

Google instala un programa de seguimiento de vacunas en su teléfono

Análisis escrito por [Dr. Joseph Mercola](#)

✓ Datos comprobados

HISTORIA EN BREVE

- › El Departamento de Salud Pública de Massachusetts se asoció con Google y Apple para crear una aplicación para teléfonos inteligentes llamada MassNotify, que rastrea y localiza a las personas, y además les informa a los usuarios sobre el estado de COVID-19 de los demás
- › Los residentes de Massachusetts se alarmaron cuando el software apareció en sus teléfonos sin su consentimiento o notificación, lo que generó preocupaciones sobre la privacidad y el software espía
- › En China, las aplicaciones de rastreo de COVID-19 se han utilizado como herramientas de vigilancia en colaboración con su sistema de crédito social, lo que genera señales de alerta de que esta aplicación de instalación forzada podría rastrear los movimientos y contactos de los residentes sin su conocimiento ni consentimiento
- › Google es una agencia de vigilancia y censura que tiene la capacidad de restringir o bloquear el acceso a sitios web a través de Internet, al decidir lo que las personas pueden ver
- › Las protestas pacíficas funcionan para proteger la privacidad y la libertad personal; si es residente de Massachusetts y no está satisfecho con el hecho de que se haya agregado un software de vigilancia a su teléfono celular sin su consentimiento, ahora es el momento de levantar la voz

El Departamento de Salud Pública de Massachusetts se asoció con Google y Apple para crear una aplicación para teléfonos inteligentes llamada MassNotify, que rastrea y localiza a las personas, y además les informa a los usuarios sobre el estado de COVID-19 de los demás.

Para ser una herramienta que dice haber sido desarrollada "con un enfoque en la privacidad", imagine la sorpresa de los residentes de Massachusetts cuando la aplicación apareció de improvisto en sus teléfonos Android. En una reseña en Google Play Store, un padre sorprendido dijo:

"Se instaló en silencio en el teléfono de mi hija sin consentimiento ni notificación. Es imposible que ella misma la haya instalado ya que usamos Family Link y tenemos que aprobar todas las instalaciones de aplicaciones.

No tengo idea de cómo lograron esto, pero supongo que Google, Samsung o ambos están involucrados. Las aplicaciones normales no se pueden instalar solas. No estoy seguro de lo que sucede aquí, pero esto no cuenta como "voluntario". Necesitamos información, y la necesitamos ahora amigos".

El sitio oficial de MassNotify, operado por el Departamento de Salud Pública de Massachusetts, no menciona que la aplicación aparecerá de forma automática en los teléfonos de los residentes sin consentimiento, y solo indica que MassNotify es una "nueva herramienta que funciona a través de teléfonos inteligentes, con un enfoque en la privacidad, para alertar a los usuarios que podrían haber estado expuestos al COVID-19".

De acuerdo con la información, el usuario debe habilitar la aplicación para que funcione, pero es muy desconcertante que la herramienta se haya agregado de forma automática a los teléfonos de las personas, ya sea que tengan la intención de usarla o no.

Los residentes están alarmados por un 'software espía' y 'extralimitación gubernamental'

Los usuarios de teléfonos Android se alarmaron cuando MassNotify apareció en sus dispositivos. La herramienta "no tiene un icono de aplicación", comentó una persona en Google Play, "es necesario entrar a la configuración y ver todas las aplicaciones. Esta es una violación a la privacidad y seguridad por parte del [gobernador Charlie Baker] y Google".

Otras personas también lo describieron como "software espía", mientras que un usuario de Hacker News escribió: "Es una auténtica locura que Play Services tenga este tipo de plan secreto. Esto es justo lo que yo consideraría una vulnerabilidad deliberada".

En China, las aplicaciones de rastreo de COVID-19 se han utilizado como herramientas de vigilancia en colaboración con su sistema de crédito social, lo que genera señales de alerta de que esta aplicación de instalación forzada podría rastrear los movimientos y contactos de los residentes sin su conocimiento ni consentimiento. Las reseñas en Google Play Store llegaron de personas preocupadas por que **violaron su privacidad**, con comentarios como:

- *"Se instala automáticamente sin consentimiento. No tiene ícono, no hay forma de abrir esto y ver lo que hace, lo cual es una señal de alerta. Creo que es software espía o un fraude electrónico como el Departamento de Salud Pública (DPH)".*
- *"Instalación forzada sin autorización ni aprobación. La aplicación está oculta en el dispositivo para evitar que las personas la desinstalen. La extralimitación del gobierno y la complicidad empresarial es algo que nunca se deben tolerar".*
- *"Es una violación poco ética de la privacidad y uso indebido por la fuerza de la propiedad personal. El grado en que mis datos se recopilan o distribuyen a través de ellos no se han revelado en forma activa ni inactiva. Solo puedo concluir y advertir a otras personas que revelan su paradero y contactos sociales sin permiso".*

MassNotify se 'integró en la configuración del dispositivo' y es difícil de quitar

Cuando se le presionó a Google para hacer comentarios, emitió una declaración a los medios, pero no abordó el problema evidente de cómo o por qué el sistema se instaló a

la fuerza sin el consentimiento de los usuarios. En cambio, solo dijeron:

“Trabajamos con el Departamento de Salud Pública de Massachusetts para permitir a los usuarios activar el Sistema de Notificaciones de Exposición desde la configuración de su teléfono Android.

