ACLU OF IL GUIDANCE: DEVELOPING A PRIVACY-PROTECTIVE CONTACT TRACING SYSTEM

Best Practices for any contact tracing system

When it comes to sharing information with the government, there is a growing issue of distrust among the public. Which is why we need to think about ways to maximize trust, protect privacy, and build in government accountability for any contact tracing efforts. To that end, we've identified some principles that can help achieve those goals:

- ✓ **Robust Security:** Decentralize storage if possible to prevent breaches. If the data must be stored in a central location, define who can specifically access the data that is stored (such as specific members of the Dept. of Public Health) and limit access to the data. This includes storing the data on a govt. server with encryption and a firewall so that no third party or other govt. agency can access the data. In the event a breach occurs, notify users

- ✓ **Minimization**: Minimize the data collected to only the information that is necessary to identify contacts and keep them safe. We also need to make sure that data collected for a public health crisis is only retained while responding to that crisis and no longer. Adopting measures to delete data on a rolling basis will also help minimize data vulnerability.

- ✓ **Anonymization**: Given the sensitive information collected, not only must the data that is collected be minimal, but it should also be as anonymous as possible. This includes only sharing necessary information with contact tracers, such as the names and contact information for anyone that needs a follow-up call without sharing information about *who* tested positive. Additionally, the database hosting all the information collected should be stripped of as many identifying details as possible.

- ✓ **Voluntariness**: Keep the process voluntary. In order to gain the trust of the public, it is essential to encourage them to participate in contact tracing efforts without mandating it. History has taught us that when a program becomes mandatory or enforcement mechanisms are adopted, people are less like to comply or cooperate. This could mean that people will stop answering calls or texts, share misinformation, or otherwise refuse to cooperate making it ineffective.

- ✓ **Oversight:** Build in mechanisms to assess the effectiveness and impact of the contact tracing system. Given the magnitude of the effort, there is an inherent risk associated with collecting this level and type of data. As such, the government needs to proactively develop an accountability mechanism, such as identifying an independent agency or organization to oversee the implementation and impact of the system. This includes developing touchpoints with privacy and public health experts to help assess the system's efficacy and security

- ✓ **Transparency**: Remain transparent about who the vendor, or company, is that the government has contracted with, what information is being collected, who is able to access that information, how long the information is being stored, and other information about the contact tracing process that implicates the public.

- ✓ **Non-punitive**: No contact tracing model should be used for punitive measures or criminalize behavior. Instead, the focus should always remain on public health and helping people who have been exposed with resources that will keep them safe.

Safeguards to build a successful and secure manual contact tracing model:

In order to make sure that a manual contact tracing model remains privacy-protective, there are additional considerations that can help safeguard the process. Namely, in addition to the principles laid out earlier, consider the following questions when developing a manual contact tracing system:

Data Collection: How will the data be collected?

This element focuses on the actual collection of data. It is imperative that contact tracers are trained on how to seek the appropriate amount of information from people during their calls, while remaining cognizant of HIPAA and other privacy sensitivities.

- ✓ The government should identify how callers will take notes during their calls. Is all the data collected immediately stored in a database? Is it encrypted? Are there other permitted ways to take notes? What security concerns exist with other mechanisms?

  > **Recommendation: Make sure that notes are exclusively collected and stored in a secure system. Specifically, it should be used for the sole purpose of collecting information during contact tracing calls and not be stored on personal computers, written down in personal notebooks, or have the ability to be emailed.**

- ✓ Since the manual process provides people with the opportunity to talk to someone, callers should also be prepared to answer questions and share resources.

Data Storage: How will the data be stored? Who will have access to the stored data?

- With a given databased provided by a private entity, there are generally two models of data storage available: (1) the government can store the data on the company/vendor servers or (2) they can purchase the software from the vendor, who then supports the government and trains users on how to collect and store data. In this second model, the government stores the data on their own servers.

  > **Recommendation: Opt for (2), in which the government is trained on how to operate the system but maintains all records on their server without third-party access.**

- The government should also make sure there are additional controls in place to make sure that no third party or other private actor is able to see the names of IL residents, their addresses, or other health information stored in any database.
- In the event data is stored in an external, third party server, there must be robust security measures on the data that limits access to the information. The government should take affirmative steps to maintain boundaries between the public and private sector, such as limiting access management.

