ACLU OF IL GUIDANCE: CONTACT TRACING AND EXPOSURE NOTIFICATION INITIATIVES

State and local governments, in partnership with other public and private entities, continue to explore efficient, effective ways to reduce the spread of COVID-19. This work now includes discussions about the identification and adoption of tools to detect and monitor those with coronavirus, so they can be offered treatment as quickly as possible and so that people with whom they have been in contact can take appropriate measures to guard against further transmission. It is imperative that this work balance public health and personal privacy.

Decision-makers are exploring options designed to protect the public that 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.

As decision-makers identify and implement these public health strategies in the effort to protect residents against COVID-19, the ACLU of Illinois offers the following suggestions and recommendations to address the crisis in a manner that respects and advances civil liberties.

OVERALL BEST PRACTICE RECOMMENDATIONS:

Adopt and utilize manual contact tracing

- 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 sensitive interviews to help the person who is infected recall where they have been and identify people who may have been exposed.
- Once this information is collected, follow-up calls are made to notify the people who were possibly exposed. 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.

Reasons why manual contact tracing is 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.
  - We cannot be confident that technology-assisted contact tracing will work, especially given the imprecision of cell phone-generated location and proximity data.

- Builds trust
  - The manual contact tracing process directly connects people to services, healthcare and other resources.
    - Relying on human connection to gather critical information creates a relationship that cannot be replicated via technology. Human outreach and interaction allow people to talk to another person, ask questions, and process the information shared.
- Privacy-protective
  - Manual contact tracing does not create a new surveillance infrastructure as technology-assisted contact tracing would. The 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.

    Note: Given the sensitive nature of the information collected, it is important to make sure that all the data collected (whether by manual or tech-assisted contact tracing) is protected by law and safe from breach. The data should be securely stored and HIPAA protections should be fully applied.
- Creates jobs
  - A patient may have been in contact with 100 other people recently, which means 100 follow-ups are needed to track down everyone who may have been exposed.
  - 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.

To better understand how this manual contact tracing process can work, below is an illustration of a team structure with four specific roles.

1. Initial Callers: These team members are trained on how to conduct sensitive telephone interviews with anyone who has tested positive for COVID-19.
   - The Department of Public Health would provide the names and contact information for anyone who has tested positive so that the initial caller can conduct the first interview.
   - The goal of these calls is to get information from the person who tested positive about anyone who came within 6 feet of them for at least 15 minutes in the past two weeks.
   - Once this information is collected, these callers share the contact information for those who may have been exposed with the Contact Tracer.

2. Contact Tracers: These team members make the follow-up calls with each of the contacts to let them know they may have been exposed.
    - Given the possibility that anyone who has tested positive and possibly exposed others to the virus may feel shame and stigma, the Contact Tracer would not share any identifying information about who tested positive.
    - Instead, they only share a date range (such as two or three days) of when they may have been exposed. This approach aims to be privacy-protective by not singling out a specific time period; however, it does not guarantee anonymity.
    - The Contact Tracer also gathers information about the individual's living environment (e.g., if they live alone or with others) and shares information on next steps (such as where to get tested and how to stay safe).
3. Support Service Coordinators: These team members help provide support service resources to anyone who has tested positive or been notified of exposure.
    - This role is often best filled by social workers who have knowledge of resources rooted in the community. With those connections, manual contact tracing teams stay connected with the tools available in the local area.
    - Support services that this caller may share include, but are not limited to, housing, food, medicine, economic support, and counseling.
4. Managers: To ensure that the overall unit functions as needed and concerns are addressed throughout the process, there should be a manager or administrator that oversees the full group.
    - The manager is responsible for making sure that all members of the team are adequately trained to serve the role they are assigned.
    - Given the sensitive nature of all information collected, the manager must ensure that the process and data storage is HIPAA-compliant and secure.

Note: This structure is similar to the model created and implemented by Partners in Health in Massachusetts to help combat COVID-19. While we reference the model, it is not an endorsement.

RECOMMENDATIONS IF ADOPTING A TECHNOLOGY-BASED APPROACH:

Utilize a tech-assisted contact tracing model

- 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. This approach can be rolled out in a privacy-protective manner that will help account for a larger population of people who may have been exposed.