Esta funcionalidad está integrada en la configuración del dispositivo y Google Play Store la distribuye de forma automática, por lo que los usuarios no tienen que descargar ninguna aplicación por separado. Las notificaciones de exposición al COVID-19 están habilitadas solo si un usuario las enciende. Los usuarios deciden si habilitar esta funcionalidad y si desean compartir información a través del sistema para ayudar a advertir a los demás sobre una posible exposición”.

La aplicación MassNotify se lanzó el 15 de junio de 2021, lo que lo identifica como el estado número 29 en lanzar una aplicación al utilizar el programa Exposure Notifications Express de Google y Apple.

El marco de software se lanzó por primera vez en abril de 2020, con el objetivo de permitir a los usuarios que dan positivo al COVID-19 reportar sus resultados, que luego envía una alerta a cualquier persona cuyo teléfono se cruce con una persona que dio positivo y que haya estado expuesta. El programa Exposure Notifications Express actúa como un modelo por el que los estados pueden implementar sus propios sistemas de seguimiento sin tener que desarrollar sus propias aplicaciones individuales.

Mientras que otros estados han requerido que los usuarios descarguen una aplicación para usar el sistema, MassNotify se integró de forma directa en el sistema operativo de los teléfonos Android. “La función de rastreo de contactos no funciona a menos que un usuario la active de forma manual, pero tampoco puede eliminar el software”, informó el Boston Globe. “(Mientras tanto, Apple agregó la función a los iPhones hace meses, con iOS 13)”.

Massachusetts insta a los residentes a habilitar MassNotify

El Departamento de Salud Pública de Massachusetts invita a los residentes a habilitar MassNotify en sus teléfonos celulares, y la Dra. Catherine Brown, epidemióloga estatal, afirma que esperan que al menos el 15 % de la población del estado, o más de 1 millón de personas la aceptan y señala que podría ser más efectiva para las personas que frecuentan lugares de trabajo o campus universitarios muy concurridos.

Una vez que se inscribe, los códigos anónimos se comparten con otros usuarios de MassNotify a través del Bluetooth de su teléfono. Si dentro de los 14 días, entra en contacto cercano (menos de 6 pies durante al menos 15 minutos) con alguien que dio positivo, se le notificará. Si el resultado es positivo, se espera que "notifique a los demás de forma fácil y anónima para detener el contagio del COVID-19".

El sistema funciona junto con el Departamento de Salud Pública de Massachusetts, que enviará un mensaje de texto con un enlace de verificación a las personas que den positivo al COVID-19. El enlace permite a los usuarios compartir el resultado de su prueba y notificar a otros usuarios de MassNotify sobre su exposición. Para las personas que no han optado por la herramienta, el enlace también sirve como una herramienta "para ayudarlo a habilitar MassNotify en su teléfono para uso futuro".

Existen muchos riesgos de privacidad y sin precedentes

Es irónico que el Departamento de Salud Pública de Massachusetts declare que MassNotify no es una aplicación de rastreo de contratos, sin embargo, se basa en la tecnología desarrollada por Apple y Google que antes se conocía como el "Proyecto de seguimiento de contactos para preservar la privacidad" y ahora se conoce como la API de notificaciones de exposición (interfaz de programación de aplicaciones).

Un artículo de Forbes del 4 de mayo del 2020 de Simon Chandler señala que, aunque las aplicaciones "pueden ser criptográficamente seguras", aún "amenazan nuestra privacidad de formas más amplias y engañosas".

"Por un lado, los investigadores de ciberseguridad ya dijeron que los malos participantes adecuadamente determinados y malévolos podrían correlacionar a las personas infectadas con otra información personal al utilizar la API. Por

otro lado, la API de Google-Apple y cualquier aplicación basada en ella conllevan dos riesgos de privacidad mucho más generales y peligrosos".

Primero, las aplicaciones solo funcionan si mantiene su teléfono celular con usted en todo momento y con el Bluetooth habilitado. "De inmediato, esta es una pérdida de privacidad", señala Chandler. "Como lo demuestran muchos estudios e investigaciones, los teléfonos inteligentes y muchas de las aplicaciones en ellos rastrean sus ubicaciones, además de grabar y compartir cualquier información que ingrese".

El otro riesgo es que es una forma más de "normalizar" algo que es completamente anormal: el uso constante de la tecnología para determinar sus libertades y comportamiento. "[M]ientras estamos acostumbrados a los anuncios que intentan estimular el comportamiento de nuestro consumidor, las aplicaciones de rastreo de contactos normalizarán el concepto de aplicaciones que dirigen y administran a escala cómo viven y se comportan millones de personas", señaló Chandler.

Recuerde, si recibe una notificación de que ha estado en contacto cercano con alguien que dio positivo, es posible que lo pongan en cuarentena. Sin duda, muchos lo harán de forma innecesaria, ya que no terminarán enfermos, lo que significa que acaban de renunciar a 14 días de libertad sin ningún motivo.

