TESTIMONY SUBMITTED BY

ELIZABETH RANDOL, LEGISLATIVE DIRECTOR

THE AMERICAN CIVIL LIBERTIES UNION OF PENNSYLVANIA

TO THE SENATE COMMUNICATIONS AND TECHNOLOGY COMMITTEE

PUBLIC HEARING ON THE DEPARTMENT OF HEALTH

COVID–19 CONTACT TRACING APP OVERSIGHT AND REVIEW

September 8, 2020

As we continue to grapple with the COVID-19 pandemic, many governments are turning to technology in the hopes that it will help fill the gaps in public health resources. State and local governments, in partnership with other public and private entities, have been exploring the adoption of tools to detect and monitor those with coronavirus. Perhaps the most prominent discussion about using technology to help fight the coronavirus has revolved around how high-tech tools can augment contact tracing, a longstanding public health technique that works by identifying everyone whom a sick person may have exposed and helping them identify their risks and take appropriate action.

Having defended privacy for 100 years, we at the American Civil Liberties Union recognize that in extraordinary times, different balances between public health and personal privacy may be warranted. The coronavirus poses grave risks, so we should not write off tools that might help stem the pandemic. But we shouldn't give up critical rights and freedoms unless a proposal is **necessary, effective, and proportionate.**

We are particularly wary of technological solutions that would interfere with or divert resources away from public health solutions with proven effectiveness or that risk exacerbating existing disparities that have already led to inequitable health outcomes. Any uses of technology should:

- Be temporary;
- Be restricted to public health agencies and purposes;
- Allow for privacy and anonymity to be protected, even as the data is used; and
- Should not substitute for a comprehensive health response that provides resources to people who cannot or will not use apps.

ACLU-PA Recommendations for Technology-Assisted Contact Tracing (TACT)

Programs designed to track the spread of coronavirus include traditional manual contact tracing, technology-assisted contact tracing (TACT) and hybrid models. All of these models work backwards from people with coronavirus infection to identify people who may have been exposed to the disease, so that they can be tested, isolated, and — when necessary and possible — treated.

The ACLU of Pennsylvania offers the following suggestions and recommendations to address the crisis in a manner that respects and advances civil liberties. The steps laid out below are necessary for the consideration of a technology-assisted contact tracing model. The first step of expanding public health resources is critical to the success of any tech-assisted effort. The second, third, and fourth steps are crucial to making sure resources are spent on something that has the capacity to be accessed by a large number of people and is effective in identifying at-risk patients. Steps five and six ensure that technology is adopted using a privacy protective framework.

1 | Continue investment in & expansion of public health resources

Even if technology-assisted contact tracing (TACT) works, it can only do so in the context of other public health interventions, specifically:

- Manual contact tracing, which directly connects people to services, healthcare and other resources, and allows potentially-infected people to talk to another person, ask questions, and process the information shared.
- Widespread availability of free and quick testing, so that people who may have been exposed have the information they need to seek treatment or return to their daily activities.
- Better equipping hospitals, and
- Having a plan and resources in place for people to safely self-isolate.

Every proposal should be predicated on the availability of widespread, affordable, accurate, and prompt testing. Even the best TACT program will generate false positives – making widespread testing even more critical to ensure that individuals do not self-isolate unnecessarily for two weeks.

No tech-assisted model should divert resources from known, effective public health measures like testing, counseling, research, and treatment. Deploying tech-assisted contact tracing at the expense of traditional medical and social interventions would be ineffective, if not counterproductive.

Challenges to tracing COVID-19

COVID-19 is a more difficult disease to trace than many others. As a group of epidemiologists explained in a recent report on contact tracing, contact tracing is less effective when:

- **The disease is transmitted through the air:** Compared to the kind of contact tracing that has long been done with HIV, where transmission takes place through sex or blood, respiratory transmission is much harder to track.
- **The infection rate in a community is high:** As of this writing (September 2020), the United States leads the world in the total number of deaths (186,663) and total number of cases (6,144,138) with approximately 40,000+ new coronavirus cases being identified every day. Contact tracing is most effective either early in the course of an outbreak or much later in the outbreak when other measures have reduced disease incidence to low levels. Until the U.S. slows its rate of community spread, experts recommend concentrating contact tracing on contacts within households, healthcare and other high-risk settings, and case clusters — an approach much more amenable to manual contact tracing.
- **A large proportion of transmissible infections are from people without symptoms:** The CDC estimates that 40 percent of new COVID-19 infections come from asymptomatic carriers.

Critical role of manual contact tracing programs

Technology-assisted contact tracing programs should only be used in conjunction with established manual contact tracing. And TACT programs must establish that they can improve upon or significantly augment old-fashioned human contact tracing to justify the investment.