- The specific features of a privacy-protective technology-assisted contact tracing model are:
    - A voluntary app that a user chooses to download onto their phone that relies on proximity-based contact tracing by using Bluetooth signals.
    - Phones send out unique number sequences to each other. These numbers change frequently (every 15 or 30 minutes, versus once a day), so that they cannot be linked back to anyone specifically.
    - The numbered signals that the phones send out are stored on the phones themselves and not in a centralized system.
    - No information is shared until someone tests positive. Then the unique number sequences are shared in a manner that warns individuals who may have been exposed.
    - The data that is collected and shared does not contain any identifying information and the process is designed to be as anonymous as possible throughout.
    - All data generated and shared is used only for public health purposes, and there is no data-sharing between non-public health government agencies.
    - At no point does someone who has been exposed to the virus get any identifying information about who exposed them.
- In order to adopt an effective technology-assisted contact tracing or exposure notification model, its ability to achieve public health goals must be measured. Factors to consider when contemplating the efficacy of a technology include:
    - Adoptability: Consider whether the proposed technology-assisted contact tracing model relies on phones or other specific technology that not everyone has access to.
    - 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: Do not share 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 create fear among the public of downloading and making use of available technology. Even if they download the technology, they may not fully comply with it out of fear of harassment or other punitive measures.

- 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 and third 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 four and five ensure that technology is adopted in a privacy-protective framework.

Step 1: Invest in and expand public health resources.

- Widespread testing is necessary to ensure that everyone who is notified of possible exposure is able to access tests quickly and efficiently. Testing is critical to help flatten the curve and decrease the spread of the disease by ensuring that everyone who is positive self-isolates or gets proper care.
    - Without cheap, widely accessible, and accurate testing people may self-isolate themselves after simply seeing a notification that they may have been exposed to the virus without ever testing positive.
- Establish fully-staffed hospitals with enough equipment to accommodate a large influx of patients.
- Ensure that all people have a safe space to isolate if they are sick. This means investing in temporary lodging options, such as hotels or dorm rooms, and making sure that they are accessible to anyone who may need them.

Note: No tech-assisted model should divert resources from known, effective public health measures like testing, counseling, research, and treatment. Every proposal is predicated on the availability of widespread, affordable, accurate, and prompt testing. Deploying tech-assisted contact tracing at the expense of traditional medical and social interventions would be ineffective.

Step 2: Identify specific goals and use of the technology

- Develop goals to help measure the effectiveness and need for the technology.
    - This can be as simple as setting a goal for 60% adoption, which can be measured by counting the number of app installations.
- Build in oversight mechanisms, including assessments before, during, and after it is implemented.
    - For example, once the technology is rolled out, identify a government agency that can monitor the number of app-facilitated contacts with the medical system and the number of self-reported self-isolations.
    - Compare these numbers with the data collected before the technology was adopted to help identify the effectiveness as well as any possible disparate impact (such as the app's failure to result in an increase of contacts among people of color).

- Identify when and how the technology will be phased out, including a plan on deleting the data collected.
    - Any technology-assisted contact tracing system that targets a particular epidemic should not last beyond the particular disease it targets or be used if it is ineffective.
    - This means that from the outset, the system should identify measures that help determine its efficacy (such as a certain threshold of downloads, decrease in positive cases, etc.) and a plan to end its use (such as shutting down servers). The public should also be given instructions on how to uninstall the app if it cannot be done on its own.

Step 3: Assess and determine the technology that will be used.

- All contact-tracing methods, both tech-assisted and manual, risk exposing the sensitive health information of an infected person to their potential contacts. Therefore, it is critical that any proposals being considered are thoroughly reviewed to ensure that they protect user privacy.
    - This means that the technology only collects data that is absolutely necessary, removes any features from the data collected that could identify specific people, and all data that is collected is stored in a safe and secure way (e.g., end-to-end encryption, decentralized storage).
    - At this time, 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. While all of these proposals and others use mobile phones, they employ different technologies. Two of the major formats are discussed below:
        - Proximity Based – 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.
            - *The only way Bluetooth technology works is if a phone has both the capacity for it and a user enables it. As such, relying on this technology means that anyone without such a phone or without Bluetooth enabled will not be accounted for (e.g. some members of communities that are low income or experiencing homelessness).*
            - *Even if people have the required technology, this method may not be effective because it would need a certain level of adoption by the public. While some experts say that 40% - 60% of the population must use such an app for it to be effective, the technology may not be able to reach that usage level. People may not download the app out of fear of punitive*

measures or selectively choose to comply based on what they feel comfortable sharing with the government.