¿Y qué pasa si termina la cuarentena y cuando sale lo vuelven a notificar de otra exposición? ¿Otros 14 días en aislamiento? Además, esta invasión aparentemente inocente tiene consecuencias muy negativas. Como dijo Chandler:

"Los usuarios se acostumbrarán a la idea de una aplicación que les diga cuándo quedarse en casa y cuándo salir. En esencia, se acostumbrarán más a delegar juicios sobre cómo deben comportarse con las aplicaciones y la tecnología digital".

Las técnicas de Google para manipular a las personas son bien conocidas

Google se ha dado a conocer como un dictador con un poder sin precedentes porque se basa en técnicas para manipular que nunca antes habían existido en la historia de la humanidad, según Robert Epstein, un psicólogo formado en Harvard que ahora es el psicólogo investigador principal del American Institute of Behavioral Research and Technology, donde durante la última década ha ayudado a exponer las prácticas manipuladoras y engañosas de Google.

No solo son una agencia de vigilancia (piense en productos como Google Wallet, Google Docs, Google Drive y YouTube), sino también una agencia de censura con la capacidad de restringir o bloquear el acceso a sitios web a través de Internet, al decidir lo que las personas pueden ver.

Google también se ha infiltrado en la educación con sus aulas de Google, cuyo uso aumentó durante la pandemia, pero muchas personas no son conscientes de que incluso también están rastreando a sus hijos. El fiscal general de Nuevo México presentó una demanda contra Google por sus herramientas educativas en aula que ayuda a "**acabar con la farsa**", dijo la profesora de Harvard Shoshana Zuboff:

"[La demanda] identifica la enorme cantidad de datos que toman sobre los niños, cómo los rastrean en Internet, si los integran con todos los demás flujos de información de Google y lo tienen como base para rastrear a todos esos niños hasta su edad adulta".

Google también respalda **Profusa**, que ha desarrollado un biosensor inyectable que permite examinar la fisiología de una persona de manera remota cuando se conecta a un teléfono inteligente. A mayor escala, Google, Amazon, Twitter y otras importantes empresas tecnológicas también están relacionadas al " complejo-militar-industrial-de-inteligencia-medios", Para citar a Edward Curtin de Off-Guardian.

Todos proporcionan funciones invaluable de vigilancia y censura, y sin ellas el sistema de control totalitario en el que ahora nos encontramos atrapados, no sería posible.

Las protestas masivas pueden terminar con las invasiones de privacidad

Como vimos en el caso de los pasaportes de vacunas, las protestas pacíficas funcionan para proteger la privacidad y la libertad personal. El Pentágono también desconectó Lifelog, un proyecto de base de datos destinado a rastrear los puntos característicos de toda la existencia de las personas con fines de vigilancia de la seguridad nacional, el 4 de febrero de 2004, en respuesta a una reacción violenta por preocupaciones de privacidad. (Aunque ese mismo día se lanzó Facebook)

Si es residente de Massachusetts y no está satisfecho con el hecho de que se haya agregado un software de vigilancia a su teléfono celular sin su consentimiento, ahora es el momento de levantar la voz. El objetivo final aquí no es rastrear los casos de COVID-19 en su ciudad natal. Los pasaportes de vacunas o cualquier otro tipo de dispositivo de seguimiento y rastreo o sistema de certificación son parte de un plan mucho más amplio para implementar un sistema de crédito social global basado en vigilancia electrónica 24 horas al día, 7 días a la semana para garantizar el cumplimiento.

Esto se expandirá para incluir no solo la infección por COVID-19 y el estado de vacunación, sino que terminará incluyendo información de personas como datos médicos, registros de identificación básicos, datos financieros y casi cualquier otra cosa que se pueda digitalizar y rastrear.

Podría significar el principio del fin de la libertad tal como la conocemos, a menos que todos, en todas partes, reconozcan el peligro y tomen medidas. La protesta pacífica y la desobediencia civil (no cumplir con las aplicaciones de rastreo, los mandatos del uso del cubrebocas, [distanciamiento social](#), [confinamientos](#), las vacunas o cualquier otra cosa) pueden ser una gran ayuda.

Fuentes y Referencias

- [Mass.gov, Enable MassNotify on your smartphone](#)
- [The National Pulse June 19, 2021](#)
- [ZeroHedge June 22, 2021](#)
- [The Verge September 1, 2020](#)
- [Boston Globe June 22, 2021](#)
- [10 WJAR June 21, 2021](#)
- [Mass.gov, Learn more about MassNotify](#)
- [Apple.com, Privacy-Preserving Contact Tracing](#)

- [Forbes May 4, 2020](#)
- [Wired April 17, 2020](#)
- [YouTube June 22, 2020](#)
- [Profusa, Our Team](#)
- [Off-Guardian February 14, 2021](#)
- [Military.com February 4, 2004](#)
- [Rapture Ready FAQ: Lifelog project](#)
- [History Facebook Launches February 4, 2004](#)