforts and data across the administrative boundaries established by industry's policy around AGEN [12].

4.1 A Path to Nation-scale Data

A solution to this issue is the creation of a privacy-preserving data exchange shared and accessible across apps and administrative boundaries — a Commons. Different public health authorities could cooperatively contribute to the Commons and individuals across many jurisdictions would access it through their apps. Such a Commons might operate at the scale of one per nation, or it might be regional with some form of federation to share keys and exposure information across individual instances. The Commons may be hosted and maintained by governmental authorities, foundations or other appropriate institutional entities.

The Commons requires no change to the EN protocols. Each individual participates in the proximity detection using daily TEKs and the RPIs generated from them without change. With no other information leaving the phone, the app on an indivual phone downloads the diagnosis keys and presents them to the SDK to obtain exposure risk scores. The difference is that those diagnosis keys are not *a priori* limited to the ones produced by users of the same app. Just as in the current decentralized protocol, an individual who tests positive — i.e. a confirmed case — and participates in contact tracing with a specific public health authority is asked to voluntarily submit their TEKs for the past period over which they are likely to have been contagious. The AGEN protocol does not stipulate how that request is formulated or how that submission is performed, but the introduction of the Commons allows us to answer that question precisely.

4.2 The PHA Experience: Federating Access to the Commons

A Commons is utilized by a well-defined set of public health authorities that are registered with it. Professionals at PHAs can authenticate to and access the Commons using well-established authentication techniques such as LDAP and OAuth. As part of requesting a patient to submit their diagnosis keys to the Commons, the professional requests a one-time authorization (OTA) from the Commons. The OTA authorizes the upload of TEKs corresponding to the extent of time during which the patient is likely to have been contagious; this will involve some days prior to the diagnosis and extend to several days or weeks following. The OTA is provided to the patient to authorize the submission of their keys to the Commons; the upload is opt-in, as under the usual AGEN protocol.

Because the OTA corresponds to a single interaction between a healthcare professional and a patient, it is a natural key on which helpful metadata can be associated. The authorizing PHA may want their identity to be associated with the submitted diagnosis keys so that the provenance of the diagnosis is preserved. This identity, realized by the TLS public key of the PHA, can be associated with generated OTAs in the Commons. This provides no more information than having each PHA host their own exposure key store, as currently envisioned. As we will discuss below, the PHA identity can also be used to filter which diagnosis keys are considered in the matching process on an individual's phone.

The OTA itself is also a useful piece of metadata when associated with the uploaded keys in the Commons. The authorizing professional will likely want to be able to determine whether the patient has in fact contributed their keys as requested to determine if follow-up is necessary. Associating the OTA with the uploaded keys places no new information in the Commons: the professional knows what they know about those they interview and they know what authorizations they have requested. Each such confirmed case can be expected to have generated some authorization request, but that information, along with all other aspects of the contact tracing process, is under the purview of the PHA. Counts of confirmed cases and other aggregate information are already regularly reported to the public.

The Commons is able to provide this functionality despite no patient data — indeed, no health or medical data of any kind — ever being entered into the Commons. The Commons also takes no position on which parts of the contact tracing process are automated and which are manual. It integrates cleanly with the existing processes established by PHAs for interviewing patients, deciding which diagnosis keys are appropiate to share, and so on. The Commons merely provides a means of carrying out the result of these decisions in a way that does not

require individuals to be using the same phone app.

4.3 The User Experience: Federating Downloads from the Commons

The current draft of the AGEN protocol says very little about how exposure notification information will be transmitted or relayed among the different instances of the diagnosis key repository. A unified Commons immediately addresses this issue — all diagnosis keys are uploaded and downloaded from the shared repository. However, under a federated regime, it is necessary to address how exposure notification and uploaded keys can be routed across instances of the Commons.

Consider a scenario where an individual is diagnosed by one PHA but may travel or may have traveled to regions covered by different PHAs. Individuals in those other regions should be able to obtain the TEKs for the diagnosed individual, even though the diagnosis was performed by a remote PHA. There are two complementary approaches.

The first approach proactively forwards diagnosis keys to relevant PHAs. A PHA professional can "tag" a requested OTA with public keys or other metadata identifying relevant remote PHAs, using information acquired as part of the interaction with the individual. The process of uploading diagnosis keys authorized by that OTA to the Commons can then incorporate a simple forwarding mechanism that replicates those keys to the federated instances of the Commons managed by those other PHAs. This can be performed by the Commons itself, or it may be performed on an opt-in basis by the individual.

Under the second approach, individuals may proactively request diagnosis key downloads from federated instances of the Commons they are interested in. An individual may subscribe to diagnosis key downloads for Commons covering regions the individual has travelled to or will travel to. Additionally, an individual may subscribe to Commons for surrounding regions.

Regardless of whether the Commons is realized as an administratively centralized server or a federated mesh, the Commons must provide some mechanism for filtering or scoping the download of diagnosis keys onto an individual's device. The number of keys downloaded from the Commons will grow with the adoption of AGEN-based apps, improvements in testing, and the spread of COVID-19. Without the ability to filter the set of keys down to a reasonable and relevant set that is still large enough to maintain the privacy-preserving properties of AGEN, the bandwidth requirements and compute requirements (for deriving the thousands of RPIs used for the matching process) may grow to be untenable.

