COUNTY OF SANTA CLARA
PRIVACY OFFICE
sccgov.org/sites/cpo

2460 North First Street | San Jose, California 95131

MEMORANDUM

DATE:	**May 25, 2021**
TO:	**Santa Clara County Health and Hospital Committee**
FROM:	**Privacy Office**
SUBJECT:	**Report back to Board of Supervisors on Data Privacy Day Event**

Table of Contents

Introduction

As the COVID-19 pandemic expanded across the globe, public health experts agreed that a three-pronged approach of protocols and procedures would be the most effective way, to augment a vaccination strategy, in an effort to contain disease transmission: isolation (including masking and social distancing), testing, and contact tracing. These protocols, along with secondary efforts such as basic hygiene improvements, have been well-understood and implemented in previous pandemics in one form or another for decades or even centuries.

However, recent developments in technology, coupled with the dramatic expansion of data intake and analysis capabilities available to both public and private entities, have the potential to fundamentally alter the nature of contact tracing, especially in future pandemic response which is a key focus of this report. Governments and the private sector have access to more data than ever before, and technological innovations have, almost overnight, created new contact tracing technologies mediated by the devices many people carry around every day. These methods are often based on geographic locations and/or proximity to other devices.

These approaches, which can assist traditional contact tracing efforts, can also reveal a much more detailed picture of individuals' lives. Thus, for all the promise of new contact tracing technologies to track the spread of a disease more accurately than ever before, there are also significant concerns when it comes to individual privacy, civil rights, and civil liberties.

To discuss the tradeoffs inherent in new contact tracing technologies, the County of Santa Clara's (County) Privacy Office, in cooperation with the Office of County Supervisor Joe Simitian (District 5), hosted its third annual Data Privacy Day event on January 28, 2021, with the theme of *Modern Contact Tracing for Future Pandemics: Balancing Utility and Privacy*. The event featured two separate panels of experts discussing the following topics, which will be highlighted as part of this report:

- Panel 1: Contact Tracing Fundamentals and New Technology; and
- Panel 2: Privacy Impacts of Modern Contact Tracing for Future Pandemic Response.

Panel 1: Contact Tracing Fundamentals and New Technology

Traditional Contact Tracing

In the first panel, participants laid the groundwork for understanding how contact tracing works and the role that technology can play. The County of Santa Clara ("County") Assistant Public Health Officer Dr. Sarah Rudman explained that contact tracing is the process of identifying, notifying, and monitoring anyone who came in close contact with an individual who has tested positive for an infectious disease. Contact tracing has historical roots dating back to the beginning of public health efforts. It allows public health officials to look backward to understand why someone is getting sick, as well as to look forward, determining who a sick person might have exposed. It may also be used to understand patterns of infection in an effort to understand viral movement among populations, factors that may have contributed to that movement, and to consider those trends to mitigate future viral migration.

Contact tracing involves a complex interaction of different stakeholders and procedures. In "traditional" or "manual" contact tracing, labs conducting tests on individuals, and clinicians diagnosing patients, provide results to a trusted, centralized authority (usually a government entity) with the means to safely manage sensitive health information. The centralized authority then releases contact information to local public health departments for individuals falling within a particular health department's jurisdiction. A local public health department can then reach out to those individuals to promote responsible behavior and obtain information about the individual's recent locations and close contacts, so those individuals can be informed regarding possible exposure, testing options, and next steps.

Although referred to as "traditional," this type of contact tracing does involve many forms of technology. For example, the rise of computers allows for test results and contact information to be tracked in a database rather than on paper, and telephone technology allows for contact to be made by phone and even text messages rather than in more labor-intensive ways. Nevertheless, the fundamentals remain the same as the earliest iterations of the process: individuals who tested positive are contacted and asked to provide locations they have visited during a prior defined period of time (e.g., previous 14 days, or potential viral transmission window) as well as the names of people they have been in close contact with during that time. In providing this information, individuals typically rely on their own memories and diverse methods of recordkeeping, such as looking back at calendars, to piece together where they have been and who they have been around.

