NNEDV

Contact Tracing & Privacy: A Guide for Survivors

Contact Tracing – An Overview

Contact tracing is a public health process that's been around for many years, and is used by health departments to help slow the spread of highly contagious diseases. Contact tracing has become a very popular topic as the United States continues to respond to the COVID-19 pandemic. The contact tracing process begins when a public health department is notified of positive cases of disease through lab results or when they are reported by doctors. Here is the general process:

1. A public health worker interviews someone who's received a positive diagnosis, and works to identify all the people they've had close contact with while they were contagious.

2. Next, the public health department notifies the people who were potentially exposed, *without* revealing the infected person's identity. This notification usually happens through phone calls, but may happen through text, email, video conference, or in person.

3. When the public health department connects with the person who may have been exposed, they give them information on how they can help prevent further disease spread, and how they can take care of themselves. This usually includes how to:
    - Self-quarantine for the recommended amount of time,
    - Get tested,
    - Monitor symptoms, and
    - Discuss options for how to get food and health care while quarantining.

Many people from communities who are marginalized, including survivors, have serious concerns about privacy and how information collected in the contact tracing process

may be used against them. The Centers for Disease Control (CDC) encourage local health departments to make contact tracing a voluntary process, and urge them to make sure the information collected is protected from outside disclosure or use. However, during the COVID-19 pandemic, some local governments have tried to force individuals to share information with contact tracers, creating financial penalties for those who don't.

If you have concerns about how the process works, reaching out to your local public health department for up to date and accurate information about the process can be helpful. You can ask:

- What information is collected,
- How it is used,
- Who has access to it, and
- What steps are being taken to ensure the only people who can access it are health officials working to prevent disease spread.

Many have websites that provide detailed information. Other helpful resources include the National Academy for State Health Policy's interactive map that provides details about contact tracing efforts in the 50 states. The CDC also offers a search tool to find resources created by local health departments in the 56 states and territories. For information related to the COVID-19 response in Indian Country, reach out to your local tribal government.

Not Contact Tracing, But Related…

In response to the COVID-19 pandemic, some communities now require local businesses to collect information about customers, so that they can get in touch with them if someone who was there at the same time tests positive. **Using visitor logs at non-profits, restaurants, or public transit stops is NOT contact tracing, but it IS preparation for contact tracing.** Similarly, government-issued forms that ask travelers from out of the area to quarantine and to tell them a local address where they are staying is also NOT contact tracing. Because this information is not being collected by public health

professionals, it may be more difficult to figure out how it will be stored and protected, or if it will be used for other purposes. The best way to learn more on this is to check your local laws and regulations to learn more about what is required. Advocates at your local victim service agency may be able to help you do this.

It also may be helpful to ask the person who is trying to collect your information. Some questions you may want to ask to help you determine if it's safe for you to participate are:

- Who will have access to this information?
- How and where is it stored?
- How is it protected?
- What rights do I have to opt out of the data collection?

One strategy a survivor might use is to provide a pseudonym and a Google Voice number, so that you can participate in the prevention process without compromising your privacy. Before doing that, it will be important to assess if there are any legal penalties for masking your identity in the tracking efforts.

Contact Tracing Apps – An Overview

At the beginning of the COVID-19 pandemic, the federal government encouraged technology companies and local governments to develop contact tracing apps to help slow the spread. Some government and health officials see contact tracing apps as more effective than person-based contact tracing, because with COVID-19, the disease is spread through the air, and so people can easily infect others who they do not know. App based contact tracing helps in situations like this because the app keeps track of who you've been near, even if you don't know the people (like when you pass strangers at the grocery store).

A major concern about contact tracing apps is that many people who can't afford the technology or do not feel safe using the technology, will not reap the benefits of it, and

will not be able to interrupt the spread of disease. There are also many people who are suspicious about how data from these apps may be used against marginalized communities, like undocumented immigrants. Many people are concerned that sharing private health information with major tech companies and government officials could put their privacy and liberty at risk, because the apps would show who they've been in contact with, where they've been, and who they know.

If you are a survivor of domestic violence, sexual assault, or stalking and are curious about what privacy considerations there are with such apps, check out the tips below that can help you assess an app's privacy practices and security features too see if it meets your unique needs.

Privacy Protective Contact Tracing Apps

When you start to look into contact tracing apps you will frequently come across the term "API", which stands for Application Programming Interface. APIs are the tools that tech companies use to create apps. An API is basically a set of instructions that lists what information on the device an app is allowed to access, and rules for how it's allowed to operate.

One of the most privacy protective APIs on the market is the Apple-Google API, known as Exposure Notification. Apps built using the Exposure Notification API have special privacy features that may be helpful for survivors:

- Apps built with the Exposure Notification API can be turned off whenever the user wants.
- To track possible exposures, apps built with the Exposure Notification API do not track or use GPS location. Instead, they generate random Bluetooth identifiers (numerical codes) that change every 15 minutes. When the app is turned on, it records the codes from other devices it gets close to that also have the app installed and turned on.

- ☐ Apps built with the Exposure Notification API do not automatically share personal information with public health authorities, Apple, Google, or other users. Information is only stored on your device. If you test positive, you can press a button in your phone that will then notify the people you've been near that they may have been exposed. The app will not provide any personal information about you to the people it notifies.

    - ***NOTE:*** There is always a risk that someone could figure out it was you, if the person tries to narrow down who they were in contact with recently. If they've only been around you and no other people, they may be able to figure out who exposed them.

- The Exposure Notification API can only be used to assist in contact tracing efforts. Google and Apple will disable it when the pandemic is over.

Check out this article for a list of states that are using the Exposure Notification API.

Additional Considerations for Exposure Notification API Based Apps

There are some other important considerations related to Exposure Notification API based apps. For instance, the Bluetooth signal can vary depending on the kind of device you have and what's around you. If something blocks the signal, an exposure may not be registered. On the other hand, if there is a strong signal that goes through a wall separating two apartments, it may register an exposure when none actually existed. And of course, the apps don't account for people wearing personal protective equipment, so you may get notified that you were exposed when you actually were pretty safe.

Assessing an App's Privacy & Security

The Exposure Notification API isn't the only API out there for app developers to build a contact tracing app on. There are many others they can choose from, and it would be

impossible to review all of them here. But there are general tips to consider if you're trying to figure out if an app works well for your privacy needs.

The best place to start is to look at the website for the app. These websites often have frequently asked questions that will help you get a better understanding of how the app works and what privacy and security features are available. This information should also be laid out in the privacy policy, but these can sometimes be written in a way that's complicated to understand. Questions to explore that can help you get an idea of if it's safe for you to use the app or not include:

- Does the app require you to create an account or enter any personally identifying information?
- Can you turn the app on and off?
- Does the app use GPS to track your location?
- What data does the app collect?
- How is it being collected?
- Where is it stored? (On the device? In an account? Where else?)
- Who has access to it?
- Is there a way an abusive person could access that data?
- Are the benefits worth the risk?

Privacy issues vary from app to app. Some apps may share location and user information with third party businesses. Others use GPS location tracking and store information on cloud-based servers instead of on the device, making them more at risk of breach.

For any survivor interested in contact tracing, it is always important to understand the risks and limitations to sharing medical information, location information and other identifiable details about themselves. While there are general privacy risks for any user, survivors of domestic violence must use extra caution when safety planning and using these types of apps.

 Supported by US DOJ-OVW Grant #2019-TA-AX-K003. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ.

We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.