Rastreo de contactos y privacidad:
Una guía para sobrevivientes

Rastreo de contactos: resumen

El rastreo de contactos es un proceso de salud pública que ha existido durante muchos años, y se lo utilizan los departamentos de salud para ayudar a reducir la propagación de enfermedades altamente contagiosas. El rastreo de contactos se ha convertido en un tema muy popular a medida que los Estados Unidos sigue respondiendo a la pandemia de COVID-19. El procedimiento de rastreo de contactos comienza cuando un departamento de salud pública recibe un aviso de casos positivos de la enfermedad mediante resultados de análisis de laboratorio o cuando son informados por médicos/as. A continuación se describe el proceso general:

1. Un/a trabajador/a de salud pública entrevista a una persona que recibió un diagnóstico positivo, por lo cual intenta identificar a todas las personas con las que tuvo contacto estrecho mientras era contagiosa.

2. A continuación, el departamento de salud pública notifica a las personas que estuvieron potencialmente expuestas, *sin* revelar la identidad de la persona infectada. Esta notificación normalmente se realiza por teléfono, pero también puede hacerse por mensaje de texto, correo electrónico videoconferencia o en persona.

3. Cuando el departamento de salud pública se pone en contacto con la persona que potencialmente estuvo expuesta, le brinda información sobre cómo pueden ayudar a prevenir que se siga propagando la enfermedad y cómo cuidarse. Esto normalmente incluye lo siguiente:
    - ponerse en cuarentena durante el tiempo recomendado;
    - someterse a una prueba;
    - controlar los síntomas; y

- analizar opciones sobre cómo comprar alimentos y acceder a atención médica durante la cuarentena.

Muchas personas de comunidades que han marginadas, incluidos los/las sobrevivientes, tienen serias preocupaciones sobre la privacidad y sobre cómo se recolecta información en el proceso del rastreo de contactos que podría utilizarse en su contra. Los Centros para el Control y Prevención de Enfermedades (CDC) animan a los departamentos de salud pública a establecer que el rastreo de contactos sea un proceso voluntario, y les piden que garanticen que la información recopilada esté protegida del uso o la divulgación fuera de ellos. Sin embargo, durante la pandemia de COVID-19, algunos gobiernos locales han intentado obligar a los individuos a compartir información con los to agentes de rastreo de contactos, lo que provoca que se impongan sanciones económicas para quienes no lo hacen.

Si tiene preocupaciones respecto de cómo funciona el proceso, es útil comunicarse con su departamento local de salud pública para obtener información precisa y actualizada del proceso. Puede hacer las siguientes preguntas:

- qué información se recopila;
- de qué manera es utilizada;
- quién tiene acceso a ella; y
- cuáles son las medidas que se están adoptando para garantizar que las personas que pueden acceder a ella sean exclusivamente funcionarios/as de salud que trabajan para prevenir la propagación de la enfermedad.

Muchos departamentos tienen sitios web que proporcionan información detallada. Otro recurso útil es el mapa interactivo de la National Academy for State Health Policy, que proporciona detalles acerca de los esfuerzos de rastreo en 50 estados. Los CDC también ofrecen una herramienta de búsqueda para encontrar recursos creados por los departamentos locales en los 56 estados y territorios. Para obtener más información

acerca de la respuesta al COVID-19 en el territorio indio, comuníquese con su gobierno tribal local.

No es acerca del rastreo de contactos, pero está relacionado…

En respuesta a la pandemia de COVID-19, algunas comunidades exigen actualmente a los negocios locales que recopilen información sobre los clientes, de forma tal que puedan comunicarse con ellos si alguien que estuvo allí a la misma hora obtuvo un resultado positivo en la prueba. **Usar los registros de los/las visitantes en entidades sin fines de lucro, restaurantes o transporte público NO es rastreo de contactos, pero SÍ es la preparación para el rastreo de contactos.** De manera similar, los formularios emitidos por el gobierno que solicitan a los/las viajeros fuera del área que se pongan en cuarentena y que indiquen el domicilio local donde residirán ese tiempo NO son un rastreo de contactos. Debido a que esta información no está siendo recolectada por profesionales de la salud pública, puede ser más difícil determinar cómo se almacenará, protegerá o si se utilizará para otros propósitos. La mejora manera para conocer más acerca de esto es consultar las normas y leyes locales para obtener más información sobre cuáles son los requisitos. Los/las intercesores/as de su agencia local de servicios a las víctimas puede ayudarlo.