Manual contact tracing relies on human contact tracers to connect directly with people who have tested positive for COVID-19. Once these individuals are identified, contact tracers conduct interviews to help the person who is infected recall where they have been and identify people who may have been exposed. Follow-up calls are made to notify the people who were possibly exposed and contact tracers provide them with next steps and information about where to get tested, resources to meet their housing or transportation needs, and any additional information that can help keep them safe.

Why manual contact tracing remains the recommended method:

- **Proven public health approach:** Manual contact tracing has been used to contain all kinds of contagions, from sexually transmitted infections, to the swine flu and Ebola outbreaks.
- **Builds trust:** The manual contact tracing process directly connects people to services, healthcare and other resources.
- **Privacy-protective:** Manual contact tracing does not create a new surveillance infrastructure as technology-assisted contact tracing would. Patients are in control of the information they reveal, such as where they went or who they came into contact with, without the added worry that an app or technology is following their every move.
- **Creates jobs:** While certain roles may require a licensed health care worker or social worker, others can be done by trained individuals equipped with a phone and laptop. This creates much-needed job opportunities for people who have otherwise lost their source of income due to the public health crisis, especially those in communities that are disproportionately impacted.

2 | Identify specific goals and use of the technology

The likely effectiveness of different uses of TACT data hinges on exactly how each is envisioned as being used in the effort to stem the spread of the coronavirus. Key questions to guide the planning process include:

- **What is the goal?** Is it tracking overall trends, helping people who have tested positive recall past contacts, identifying unknown individuals who may have been infected by the patient, or enforcement of quarantines or stay-at-home orders?
- **What data?** Is it aggregate and anonymized data or individually identifying information? How precisely can the information pinpoint individuals' locations? Is the dataset complete enough that one can draw meaningful conclusions? Will the data under– or misrepresent people of color or low-income communities in a manner that could lead to prejudicial results?
- **Who gets the data?** Does the government get access to the raw data? Is it shared only with public health entities such as qualified academics or hospitals, or does it remain in the hands of the private entity that originally collected it?
- **How is the data used?** Is data used for centralized government action, such as issuing or enforcing quarantine orders or other punitive measures? Or does it enable decentralized individual decision-making such as checking announcements of possible exposure points and choosing to go to a testing center?
- **What is the life cycle of the data?** Any corpus of data is likely to create risks to the people it represents. A responsible steward of other peoples' data will have plans for data destruction once the data's relevance is diminished, to mitigate future compromise.

3 | Assess and determine the technology that will be used

Generally, a tech-assisted contact tracing model is a hybrid system that relies on a staggered approach to contact tracing. It is built on the same principles of manual contact tracing and uses technology to enhance the process. These proposals differ from the traditional public health technique of "contact tracing" to try to stop the spread of a disease. In place of human interviewers, they would use location or proximity data generated by mobile phones to contact people who may have been exposed.

While some of these systems could offer public health benefits, they may also cause significant risks to privacy, civil rights, and civil liberties. If such systems are to work, they must be widely adopted, but that will not happen if people do not trust them.

While we have a lot of skepticism about whether this concept is likely to prove practical, the ACLU has outlined a set of technology principles that the public and developers should use to assess any such proposal and has outlined principles to inform policies and procedures governing the use of these untested technologies.

Location tracking

Early technology-assisted contact tracing (TACT) proposals relied on location detection by mobile phones to selectively deliver alerts about potential exposures. Location-based tracking relies on cell signals, GPS, and WIFI to access location data. Once a user opts-in, the app tracks the user's location to build a trail of where they have been.

Most of these early proposals have rightly been dismissed. Mobile phone location data is almost impossible to anonymize and is not nearly accurate enough for identifying those who have been exposed to an infected person. And even if it were, this data is collected through a variety of technologies and is scattered among a variety of companies. Much of this data is gathered by privacy-invading companies that sneak tracking software into phone apps or exploit the pandemic to market their products. Attempts to deploy this concept have not gone well, often producing many false positives, rendering it virtually unusable.

Proximity tracking

More viable proposals have centered around using Bluetooth technology to allow phones to detect other phones that come nearby and use that to automatically keep track of who may have been exposed to an infected person. Proximity tracking generally relies on Bluetooth signals that can be sent to/from phones within 30 feet of one another. The alerts sent out through this system are not real-time and only happen if a person tests positive and they alert other users via the app of their status.