- *Using Bluetooth signals to identify when someone is in close enough proximity to another person that they may have been infected may not work – the strength of the signal is highly dependent on the situation. There will be a lot of false positives and negatives.*

– Location Based – 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.

- *This technology is not sufficiently precise to build a robust contact tracing system that can adequately reach a wide population in an effective way.*

- *It is also incredibly difficult to actually anonymize the data collected when using a location-based system. As used in Israel, the system is also producing many false positives, rendering it essentially unusable.*

- 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 meet other privacy protective principles discussed in step five.

Note: Government entities should heed advice from public health experts to identify the specific public health need to be addressed by a technological tool, but it should be implemented only after careful review by privacy experts to contemplate and assess the implications of any technology tool. All technology employed must be narrowly tailored to address a critical public health challenge in a manner that respects civil rights, privacy, and individual safety for everyone.

Step 4: Identify who will 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 effective manner, identify who will manage and administer the data.

– 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.

– The government should make a conscious effort to limit who can access and use the data. In an ideal scenario, only the phones themselves and the Department of Public Health will get access to the data collected. No data-

sharing among other governmental agencies or third parties should be permitted.

- 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.

Step 5: Maintain privacy-protective principles.

- **Minimization**: Minimize the data collected and define an expiration date at which point the data will be completely purged from the system.
- **Voluntariness**: Keep the technology voluntary. In order to gain the trust of the public, it is essential to encourage them to download the app without making it mandatory.
- **Anonymization**: Both the raw (data as it is collected) and analyzed (data once it has run through an algorithm or been analyzed) data should be anonymized. Additionally, do not rely on persistent identifiers, or 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, versus once a day).
- **Transparency**: Remain transparent about who the vendor, or company, is 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.
- **Interoperability**: Build a technology-assisted contact tracing model that can operate on all operating systems *(Android & iOS)*.
- **Decentralization**: Decentralize storage to prevent breaches. If a breach occurs, notify users.
- **Non-punitive**: No contact tracing model should be used for punitive measures. Instead, they should focus on helping people who have been exposed with resources that will keep them safe.
- **Oversight:** Build in mechanisms that can assess the effectiveness and impact of the technology before, during and after its use. Identify who will be overseeing this assessment process and consult with privacy and public health experts throughout.

AT THIS TIME, WE DO NOT RECOMMEND A TECH-ONLY CONTACT TRACING EFFORT. NO TECH-ONLY CONTACT TRACING EFFORT HAS BEEN IMPLEMENTED AND PROVEN BOTH EFFECTIVE AND PRIVACY-PROTECTIVE.

FAQ – Other Technology Options:

What about other technology that is being used to combat COVID-19? How can that technology be assessed for both efficacy and privacy?

- A number of other technological options have also been developed and proposed to fight COVID-19; among them are data scraping and analyzing technology that gather and analyze information from thousands of apps being used on individual cell phones (such as maps, social media, or search engines).
    - Based on the data gathered, companies have been able to work with government agencies and share location information to track where residents are going, if they are staying home or not, and other travel patterns.
    - While this type of technology can be effective in understanding travel patterns and behaviors during the public health crisis, it does so at the cost of individual privacy. Users do not know that they are giving away information about themselves to third-party companies when they are using other apps or search engines on their phones.
    - Government reliance on these types of data scraping technologies may also heighten the public's resistance to downloading any future contact tracing apps out of fear that their data is being collected, used and shared for purposes other than those stated or for which the app was created.
- Questions that should be asked when considering utilizing scraping technology:
    - Where is the technological platform getting their information?
    - What are the biases and unintended consequences of the process?
    - What are they doing with the information they are collecting?
    - What does the processing reveal about their data analysis?
    - What action is taken as a result of the data collected?

What are thermal imaging, or fever detection, technologies? Can they help combat the spread of COVID-19?

- Thermal Imaging: This technology generally takes the form of an artificially intelligent (or "smart") thermal camera and sensor system that can read heat signatures on people and objects.
    - Thermal imaging tools are also known as fever detection technology because they aim to detect fevers and alert users to the presence of someone who may be carrying COVID-19.