For contact tracing to work, trust is essential. Public health departments go to great lengths to build and maintain trust within the communities they serve. For example, County Public Health Department (PHD) staff engage in a conversation with individuals they contact to help them understand why providing the PHD with information the individual may consider private is important from a personal, family, and community perspective. Among other techniques, the PHD contacts individuals using a standard phone number, provides verification that the call is coming from the PHD, and provides the individual with resources they can use to keep their families, friends, co-workers, and neighbors safe. Additionally, the PHD follows standard privacy practices such as collecting only information that is necessary to fulfill the purpose of contact tracing and keeping information confidential in accordance with the law.

Dr. Rudman explained that traditional contact tracing in the COVID-19 context is challenging for several reasons. First, COVID-19 infections move relatively quickly, yet contact tracing works best when a disease moves slowly offering time to respond. Second, contact tracing is more effective when individuals are able to identify with certainty where they have been and who they have been in close contact with over a defined period of time. A predominantly airborne disease such as COVID-19 makes identifying close contacts difficult, because they might include all members of a gathering an individual attended. Third, as in many other instances, underserved populations can also be underserved by contact tracing if measures are not in place to address specific challenges for outreach and other needs. Finally, contact tracing is only one prong of the overall COVID-19 response. If safe ways of quarantining are not available or if a jurisdiction has no testing capacity, individuals' efforts to respond after being contacted by public health authorities can be hampered.

One panelist addressed how these challenges were being met in San Francisco, noting that around 70% of individuals contacted were answering their phones, and response times had been cut from a five-day average to within 24 hours. Additionally, by virtue of mobilizing a workforce that is diverse and multi-lingual, such as those proficient in Spanish, San Francisco has been successful in reaching about 80% of Latin/Hispanic underserved populations. From that point, around 50-60% of those informed through contact tracing that they may have been exposed are able to get a test. While public health authorities do strive to improve outcomes, this demonstrates that traditional contact tracing can respond to the unique challenges posed by a virus such as COVID-19.

New Methods of Contact Tracing

New methods of contact tracing are also being developed. The variety of available technology makes classification difficult, but researchers at Johns Hopkins University have suggested a spectrum consisting of, "maximal" approaches involving centralized data collection, "minimal" approaches using "decentralized privacy-protecting proximity

tracking," "and a diverse middle ground that aims to augment manual contact tracing with the collection of digital data."[1]

Portable, network connected devices (hereinafter "mobile devices"), such as cellular phones, represent one category of a potentially paradigm-shifting capability for contact tracing. Two main reasons can account for this. First, mobile devices typically allow for location information to be tracked more completely and precisely. As noted above, location plays a key role in contact tracing, and traditional methods generally rely on individuals' memories of where they have been within a prior relevant period of time. Mobile devices, on the other hand, are almost always on, and are almost always tracking location in some way and doing so on a frequent basis even in the background while a person is not actively using the device. Accessing this information can provide contact tracers with a more precise record of an individual's whereabouts. When information from the devices of many individuals is combined, it can reveal whether those devices were in close proximity and thus whether individuals were exposed to someone who was infected.

Second, mobile devices are nearly ubiquitous in American society. According to the Pew Research Center, "the vast majority of Americans – 96% – now own a cellphone of some kind. The share of Americans that own smartphones is now 81%."[2] The sheer number of mobile devices with location tracking capabilities means that information gaps can be reduced and more precise conclusions about where people have been and who they have been around, in cases where they may even visit a public location or store and not know those who they passed by, can now be drawn leveraging such technologies.

Exposure Notification Apps

There are a variety of different methods to use location information provided by mobile devices in the context of contact tracing. At the minimal end of the spectrum, "proximity tracing and exposure notification" apps typically rely on the Bluetooth signals of mobile devices to record close contact between users. In general, these designs store information on mobile devices in an anonymized form that prevents direct re-identification of users and notifies them of potential exposure to someone who has tested positive for COVID-19. A report published by the Johns Hopkins University Press states,

> *If a user with a[n exposure notification] app installed on their phone tests positive and enters test results into their app, those who have been identified as having been in close proximity to them can be notified by the app. This notification can be*

[1] Kahn, Jeffrey and Johns Hopkins Project on Ethics and Governance of Digital Contact Tracing Technologies. Digital Contact Tracing for Pandemic Response: Ethics and Governance Guidance. Johns Hopkins University Press, 2020.