Of course, the only way Bluetooth technology works is if a phone has both the capacity for it and a user enables it. And there are significant technical challenges with using smartphones, including how Bluetooth is used to determine which encounters should be recorded as potential transmission events. Bluetooth can't reliably measure distances — the strength of a Bluetooth signal varies not only with distance, but also from phone to phone, and from owner to owner. The frequency at which Bluetooth operates (2.4 GHz) is one that is easily absorbed by water, including the water in the human body, which means that signal strength can vary significantly depending upon whether a person has their phone in their front or back pocket, and how much that person weighs. This may result in false positives and negatives.

But if done properly, this approach can be more privacy-protective because it does not require the collection of sensitive location data and stores data locally and in ways that don't identify people. Currently, there are several system proposals that aim to be privacy-friendly, including the Decentralized Privacy-Preserving

Proximity Tracing (DP-3T), Private Automated Contact Tracing (PACT), Temporary Contact Numbers (TCN), and the Apple-Google proposal.

The Bluetooth-enabled approach gained traction when Apple and Google announced a joint contact tracing effort that would use Bluetooth technology to help alert people who have been in close proximity to someone who tested positive for COVID-19. Like location histories, proximity records can be highly revealing because they expose who we spend time with. To their credit, the Apple/Google developers have considered that privacy problem. Rather than track personally-identifying location histories, apps based on the Apple/Google protocol would use identifiers that cannot easily be traced back to phone owners.

The Apple/Google proposal offers a strong start when measured against privacy-protective technology principles, which includes a plan to terminate their tracking tools at the end of the pandemic. But while they (and others) have created the best possible chance of engendering trust in TACT apps, those protections still have gaps and raise additional questions.

Given the strengths and weaknesses of the technologies, proximity-based contact tracing is currently the strongest tech-assisted proposal, though its value is still unproven. While it carries accessibility concerns, proximity-based tools could realistically meet other privacy-protective principles.

Resource aggregating apps

While tech-assisted contact tracing proposals have been widely discussed, there are other ways to use technology that can help the public during this health crisis. One such way is by providing the public with a resource-based app that provides city/state-specific information on COVID-19, such as where to get tested, how to stay safe, and contact information for social workers, health care professionals, counselors, and others.

Benefits of a resource-based app:

- It is a one-stop-shop approach in the fight against COVID-19 — it can be consistently updated with more information about new testing sites, medical developments, and other helpful tools that are otherwise scattered across various platforms or websites.
- Since no personal information is involved, it is privacy-protective.
- Unlike TACT proposals, which need time to be rolled out, a resource-based app could be made available relatively quickly and easily accessible across multiple operating systems.
- Given the limited funding and resources needed to actually develop and introduce this sort of app, adoption of this method would help free up funds and other resources that can be dedicated towards manual contact tracing efforts.

4 | Set benchmarks for efficacy and equity

Is it effective?

Contact tracing or related technology should be deployed only if it promises to be effective and should continue to be used only if it is shown to work. Therefore, governments should set benchmarks for the efficacy of the technology, factoring in accuracy, risk of false positives/negatives, and known limitations.

To prevent improper reliance on contact tracing or related technologies, health agencies should also set clear public benchmarks for what standards a tool must meet to be considered effective. These benchmarks should consider the following factors when analyzing the efficacy of using any technology:

- **Accuracy:** Identify the overall rates of accuracy for notifying individuals of potential exposure. Inaccurate results risks generating far too many “exposure notifications.” Swamping users with false

notifications would be useless and annoying at best, and seriously disruptive and counterproductive at worst.

- **Adoptability**: Consider whether the proposed technology-assisted contact tracing model relies on phones or other specific technology to which not everyone has access. A benchmark can be as simple as setting a goal for 60% adoption and measured by counting the number of app installations.
- **Interoperability**: Determine whether the technology can operate on all operating systems (e.g., Android and iOS).
- **Data Usage:** Ensure that the public is aware of what information they are agreeing to share by using the technology and how the data that is collected will be used. It is imperative that all uses of the data are stated so that people are aware of what information they are agreeing to share.
- **Data Sharing:** Prohibit sharing the data with non-public health government agencies or other third parties. Downloading an app and agreeing to share certain data for a stated public health purpose, only to discover that the data was shared with law enforcement or immigration authorities, would sow fear and distrust within the public.

Information should be made public about how these tools measure against these benchmarks so that the public has a clear understanding of how and whether they are reliable. To the extent public health agencies contract with developers to create these tools, the developers should be required to provide the necessary information to conduct this analysis.

Is it equitable?

Governments should proactively develop projections and plans to target deployment of additional health resources to high-risk communities and those who lack technology access. Many of these populations may be disproportionately left behind if TACT is the sole or primary means of allocating COVID health resources.

