**¿Cómo funcionan las aplicaciones de proximidad?**

Hay muchas propuestas diferentes para aplicaciones de rastreo de proximidad basadas en Bluetooth, pero a un alto nivel, comienzan con un enfoque similar. La aplicación emite un identificador único a través de Bluetooth que otros teléfonos cercanos pueden detectar. Para proteger la privacidad, muchas propuestas, incluidas las[API de Apple y de Google](https://www.washingtonpost.com/technology/2020/04/10/apple-google-tracking-coronavirus/), hacen que el identificador de cada teléfono se rote con frecuencia para limitar el riesgo de seguimiento por parte de terceros.

Cuando dos usuarios de la aplicación se acercan entre sí, ambas aplicaciones estiman la distancia entre ellas usando la fuerza de la señal de Bluetooth. Si las aplicaciones estiman que están a menos de aproximadamente seis pies (o dos metros) de distancia durante un período de tiempo suficiente, las aplicaciones intercambian identificadores. Cada aplicación registra un encuentro con el identificador de la otra. La ubicación de los usuarios no es necesaria, ya que la aplicación sólo necesita saber si los usuarios están lo suficientemente cerca como para crear un riesgo de infección.

Cuando un usuario de la aplicación se entera de que está infectado con COVID-19, se puede notificar a otros usuarios de su propio riesgo de infección. Aquí es donde los diferentes diseños de la aplicación difieren significativamente.

Algunas aplicaciones dependen de una o más autoridades centrales que tienen acceso privilegiado a la información sobre los dispositivos de los usuarios. Por ejemplo, TraceTogether, desarrollado para el gobierno de Singapur, exige que todos los usuarios compartan su información de contacto con los administradores de la aplicación. En este modelo, la autoridad mantiene una base de datos que asigna los identificadores de la aplicación a la información de contacto. Cuando un usuario da un resultado positivo, su aplicación sube una lista de todos los identificadores con los que ha entrado en contacto en las dos últimas semanas. La autoridad central busca esos identificadores en su base de datos y utiliza los números de teléfono o las direcciones de correo electrónico para comunicarse con otros usuarios que puedan haber estado expuestos. Esto coloca mucha información de los usuarios fuera de su propio control y en manos del gobierno. Este modelo crea riesgos inaceptables de rastreo generalizado de las asociaciones de individuos y no debe ser empleado por otras entidades de salud pública.

Otros modelos se basan en una base de datos que no almacena tanta información sobre los usuarios de la aplicación. Por ejemplo, no es necesario que una autoridad almacene información de contacto real. En cambio, los usuarios infectados pueden subir sus registros de contactos a una base de datos central, que almacena identificadores anónimos de todos los que puedan haber estado expuestos. Entonces, los dispositivos de los usuarios que no están infectados pueden hacer regularmente ping a la autoridad con sus propios identificadores. La autoridad responde a cada ping con la indicación de si el usuario ha sido expuesto. Con las salvaguardias básicas en su lugar, este modelo podría ser más protector de la privacidad del usuario. Lamentablemente, todavía puede permitir a la autoridad conocer las identidades reales de los usuarios infectados. Con salvaguardas más sofisticadas, como la mezcla criptográfica, el sistema podría ofrecer garantías de privacidad un poco más fuertes.

Algunas propuestas van más allá, publicando toda la base de datos públicamente. Por ejemplo, la propuestas de [Apple](https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/) y [Google](https://www.blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology/), publicada el 10 de abril, [difundiría](https://www.blog.google/documents/57/Overview_of_COVID-19_Contact_Tracing_Using_BLE.pdf) una lista de claves asociadas a personas infectadas a las personas cercanas con la aplicación. Este modelo deposita menos confianza en una autoridad central, pero crea[nuevos usuarios](https://arxiv.org/pdf/2003.11511.pdf) que comparten su estado de infección que deben ser mitigados o aceptados.

Algunas aplicaciones requieren que las autoridades, como los funcionarios de salud, certifiquen que una persona está infectada antes de que puedan alertar a otros usuarios de la aplicación. Otros modelos podrían permitir a los usuarios informar por sí mismos sobre el estado de la infección o los síntomas, pero eso puede dar lugar a un número considerable de falsos positivos, lo que podría socavar la utilidad de la aplicación.

En resumen, mientras que hay una promesa temprana en algunas de las ideas para la ingeniería de aplicaciones de rastreo de proximidad, hay muchas preguntas abiertas.