[2] Pew Research Center, Mobile Fact Sheet, June 12, 2019, available at https://www.pewresearch.org/internet/fact-sheet/mobile/.

automatic or at the discretion of the person who is [positive for COVID-19], depending on the app design. If notified, a user who has been in contact with a [COVID-19 positive] individual would receive a push notification alerting them to possible exposure (which may be timestamped), but with no other identifying information.[3]

One prominent example of the exposure notification approach is the application programming interface (API) built through a partnership between Google and Apple (Google/Apple API). The Google/Apple API creates random IDs for each device every 10-20 minutes, which contain no location or personal information. Each device periodically cross checks all of the random IDs associated with a COVID-19 positive case against its own list of IDs to look for a match. When a match is detected, the app sends a notification to the exposed individual and guidance on next steps are also provided through the app (e.g., location of COVID-19 testing sites, online resources, and contact information). To further protect privacy, the random IDs are stored locally on each individual's device and after 14 days the IDs are deleted.[4]

The Google/Apple API technology is designed to be leveraged by public health authorities around the nation and globe to create customized contact tracing applications. For instance, California is using the Google/Apple API exposure notification technology as the basis for its application, CA Notify. CA Notify is the official Statewide exposure notification application supported by the California Department of Public Health (CDPH). It was developed in collaboration with Google, Apple, CDPH, California Department of Technology, and the University of California to support local contact tracing efforts and the State's COVID-19 prevention program. CA Notify uses the Google/Apple API to determine exposure and send notifications. At no point is specific location information or personal information, collected, stored, or shared through the CA Notify app.[5]

The panel noted that exposure notification apps can be beneficial because they can provide notification on a mass scale more quickly than individual contact tracing alone. Furthermore, exposure notification apps allow for the notification of anyone within proximity of a particular mobile device, whereas traditional contact tracing relies on the individual knowing the identities of other individuals they may have had close contact with, which can lead to missed locations and potentially impacted individuals.

---

[3] Kahn, Jeffrey and Johns Hopkins Project on Ethics and Governance of Digital Contact Tracing Technologies. Digital Contact Tracing for Pandemic Response: Ethics and Governance Guidance. Johns Hopkins University Press, 2020.

[4] S.E. Freeman, Technologies of Pandemic Control: Privacy and Ethics for COVID-19 Surveillance, CITRIS Policy Lab (October 2020).

[5] California Department of Technology, CA Notify, available at https://play.google.com/store/apps/details?id=gov.ca.covid19.exposurenotifications&hl=en_US&gl=US.

It should be noted that certain gaps are inherent in the use of these apps. They are based entirely on opting-in at this point, which, while supportive of a key aspect of privacy rights, means that the pool of individuals who decide to opt-in could be relatively limited. Reaching a critical mass of app subscribers would be an outreach effort worthy of consideration in both to inform the public about the privacy protections designed to protect their personal and location information as well as the personal and community benefits to mitigate a pandemic. Such apps also require a smartphone or smart device, which means that access to such apps may be limited to certain demographics with the means to own such devices.

Panel 1 Conclusion

Some of the inherent challenges to traditional contact tracing methods are that they are highly labor-intensive and rely on individuals to accurately recall and share information. This is where new contact tracing technologies offer some solutions. Specifically, proximity tracing and exposure notification applications such as CA Notify, which store information locally in an anonymized form to prevent direct re-identification of users, provide more complete and accurate information, while protecting individual privacy. However, as mentioned, these modern technologies are not without their own challenges and limitations. Thus, new contact tracing and exposure notification technologies should be leveraged in tandem with traditional contact tracing methods to support a more comprehensive approach going forward.