También puede ser útil preguntarle a la persona que intenta recopilar su información. A continuación detallamos algunas preguntas que tal vez quiera hacer para ayudarlo a determinar si es seguro que participe:

- ¿Quién tendrá acceso a esta información?
- ¿De qué manera y dónde estará almacenada?
- ¿Cómo está protegida?
- ¿Qué derechos tengo si decido no participar en la recopilación de datos?

Una estrategia que un/a sobreviviente puede usar es proporcionar un seudónimo y un número de Google Voice, de forma que pueda participar en el proceso de prevención

sin comprometer su privacidad. Antes de hacerlo, es importante analizar si existen sanciones legales por ocultar su identidad en el esfuerzo de rastreo.

Aplicaciones de rastreo de contactos - Resumen

Al inicio de la pandemia de COVID-19, el gobierno federal animó a las empresas de tecnología y a los gobiernos locales a desarrollar aplicaciones de rastro de contactos para ayudar a disminuir la propagación. Algunos gobiernos y funcionarios/as de salud consideran que las aplicaciones de rastreo de contactos son más efectivas que el rastro basado en persona ya que,con el COVID-19, la enfermedad es de transmisión aérea, y las personas pueden fácilmente infectar a otras que no conocen. El rastreo de contactos a través de aplicaciones es útil en situaciones como esta porque la aplicación lleva un registro de las personas que estuvieron cerca de usted, incluso si no los/las conoce (por ejemplo, cuando pasa al lado de un desconocido en el supermercado).

Una gran preocupación respecto de las aplicaciones de rastreo de contactos es que muchas personas no pueden afrontar el costo de la tecnología o no se sienten seguros/as usándola, que no percibirán beneficios, y que no lograrán interrumpir la propagación de la enfermedad. También hay muchas personas que desconfían de que los datos obtenidos en estas aplicaciones pueden ser utilizados contra las comunidades marginadas, como los inmigrantes indocumentados. A muchas personas les preocupa que la divulgación de información de salud privada a través de empresas de alta tecnología y funcionarios/as del gobierno podría poner en riesgo su privacidad y libertad, ya que mostrarían con quiénes estuvieron en contacto, dónde estuvieron y a quiénes conocen.

Si usted es un/a sobreviviente de violencia doméstica, agresión sexual o acecho y le interesa saber sobre las consideraciones de privacidad de tales aplicaciones, los siguientes consejos pueden ayudarlo/a a evaluar las prácticas de privacidad y características de seguridad de una aplicación con el fin de determinar si cumple con sus necesidades exclusivas.

Aplicaciones de rastreo de contactos que protegen la privacidad

Cuando comienza a analizar las aplicaciones de rastreo de contactos, encontrará frecuentemente el término “API”, que significa Interfaz de programación de aplicaciones. Las API son herramientas que las empresas de tecnología utilizan para crear aplicaciones. Una API es básicamente un conjunto de instrucciones que detalla a qué información en el dispositivo puede acceder una aplicación, y las reglas sobre cómo están autorizadas a operar.

Una de las API con la mayor protección de la privacidad es Apple-Google API, conocida como Exposure Notification. Las aplicaciones desarrolladas utilizando la API Exposure Notification cuentan con características especiales de privacidad que pueden ser útiles para los/las sobrevivientes:

- Las aplicaciones desarrolladas con la API Exposure Notification pueden ser deshabilitadas en cualquier momento que el usuario lo desee.
- ☐ Para rastrear posibles exposiciones, las aplicaciones desarrolladas con la API Exposure Notification no rastrean ni usan ubicación GPS. En cambio, generan identificadores Bluetooth aleatorios (códigos numéricos) que cambian cada 15 minutos. Cuando se enciende la aplicación, registra los códigos de otros dispositivos cercanos que también tienen la aplicación instalada y activa.
- ☐ Las aplicaciones desarrolladas con la API Exposure Notification no comparten información personal automáticamente con autoridades de salud pública, Apple, Google u otros usuarios/as. La información solo está almacenada en su dispositivo. Si el resultado de su prueba es positivo, puede presionar un botón en su teléfono que notificará a las personas que estuvieron cerca suyo que podrían haber estado expuestas. La aplicación no brindará su información personal a las personas a quienes notifica.