Recommendation: Regardless of where the database is stored (on an internal or external server), the government should maintain an "access log" that identifies who access what data at what time. This process helps establish a paper trail for the time period during which data is collected and makes it easier to identify possible weaknesses in security, tampering with data, or gaps in record keeping. It is also helpful in making sure everyone that needs to be contacted is contacted.

Data Usage: How will the data be used?

- The government must make sure that people are given a meaningful opportunity to understand what contact tracing is how information they are sharing will be used.

  Recommendation: Clearly state on a website, app, text message, or call what information is being sought, how it will be used, how long it will be stored, and seek the callers consent to proceed. This process of seeking informed consent will help build trust because people will have a clear understanding of the purpose and role of the contact tracing system.

- Similarly, limit the access and use of the data to public health purposes and make sure it isn't use for enforcement purposes. Answering a contact tracing call and sharing information 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 that can lead to them not answering the phone, sharing misinformation or otherwise not cooperating out of fear of harassment or other punitive measures.

  Recommendation: Establish a firewall between agencies to make sure data cannot be shared with other non-public health government agencies or third parties.

Data Destruction: How will the data that is collected be destroyed? When will it be deleted?

- Information that is collected should not be retained for any period longer than what is necessary. This means that the government needs to develop a data retention and destruction plan that is fixed and reliable in order to hold itself accountable.

  Recommendation: Develop and adopt a rolling deletion protocol. This means that data entered into a system will be deleted after a defined time period, such as four or six weeks. By establishing a rolling plan to delete records, the government does not have to worry about retaining a large dataset that can be vulnerable to hacks throughout the duration of the pandemic.

Data Security: How will the database be secure? What privacy and security measures will be in place to assess the level of threat to a system?

- Given the large amount of data that will be collected, it is critical for any database hosting this data be secure and privacy-protective. While there are back-end measures a developer will be responsible for producing, the government needs to hold the private entity to the same standards in this public-private partnership.

Recommendation: Publicly document the data systems that will be relied upon to host the data. This does not mean publishing the data itself. Instead, document what sets of data are collected, what happens to them once collected, who is able to see the different kinds of data, what type of backup structure is in place, and additional mechanisms or processes related to the information collected.

- Even the most secure system can become vulnerable to access and usage threats. It is imperative to anticipate possible threats and develop a plan that includes security measures to follow-up on any threats that may come up.

Recommendation: Develop a threat model that anticipates what "threats," or things that could go wrong when utilizing the technology and identify how the government plans to address those threats.

  - This includes both internal and external threats, such as: contact tracers sharing confidential information with their friends and family, or identity thieves trying to break into the government database.
  - The threat model should also state how it is addressing the identified threats. For example, is it adding a firewall to limit access to the data? Will only specific users be granted access to certain parts of the database? Will the government be relying on the vendor's security system and privacy protocols to protect the database from external threats?
  - A threat model should be created and shared publicly to highlight security and quality assurance measures the government is taking when implementing a robust contact tracing system.

Concerns associated with a TACT model

- While a number of technology-assisted models have been proposed, none of them are able to embody all the principles we've identified and be effective at the same time.
- Since there is a strong manual contact tracing model that can be both effective in limiting the spread of COVID-19 while remaining privacy-protective, it is critical to focus our resources on those efforts without getting distracted by tech-assisted models.
- This doesn't mean that a tech-assisted model may never be helpful. It just means that right now, resources should not be diverted from public health needs to fund the exploration or implementation of a TACT model. In order to get to a point where you can consider a TACT model, like a location-based or proximity-based system, you need to make sure you have:

- ✓ A robust public health infrastructure, including –
  - Widespread testing that is accessible and accurate;
  - Fully-staffed hospitals with enough equipment to accommodate patients; and
  - Resources for people to safely self-isolate.
- ✓ A privacy-protective TACT model, which is built with the principles we laid out –
  - Robust Security; Minimization; Anonymization; Voluntariness; Oversight; Transparency; Non-punitive

Contact tracing will be an evolving process that responds to the concerns raised by the public health crisis. As such, it is critical to maintain a dialogue with us to help make sure the effort continues to be rolled-out thoughtfully, in a privacy-protective manner that represents the best use of government resources.

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