Data on the COVID-19 outbreak in the United States show that Black communities have been disproportionately afflicted, as have other communities of color. If governments rely on these technologies as the sole means of contact tracing and fail to provide additional resources to assist those communities, they will exacerbate existing health inequities and undermine our overall ability to prevent community transmission.

Contact tracing apps require the use of a smartphone, which will likely exclude vulnerable and/or marginalized community members — who may be unable or unwilling to use a contact tracing app — from the benefits of this technology. Reliance on access to smartphones creates its own set of inequities:

- Smartphone ownership is not evenly distributed by income, race, or age.
- Studies have found that over 40 percent of individuals over age 65 do not have a smartphone — a population that accounts for over three-quarters of COVID-related deaths.
- Nearly 30 percent of individuals earning less than $30,000 annually do not own a smartphone.
- Individuals with disabilities are 20 percent less likely to own such devices than the general population.
- Additional at-risk groups, including people who are homeless or incarcerated, also lack access.

Affordable internet connectivity may also pose a challenge to using a contact tracing app, given the need to transmit data. An estimated 24 million Americans and 30 percent of rural Americans lack access to broadband service. Even for those who have access to a smartphone and affordable broadband, technical capability and lack of support may pose a challenge.

Additionally, health agencies, in partnership with the private sector where appropriate, should ensure that any rollout of new technology is coupled with efforts to provide technical assistance to those who may need it. In particular, communications about the tools, including information about privacy, should be:

- In plain language and written at a fourth-grade reading level (or less) to reach the widest audience.
- Materials on websites should be accessible to screen readers and other assistive technologies, and consistent with WCAG 2.0 AA standards.
- Televised announcement should include closed captioning and a qualified American Sign Language (ASL) interpreter.

5 | Identify who can access and manage the technology

To ensure that a large number of people download and use the technology and that the data collected is used in the most responsible manner, identify who can access and who will manage and administer the data.

Limited access, non–punitive use

Governments should require that any data obtained from these tools be used only by public health agencies and for public health purposes related to the pandemic. They should also prohibit disclosure of personal information to non-public health agencies or other third-parties and require destruction of the data once its utility has expired. In an ideal scenario, only the phones themselves and a public health agency will get access to the data collected.

The data should not be used for purposes other than public health — especially not for any punitive or law enforcement purposes. Lack of trust in the authorities among Black, brown, and immigrant communities severely complicates plans for using TACT systems. All technologies carry the risk of raising fears among vulnerable communities that downloading an app could expose them to law enforcement or immigration authorities, or privacy-protective individuals who worry about how their data will be used, stored, and shared. This may result in people not downloading the app at all or simply not complying with it if they do download it out of fear of who is getting the data.

Decentralize data storage

Data storage should be decentralized to prevent breaches. Numbered signals emitted from phones should be stored on the phones themselves and not in a centralized system. And if a breach occurs, programs should have the ability to quickly notify users.

6 | Maintain privacy-protective safeguards

For both manual and technology-assisted contact tracing models, privacy–protective policies should govern the exposure database and keep it secure from a possible breach. Technology principles that embed privacy by design are one important type of protection. There still need to be strict policies to mitigate against overreach and abuse. These policies, at a minimum, should include the following elements:

Voluntary use

Consistent with the long-standing advice of public health professionals, any use of TACT must be truly voluntary. Coercive health tactics often backfire, engendering community distrust. TACT programs will not be as effective if individuals who have been infected resist supplementing the data collected with their personal knowledge.

Whenever possible, a person testing positive must consent to any data sharing by the app. The decision to use a tracking app should be voluntary and uncoerced. Installation, use, or reporting **must not** be a precondition for returning to work or school, for example.

Important public benefits should not be conditioned on use of a contract tracing app. Governments should prohibit private and public entities from coercing individuals into using a contact tracing app by making the use of an app or technology a condition of access to employment, public transportation, housing, and other necessities and critical services, such as grocery stores and pharmacies.

Minimized and anonymized data collection

For communities to feel comfortable using TACT, they must have assurances that there are clear limits on the use, sharing, and retention of their information. The best way to ensure such limits is to design the tools to protect privacy by collecting no more information than is necessary and anonymizing where possible information that is collected.

Minimize the type of data collected and define an expiration date at which point the data will be completely purged from the system. Data that is collected and shared should not contain any identifying information and the process should be designed to be as anonymous as possible throughout.