Panel 2: Privacy Impacts of Modern Contact Tracing for Future Pandemic Response

The second panel discussion focused on the potential impacts of new contact tracing technologies on privacy and civil liberties. Building on the discussion of the previous panel, the panelists recognized that the use of technology to augment traditional contact tracing raises privacy and civil liberties concerns due to the potential to collect, share, and/or use greater quantities of information about individuals. This means that when designing technology for contact tracing, designers must think not only about the benefits of the technology but also its risks, including possible abuse of information if it was obtained by those without a need to know.

In addition, the panel noted that the infrastructure of new technologies for contact tracing is often built by private companies. As a result, many of the technical decisions that affect data flows in this context are being made by the private sector. Thus, the rules they follow for designing technology, whether internal or set by regulators, are critical to ensuring protections for privacy and civil liberties. Additionally, the involvement of the private

sector means that government must be aware of any issues with limited vendors capable of producing such technologies and the willingness to make them inter-operable.

Building Contact Tracing Technology

One of the event panelists is a key member of an MIT-led group that developed an app called PrivateKit that is intended to address many of the previously stated concerns.[6] PrivateKit occupies what Johns Hopkins University researchers have described as the "middle-ground approach" in digital contact tracing technology. Similar to exposure notification apps, PrivateKit is opt-in and designed to initially store information on users' mobile devices. However, PrivateKit uses overlapped GPS and Bluetooth capabilities of mobile devices to store geographic information for a certain period of time, which users can then voluntarily upload to a database accessible to public health officials.

PrivateKit incorporates a number of approaches that are meant to address concerns related to privacy and reliance on the private sector. It is opt-in, meaning that users must consent to downloading and using the app. It is "decentralized," meaning that information is initially stored on users' mobile devices rather than immediately transmitted to a single entity. And it is built on software code that is "open source." This aspect of the design means that the app's code is available for examination by the open source software community, which includes developers, designers, product managers, test engineers and public health authorities. Another aspect of PrivateKit is that it is being developed by a diverse group of stakeholders, including academic institutions, health care providers, government, and the private sector.

Obtaining Public Input

While including a diverse group of stakeholders at the design table is critical, a major challenge of integrating new technology into contact tracing techniques is how to engage the public in the process. According to the California Institute for Local Government, public engagement results in a number of beneficial outcomes, including better identification of the public's values, ideas and recommendations, more informed residents, and, crucially, more community buy-in and support.[7] Public buy-in and support is vital for successful contact tracing efforts, which, as noted above, depends upon public trust to be effective.

Of course, public participation is not without its challenges. Providing accessible forums for the public can be difficult, and as a practical matter increased participation can slow down the design process. This is a difficult dynamic to navigate under any circumstances,

[6] MIT Media Lab, Safe Path's Overview, available at https://www.media.mit.edu/projects/safepaths/overview/.
[7] California Institute for Local Government, Why Engage the Public?, available at https://www.ca-ilg.org/sites/main/files/file-attachments/why_engage_the_public_2.pdf.

but particularly so when responding to an emergency such as COVID-19; and this is why considering such factors when building these technologies for future pandemics can allow for the necessary time to develop solutions that balance the utility necessary to be of good use and the privacy safeguards necessary to protect personal information and support the public's trust.

One example noted by the panel of a relevant forum in another jurisdiction was the Oakland Privacy Advisory Commission (OPAC). OPAC was established by an Oakland city ordinance in 2015 to advise on citywide privacy concerns. OPAC provides a public forum where issues relevant to privacy in Oakland are discussed and members of the public can participate and provide their perspective. OPAC also makes recommendations to the City Council regarding the city's use of surveillance technology. These recommendations are made using the framework established by Oakland's municipal code, which sets forth rules for the city's acquisition and use of surveillance technology. Several local governments, including the County, have enacted similar requirements for acquisitions of surveillance technology, and the panel noted that the model is versatile enough to increase transparency and provide people the chance to have a say in many different contexts.