4.4 Extending the Commons

Once this basic separation of key repository has been established, along with the method for authorizing submissions and routing them to queries, it becomes possible to meaningfully entertain the question of including earlier stages. Especially with testing being scarce, confirmation occurs late and involves the contact tracing processes of public health authorities. Prior to that stage, we have Probable Covid (where a diagnosis has been performed based on defined symptom criteria), preceded by Suspected Covid, and often preceded by individual state of concern. Associated with each stage is a process, an (increasingly large) set of principals who might authorize a submission, and a reduced significance in conveying exposure. For example, the physician or health service making a Probable Covid diagnosis (and typically also authorizing testing) would be the natural principal to authorize the individual to submit "Probable Keys". The privacy-sensitive protocol could access these, as well as the "Confirmed Keys" referred to as Diagnosis Keys in the EN protocol. The protocol permits the distinction to be reflected in metadata carried along with the keys. Thus they might factor in, perhaps with lesser weight, into the risk score.

5 Conclusion

With these two simple innovations, we can move past the conflicts and controversy and on to utilizing privacy-sensitive mobile contact tracing to improve the efficacy of public health measures - thereby saving lives and unnecessary suffering - while respecting civil liberty. The companies should provide the interoperable building blocks without themselves getting into the business of providing the Apps or holding the data. They can maintain their privacy-first, decentralization posture, but should advocate for an interoperable COVID key Commons, rather than dictating policy on the app ecosystem. Government actors can regain policy determination and influence the app ecosystem so as to best tailor offerings to their constituents. The tailoring could include questions around how best to provide a Commons of appropriate scale, and utilize physical measures to relate anonymous key reports to the places within their jurisdiction. Government actors already have extensive experience with civic infrastructure such as security cameras, traffic signals and health inspections. They can apply the similar principles towards recognizing the importance of public awareness, potential for creating stigma, and bringing benefit to non-participating members of the communities. The technology can assist the contact tracing process, but should not be dictating it or replacing the human relationship of the patient and the health professionals performing interviews and care. The trust that is built there is what makes opt-in approaches viable, and only with appropriate individual protections.

References

[1] A. Inc., *"Apple and Google partner on COVID-19 contact tracing technology"*, 10 April 2020 (accessed 25 May 2020). [Online]. Available: https://web.archive.org/web/20200410171128/https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/

[2] J. Chan, D. Foster, S. Gollakota, E. Horvitz, J. Jaeger, S. Kakade, T. Kohno, J. Langford, J. Larson, P. Sharma, S. Singanamalla, J. Sunshine, and S. Tessaro, "Pact: Privacy sensitive protocols and mechanisms for mobile contact tracing," 2020.

[3] C. e. a. Troncoso, *Decentralized Privacy-Preserving Proximity Tracing*. [Online]. Available: https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf

[4] *20 April 2020 - One Month On*, 20 April 2020 (Accessed 24 May 2020). [Online]. Available: https://web.archive.org/web/20200524045214/https://support.tracetogether.gov.sg/hc/en-sg/articles/360046475654-20-April-2020-One-Month-On

[5] J. Lu, J. Gu, K. Li, C. Xu, W. Su, and Z. e. a. Lai, "Covid-19 outbreak associated with air conditioning in restaurant, guangzhou, china, 2020," *Emerging Infectious Disease*, 2020, https://doi.org/10.3201/eid2607.200764.

[6] E. Y.-J. Kang, *Asian Americans Feel The Bite Of Prejudice During The COVID-19 Pandemic*, National Public Radio, 31 March 2020 (Accessed 2 April 2020). [Online]. Available: https://web.archive.org/web/20200402203217/https://www.npr.org/local/309/2020/03/31/824397216/asian-americans-feel-the-bite-of-prejudice-during-the-c-o-v-i-d-19-pandemic

[7] H. Shin and J. Smith, "South korea scrambles to contain nightclub coronavirus outbreak," *Reuters*, 2020. [Online]. Available: https://www.reuters.com/article/us-health-coronavirus-southkorea/south-korea-scrambles-to-contain-nightclub-coronavirus-outbreak-idUSKBN22N0DA

[8] R. Hinch, W. Probert, A. Nurtay, M. Kendall, C. Wymant, M. Hall, and C. Fraser, "Effective configurations of a digital contact tracing app: A report to nhsx," 2020. [Online]. Available: https://github.com/BDI-pathogens/covid-19_instant_tracing/blob/master/Report-EffectiveConfigurationsofaDigitalContactTracingApp.pdf

[9] *Exposure Notification API launches to support public health agencies*, Apple Incorporated, Google LLC, 20 May 2020 (Accessed 24 May 2020). [Online]. Available: http://web.archive.org/web/20200524152945/https://blog.google/inside-google/company-announcements/apple-google-exposure-notification-api-launches/

[10] C. Ho, "Bay area coronavirus tests: Where can i get one?" 21 May 2020 (Accessed 25 May 2020). [Online]. Available: http://web.archive.org/web/20200525201614/https://www.sfchronicle.com/health/article/Where-can-I-get-a-coronavirus-test-in-the-Bay-15136054.php

[11] N. A. of County and C. H. Officials, "Directory of local health departments," 24 May 2020 (Accessed 24 May 2020). [Online]. Available: http://web.archive.org/web/20200524090932/https://www.naccho.org/membership/lhd-directory

[12] N. N. York, "What you need to know about New York's 'monumental' contact tracing program," 22 April 2020 (Accessed 24 May 2020). [Online]. Available: http://web.archive.org/web/20200524162632/https://www.nbcnewyork.com/news/coronavirus/what-you-need-to-know-about-new-yorks-monumental-contact-tracing-program/2385611/