- ***AVISO:*** Siempre existe un riesgo de que una persona pueda descubrir que fue usted, si la persona intenta limitar los individuos con quienes estuvieron en contacto recientemente. Si solo tuvieron contacto con usted y nadie más, podrían descubrir quién los expuso.

- La API Exposure Notification solo puede ser utilizada para colaborar con los esfuerzos de rastreo de contactos. Google y Apple la deshabilitarán cuando finalice la pandemia.

Consulte este artículo para obtener una lista de estados que están utilizando la API Exposure Notification.

Consideraciones adicionales de las aplicaciones basadas en la API Exposure Notification

Hay otras consideraciones importantes relacionadas con las aplicaciones basadas en la API Exposure Notification. Por ejemplo, la señal de Bluetooth puede variar en función del tipo de dispositivo que tiene y qué cosas lo rodean. Si algo bloquea la señal, tal vez no se registre una exposición. Por otro lado, si la señal es fuerte y atraviesa una pared que separa dos departamentos, podría registrar una exposición que no sucedió. Y obviamente, las aplicaciones no tienen en cuenta las personas que usan equipo protector personal, por lo cual pude recibir una notificación de que estuvo expuesto cuando, en realidad, estuvo muy seguro/a.

Evaluar la privacidad y seguridad de una aplicación

La API Exposure Notification no es la única disponible para los desarrolladores de aplicaciones para crear una aplicación de rastreo de contactos. Existen muchas otras que puede elegir, y sería imposible analizarlas a todas aquí. Sin embargo, hay consejos generales para tener en cuenta si está buscando una aplicación que satisfaga sus necesidades de privacidad.

El mejor lugar para empezar a buscar es el sitio web de la aplicación. Los sitios web suelen tener una sección de preguntas frecuentes que lo ayudarán a comprender mejor cómo funciona la aplicación y qué características de seguridad y privacidad están disponibles. Esta información debería estar detallada en la política de privacidad, pero algunas veces tales políticas están escritas de una forma difícil de comprender. Las preguntas para explorar que pueden ayudarlo a tener una idea de lo que es seguro para que utilice o no la aplicación incluyen:

- ¿Requiere la aplicación que cree una cuenta o ingrese información personal identificable?
- ¿Es posible prender y apagar la aplicación?
- ¿Utiliza GPS para rastrear la ubicación?
- ¿Qué datos recopila?
- ¿De qué manera los recopila?
- ¿Dónde estará almacenada? (¿en un dispositivo? ¿en una cuenta? ¿en qué otro lugar?)
- ¿Quién tiene acceso?
- ¿Existe alguna forma en que una persona abusiva pueda acceder a los datos?
- ¿Los beneficios superan a los riesgos?

Las cuestiones de privacidad varían en función de la aplicación. Algunas aplicaciones pueden compartir la ubicación y la información del usuario con otras empresas. Otras utilizan el rastreo de ubicación GPS y almacenan información en servidores en la nube en lugar de hacerlo en un dispositivo, lo cual resulta en un mayor riesgo de violación.

Para cualquier sobreviviente interesado en el rastreo de contactos, siempre es importante comprender los riesgos y las limitaciones al compartir información médica, información de ubicación y otros detalles identificables personales. Si bien hay riesgos generales de la privacidad para cualquier usuario, los/las sobrevivientes de violencia

doméstica deben tener mayor precaución al realizar el plan de seguridad y utilizar este tipo de aplicaciones.

 Financiado por US DOJ-OVW subvención n.° 2019-TA-AX-K003. Las opiniones, los hallazgos, las conclusiones o las recomendaciones aquí expresados pertenecen a el/la autor/a y no necesariamente reflejan los puntos de vista del Departamento de Justicia (DOJ, por sus siglas en inglés).

Actualizamos nuestro material con frecuencia. Visite TechSafety.org para obtener la última versión de este y otros materiales.