Policies must be in place to ensure that only necessary information is collected and to prohibit any data sharing with anyone outside of the public health effort. Recommended practices include:

- Anonymize both the raw (data as it is collected) and analyzed (data once it has run through an algorithm or been analyzed) data.
- Do not rely on persistent identifiers (signals sent from phones to each other) that can be linked back to a user or location. This can be accomplished by making sure the phones send out unique numbers to each other that change frequently (every 15 or 30 minutes instead of once a day).
- No information should be shared until someone tests positive, at which point the unique number sequences are shared in a manner that warns individuals who may have been exposed.
- At no point should someone who has been exposed to the virus get any identifying information about who exposed them.

Enforceable rights

Putting users in control of their data is the best way to ensure privacy limits are in place. However, even with good design features, some information will likely still be collected, and individuals will need a way to enforce their rights in cases of abuse or inadvertent error.

Health privacy laws, like the Health Insurance Portability and Accountability Act (HIPAA), generally do not apply to health data generated by private consumer apps and devices, and the federal government has waived the law in certain COVID-19 contexts. At the same time, the United States lacks a strong, comprehensive federal data privacy law that would protect consumers' rights. At the state level, there are a patchwork of privacy protections that largely fall short.

To ensure that individuals who use contact tracing technologies have enforceable privacy rights, public health agencies should only use or contract with companies that have strong privacy protections built into their terms of service. Those terms should:

- Notify users in plain language of what information is being collected and how it is being used;
- Limit data collection, use, and retention to what is necessary to provide the contact tracing service;

- Permit the use and transfer of information only to public health agencies and only for public health purposes, safeguarding information from law or immigration enforcement officials;
- Require specific opt-in consent to transfer any data from the user's device;
- Prohibit surreptitious collection of location and other information without the user's specific opt-in consent;
- Require any health agency that receives data to limit subsequent transfers without the user's specific opt-in consent;
- Exclude provisions, like mandatory arbitration, that make it difficult for individuals to seek redress in cases where terms of service are violated;
- Permit a consumer to request information about personal information that has been collected, used, or retained about them, and to delete it; and
- Cease functioning and delete personal data based on specific criteria that indicate the pandemic has ended.

Data destruction

Tracing technology should not outlive the effort against COVID-19. Any technology-assisted contact tracing system that targets a particular epidemic should not last beyond the particular disease it targets.

Governments should identify when and how the technology will be phased out, including a plan on ending its use (such as shutting down servers) and deleting the data collected. The public should also be given instructions on how to uninstall the app if it cannot be done on its own.

Transparency, oversight, and accountability

Governments should adopt independent auditing and oversight measures to ensure that any contact tracing app is used solely for public health, operates as intended, and is limited to the duration of the pandemic.

Governments should also adopt a policy of proactive transparency that includes the full public release of contracts related to development of the technology, audits, and agency guidelines governing the treatment of any information related to the tool. They should disclose the vendor/company that the government has contracted with, who is accessing the data that is being collected, what information is being collected, how long the information is being stored, and other information about the technology-assisted contact tracing process.

And governments should only commit to using apps with terms of service that provide strong enforceable privacy protections. Technology developers should also commit to providing such protections, and distributors of technology (like Apple and Google) should limit their distribution to technology that is accompanied by these protections. This transparency is essential to maintain public trust and ensure that individuals can feel confident that their rights are being fully protected.

These policies, at a minimum, must be in place to ensure that any tracking app will be effective and will accord with civil liberties and human rights.

Conclusion

Governments considering the use of contact tracing or related technologies must take steps to ensure voluntary use of any tool, ensure equitable health resources, limit use of any data obtained to public health purposes, provide individuals with enforceable rights, and maintain appropriate oversight, accountability, and transparency.

Even if these tools are adopted with appropriate safeguards, it is important to recognize that they are far from a silver bullet. They will not resolve testing shortages, which are essential for notified individuals to determine if they have in fact been infected. They will not ensure individuals who are infected get adequate and equitable treatment. And they are not a substitute for clear guidelines for the public to determine what they can do to better protect themselves, their families, and their communities. These tools can only be part of a broader health strategy that resolves these and other significant issues.

Resources

ACLU research, white papers and guidance

- Principles for Technology-Assisted Contact-Tracing
- The Limits of Location Tracking in an Epidemic
- Government Safeguards for Tech-Assisted Contact Tracing
- Pandemic Preparedness: The Need for a Public Health — Not a Law Enforcement/National Security — Approach
- Apple and Google Announced a Coronavirus Tracking System. How Worried Should We Be?

Data resources

- Apple-Google proposal: Apple | Google
- Decentralized Privacy-Preserving Proximity Tracing (DP-3T)
- Private Automated Contact Tracing (PACT)
- Temporary Contact Numbers (TCN)
- Contact-Tracing Apps are not a Solution to the COVID-19 Crisis