New Contact Tracing Methods and "Surveillance"

New technologies used to augment contact tracing can be deployed in a variety of approaches, some privacy forward and others to the contrary. Methods that fall near the "maximal" approaches end of the spectrum described by Johns Hopkins researchers involve factors that evoke comparisons with popular notions of surveillance.[8] These include the Israeli government's authorization in March 2020 of its internal security service to collect location data from mobile devices to predict which citizens had been exposed to the virus and send alerts to their mobile devices ordering them to self-quarantine. Russia and Ecuador have employed similar approaches, using data from mobile devices to identify close contacts of people who tested positive for the virus and to monitor individuals under isolation when entering from abroad.[9] These maximal approaches often contain similar design choices, such as mandatory usage and a centralized entity that manages data. While these maximal approaches are relatively dramatic examples, even approaches that occupy the middle ground or are minimal in nature can utilize techniques that blur easy categorizations.

[8] Kahn, Jeffrey and Johns Hopkins Project on Ethics and Governance of Digital Contact Tracing Technologies. Digital Contact Tracing for Pandemic Response: Ethics and Governance Guidance. Johns Hopkins University Press, 2020.

[9] Human Rights Watch, Mobile Location Data and Covid-19: Q&A, May 13, 2020, available at https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa.

Contact tracing methods using technology based on granular, long-term, and comprehensive information about individuals begin to take on aspects of "surveillance" that, while clearly offering benefits, also include risks, including risks to privacy. As the panel noted, it is important to keep in mind that privacy in this context is not so much about anonymity as it is about appropriate data flows and ensuring that the right information is provided to the right people at the right time. Thus, the panel suggested that frameworks for evaluating the risks to privacy and civil liberties posed by surveillance used for traditional purposes such as law enforcement could be useful when considering new contact tracing technologies for public health purposes. Determining a community's acceptance of using this technology with their expectations of protecting individual privacy will be essential to address future implementations of new contact tracing technologies.

The Role of Procurement

A final issue that the panel discussed was the role that government procurement processes play in acquiring technology that embeds many policy choices. For example, vendors can sell contact tracing technology with a variety of features that governments can choose from. The choices include, to name just a few examples, Bluetooth versus GPS-based or a hybrid approach, open source versus proprietary, decentralized versus centralized, opt-in versus mandatory, inter-operability with other apps, exposure notification to subscribers only or to subscribers and public health authorities. Each of these decisions and features has the potential to impact privacy and civil liberties; and thus the selection of particular vendors will inherently include policy decisions related to the type, quantity, and management of information used for contact tracing. Hence it is helpful to continue to have these conversations among public and private partners to offer technology developers the opportunity to integrate policy decisions, privacy controls, and public interests in solutions during design and development. In light of the prospect of a future pandemic, creating these solutions upfront may allow for more concerted pandemic mitigations and improved outcomes that may save lives.

Panel 2 Conclusion

Overall, it is imperative to keep in mind that privacy in the context of modern contact tracing is not so much about anonymity as it is about appropriate data flows and understanding the public health response and privacy expectations of the public. Complete anonymity would mean that public health departments would not know the identities of individuals to contact, thus undermining a central purpose of contact tracing efforts. As a result, anonymity, while being privacy protective in the abstract, in this context is not the goal. Instead, the goal is ensuring that the right information is provided

to the right people at the right time. The personal information of people used for such important endeavors as pandemic response should be respected and not otherwise used for gain without consent. This goal is especially important to consider when new technologies that can disrupt previous practices of collecting and sharing information are employed.

Lessons Learned

- Trust is key in effective contact tracing, and thus decisions about employing new technologies to augment traditional contact tracing should be carefully considered.
- Members of the public may wish to review material and privacy policies about new contact tracing technologies, and consider downloading and/or enabling exposure notification apps such as CA Notify or other appropriately vetted apps.
- Exposure notification apps can be helpful, but they should be used in conjunction with rather than in place of manual contact tracing.
- Government procurement plays an important role because technologies are designed in ways that embed policy decisions.
- Contact tracing technology should be evaluated using frameworks to identify costs and benefits that allow for informed decision making.
- Public participation is critical for incorporating diverse perspectives and promoting buy-in that increases engagement and use of voluntary tools.

Appendices

- Privacy Day Flyer
- Privacy Day Program