Las compañías tecnológicas Apple y Google, unieron sus fuerzas para desarrollar una herramienta interoperable de rastreo de contratos que ayudará a las personas a determinar si han entrado en contacto con alguien infectado con COVID-19.

Como parte de esta nueva iniciativa, se espera que las compañías publiquen una API que las agencias públicas pueden integrar en sus aplicaciones. La próxima jugada será una plataforma de nivel de sistema incorporada que utiliza balizas Bluetooth de baja energía (BLE) para permitir el rastreo de contactos de forma opcional.

Se espera que las API estén disponibles a mediados de mayo para Android e iOS, con el sistema de seguimiento de contactos más amplio listo para implementarse *«en los próximos meses»*.

> *«La privacidad, la transparencia y el consentimiento son de suma importancia en este esfuerzo, y esperamos construir esta funcionalidad en consulta con las partes interesadas»*, dijeron las compañías.

La rara colaboración se produce cuando los gobiernos de todo el mundo recurren cada vez más a la tecnología, como el seguimiento telefónico y el reconocimiento facial para combatir el virus y contener el brote del coronavirus.

Apple también lanzó una nueva página web que anuncia la función, y detalla las especificaciones perliminares de Bluetooth, las especificaciones de criptografía y la API marco, en la que se basará el sistema de seguimiento de contactos.

A diferencia de las aplicaciones existentes desarrolladas por distintos países que utilizan el seguimiento de ubicación en tiempo real para hacer cumplir las reglas de cuarentena, el sistema propuesto no implica el seguimiento de las ubicaciones de los usuarios u otros datos de identificación.

En cambio, aprovecha las balizas BLE para identificar si su individuo ha estado cerca de otras

personas que han dado positivo COVID-19, asegurando así que la privacidad personal no se vea comprometida.

Tanto Apple como Google han enfatizado que los usuarios deberán proporcionar su consentimiento explícito para que funcione. Esto también significa que para que sea efectivo, millones de personas necesitarían saber que Apple y Google deberán salvaguardar la privacidad de los usuarios.

Según un documento técnico publicado por Google, así es como podría funcionar un sistema de este tipo:

- Cuando dos personas entran en contacto cercano durante un cierto período de tiempo (por ejemplo, 10 minutos o más), sus teléfonos intercambiarán balizas de identificación anónimas. Los identificadores rotan cada 15 minutos y no tienen información de identificación personal.
- Si uno de los dos es diagnosticado positivamente para COVID-19, esa persona infectada puede ingresar el resultado de la prueba en una aplicación de una autoridad de salud pública que ha integrado el API mencionado anteriormente.
- Luego, la persona infectada puede dar su consentimiento para cargar los últimos 14 días de sus balizas de transmisión al sistema.
- Cualquier otra persona que haya estado muy cerca de la persona que recibió el resultado positivo recibirá una alerta si existe una señal para el dispositivo que coincida con las señales de transmisión de todos los que dieron positivo para COVID-19 en la región.
- La aplicación luego proporciona al individuo información sobre los próximos pasos.

> *«Este modelo podría crear menos confianza en una autoridad central, a la vez que crea nuevos riesgos para los usuarios que comparten su estado de infección que debe ser mitigado o aceptado»,* dijo la Electronic Frontier Foundation (EFF).

> *«La transparencia total sobre cómo funcionan las aplicaciones y las API, incluido el código fuente abierto, es necesaria para que las personas comprendan y den su consentimiento informado a los riesgos»,* agregó.

El sistema de Apple y Google está en la línea de TraceTogether, una aplicación desarrollada por funcionarios del gobierno de Singapur para permitir el rastreo de contactos por medio de Bluetooth.

La aplicación, que ahora es de código abierto, utiliza lecturas del indicador de intensidad de la señal relativa de Bluetooth (RSS) entre dispositivos para determinar la proximidad y la duración de un encuentro entre dos personas. Los registros de encuentros se almacenan en sus respectivos teléfonos durante 21 días.

Aplicaciones como COVID-Watch y el Kit privado del MIT: Safe Paths, del mismo modo, se basan en una combinación de datos de GPS y Bluetooth para rastrear a las personas que se han cruzado con otras personas durante un período de 14 días.

Además, un grupo de académicos de instituciones de investigación europeas ha propuesto un sistema descentralizado para el rastreo de contactos COVID-19 basado en Bluetooth, denominado *«Rastreo de proximidad para preservar la privacidad descentralizada»* (DP-PPT), cuyo objetivo es *«minimizar los riesgos de privacidad y seguridad para las personas y comunidades y garantizar el más alto nivel de protección de datos».*

La necesidad de identificar a las personas infectadas y mantener las cuarentenas ha llevado a los gobiernos de todo el mundo a adoptar medidas estrictas de vigilancia. Hasta el momento, más de 28 países han adoptado una combinación de rastreo de teléfonos inteligentes, pulseras de rastreo electrónico, e incluso requieren que los ciudadanos envíen una foto de sí mismos a sus hogares en 20 minutos o que enfrenten una multa.

En respuesta a las preocupaciones de privacidad planteadas por el Supervisor Europeo de Protección de Datos, la Unión Europea afirmó que adoptaría un *«enfoque panaeuropeo»* para

utilizar aplicaciones móviles para rastrear la propagación del coronavirus e incluir un esquema común para usar datos agregados anónimos para rastrear a las personas que entran en contacto con las personas infectadas y controlar a las personas en cuarentena.

A inicios de la semana, la Unión Americana de Libertades Civiles (ACLU), expresó su preocupación por el seguimiento de los usuarios con datos telefónicos agregados, argumentando que cualquier sistema tendría que tener un alcance limitado y evitar posibles invasiones de privacidad y abuso.

Aunque países como Corea del Sur han podido minimizar el brote por medio de un extenso programa de seguimiento de contactos, también plantea preguntas sobre el consentimiento, como por ejemplo si los usuarios pueden optar por no participar antes de que se recopilen y almacenen esos datos, sin mencionar el peligro potencial de cambio hacer la vista gorda a sus riesgos de privacidad.

El experto en seguridad cibernética Bruce Schneier dijo que cualquier iniciativa de recopilación de datos y monitoreo digital *«debe estar científicamente justificada y ser considerada necesaria por expertos en salud pública con el propósito de contenerla. Y que el procesamiento de datos debe ser proporcional a la necesidad».*

Instando a la necesidad de proteger las libertades civiles durante la crisis, el FEP dijo que se justifica eludir ciertas protecciones de privacidad, pero advirtió que *«cualquier medida extraordinaria utilizada para manejar una crisis específica no debe convertirse en elementos permanentes en el panorama del gobierno intrusiones en la vida diaria».*

Dicho de otra forma, estos programas no deberían allanar el camino para la extralimitación del gobierno o los sistemas de monitoreo draconianos que seguirán viviendo incluso después de que el brote actual haya desaparecido. Incluyendo fuertes garantías de privacidad son los medios correctos para garantizar que las medidas de emergencia no se convierten en la nueva normalidad.