- Vendors are actively working to equip traditional fever-detection technology with facial recognition capabilities. Others are exploring remote options by using drones to identify when someone has a fever or a cough.

- This technology has traditionally been used industrial and military settings. It is now being proposed to be used in grocery stores, hospitals, and voting locations.

    - *One vendor is currently deploying this technology at government agencies, airports and Fortune 500 companies.*

- Concerns:

    - Thermal imaging cameras are still surveillance cameras and risk chilling free expression, movement, and association in public places; over-policing of vulnerable populations; and open the door to facial recognition.

        - *Spending money to acquire and install a thermal imaging infrastructure increases the likelihood that the hardware will outlive the public health crisis.*

        - *Even during the crisis, these cameras risk constantly surveilling the public wherever they go.*

    - Thermal imaging from a distance may not be effective in detecting a fever. The cameras typically only have an accuracy of about +/- 4 degrees Fahrenheit at best.

        - *Given how widely human temperatures tend to vary, this technology carries a high risk of false positives, involuntary isolation, and harassment.*

    - Thermal imaging technology cannot help detect the virus itself. Instead, they merely measure whether or not a person has an elevated skin temperature.

        - *As such, the technology is not on its own effective in lowering the spread of COVID-19 since not everyone with coronavirus develops a fever.*

        - *It also carries the risk of scaring members of the public into self-isolating when they have not tested positive.*

    - The technology is unable to precisely isolate an individual person when it comes to tracking their temptations.

        - *Thermal imaging tools are not able to adequately isolate people as they come through checkpoints equipped with the technology.*

- Even if the technology is able to identify a person with a fever accurately (which has yet to be tested and determined), there are logistical challenges with deploying the technology.
    - *Once someone tests positive with a fever, staff would need to isolate the person and test them for COVID-19. In a public facility, this would not only take a lot of time and resources, but it would also create a large backlog.*
    - *Additional staff would also be required to disinfect contaminated areas.*

Given the high financial and privacy costs of thermal imaging technology and its ineffectiveness in combatting the spread of COVID-19, we do not recommend its use.

How else can decision-makers leverage technology in a way that can help the public and combat the spread of COVID-19?

- While tech-assisted contact tracing proposals have been widely discussed around the world, there are other ways to use technology that can help the public during this public health crisis. One such way is by providing the public with a *resource-based app*:
- How it could work:
    - Accessible on both Android and iOS devices, this could take the form of an app that provides information on COVID-19, where to get tested, how to stay safe, etc.
    - Additionally, the app can connect the public with helpful resources in the City or State, such as contact information for social workers, health care professionals, counselors, and others.
    - Finally, the app can be consistently updated with more information about new testing sites, developments in the fight against COVID-19 and other helpful tools that are otherwise scattered across various platforms or webpages.
- Why a resource-based app could be helpful:
    - This one-stop-shop approach to battling the current public health crisis will utilize technology in a way that is easily accessible and privacy-protective (since no personal information is involved).
    - Unlike TACT proposals, which need time to be rolled out, this app could be made available relatively quickly.

- Given the limited funding and resources needed to actually develop and introduce this sort of app (since most of the information is already available and can be easily gathered through conversations with public health workers), adoption of this method would also help free up funds and other resources that can be dedicated towards manual contact tracing efforts.

Additional Resources:

ACLU Contacts:

If you are a decision-maker or government agency considering contact tracing or other technology-based tools to combat COVID-19, please reach out to us and we can provide additional information about the privacy and civil liberties implications of a proposal.

We can also connect you with a technologist and provide additional resources to help guide your decision to adopt a certain tool.

Links to additional research, white papers and tools:

- Principles for Technology-Assisted Contact-Tracing
- The Limits of Location Tracking in an Epidemic

  Apple and Google Announced a Coronavirus Tracking System. How Worried Should We Be?

Links to resources cited in this guidance:

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

For more information, contact:

Khadine Bennett, Director of Advocacy and Intergovernmental Affairs
kbennett@aclu-il.org | 312.607.3355
Sapna Khatri, Advocacy and Policy Counsel *(Privacy, Technology and Surveillance)*
skhatri@aclu-il.org | 417.693.7871

ACLU Illinois