**¿Serían efectivas las aplicaciones de proximidad?**

El [seguimiento tradicional de contactos](https://en.wikipedia.org/wiki/Contact_tracing#Steps_in_contact_tracing) es bastante laborioso, pero puede ser bastante detallado. Los trabajadores de la salud pública entrevistan a la persona con la enfermedad para conocer sus movimientos y las personas con las que han estado en contacto cercano. Esto puede incluir entrevistas con los miembros de la familia y otras personas que pueden conocer más detalles. Los trabajadores de salud pública se ponen en contacto con estas personas para ofrecerles ayuda y tratamiento según sea necesario, y a veces las entrevistan para seguir la cadena de contactos. Es difícil hacer esto a escala durante una pandemia. Además, la memoria humana es falible, por lo que incluso el cuadro más detallado obtenido a través de las entrevistas puede tener lagunas o errores importantes.

Las aplicaciones de rastreo de contactos por proximidad no sustituyen la intervención directa de los trabajadores de la salud pública. También es dudoso que una aplicación basada en criterios de proximidad pueda ayudar sustancialmente a realizar el rastreo de contactos del COVID-19 en una época como la actual, en la que la transmisión en la comunidad es tan elevada [que gran parte de la población general](https://www.wsj.com/articles/a-state-by-state-guide-to-coronavirus-lockdowns-11584749351) se[refugia en su hogar](https://www.statista.com/chart/21240/enforced-covid-19-lockdowns-by-people-affected-per-country/), y cuando [no hay suficientes pruebas](https://www.vox.com/2020/4/10/21214218/trump-coronavirus-testing-social-distancing) para rastrear el virus. Cuando hay tantas personas infecciosas sin diagnosticar en la población, [una gran parte](https://www.nytimes.com/2020/03/31/health/coronavirus-asymptomatic-transmission.html) de las cuales son [asintomáticas](https://www.nbcnews.com/news/world/new-chinese-data-asymptomatic-coronavirus-cases-could-help-world-response-n1173896), una aplicación de proximidad no podrá advertir de la mayoría de los riesgos de infección. Además, sin pruebas rápidas y ampliamente disponibles, ni siquiera alguien con síntomas puede confirmar el inicio del proceso de notificación. Y ya se está pidiendo a todo el mundo que evite la proximidad con personas ajenas a su hogar.

Sin embargo, una aplicación de este tipo podría ser útil para el rastreo de contactos en un momento que esperamos que llegue pronto, cuando la transmisión en la comunidad sea lo suficientemente baja como para que la población pueda dejar de refugiarse en el hogar, y cuando haya suficientes pruebas para diagnosticar rápida y eficientemente COVID-19 a escala.

El rastreo de contactos tradicional sólo es útil para los contactos que el sujeto puede identificar. COVID-19 es excepcionalmente contagioso y puede transmitirse de persona a persona incluso durante encuentros breves. Un breve intercambio entre un empleado de tienda de comestibles y un cliente, o entre dos pasajeros de un transporte público, puede ser suficiente para que un individuo infecte al otro. La mayoría de las personas no recopilan información de contacto de todas las personas con las que se encuentran, pero las aplicaciones pueden hacerlo automáticamente. Esto puede ser un complemento útil para el rastreo de contactos tradicional.

Pero una aplicación tratará el contacto entre dos personas que pasan por la acera de la misma manera que el contacto entre compañeros de habitación o parejas románticas, aunque estos últimos conllevan riesgos de transmisión mucho mayores. Sin probar una aplicación en el mundo real, lo que implica riesgos de privacidad y seguridad, no podemos estar seguros de que una aplicación no registre también las conexiones entre personas separadas por paredes o en dos coches adyacentes detenidos en un semáforo. Las aplicaciones tampoco tienen en cuenta si sus usuarios llevan equipo de protección, y pueden informar en exceso sobre la exposición de usuarios como el personal de un hospital o los trabajadores de una tienda de comestibles, a pesar de sus precauciones adicionales contra la infección. No está claro cómo las limitaciones tecnológicas de los cálculos de proximidad del Bluetooth influirán en las decisiones de salud pública para notificar a las personas potencialmente infectadas. ¿Es mejor que estas aplicaciones sean ligeramente hipersensibles y se arriesguen a notificar en exceso a personas que tal vez no hayan estado realmente a menos de seis pies de un usuario infectado durante el tiempo necesario? ¿O debería la aplicación tener umbrales más altos para que un usuario notificado pueda tener más confianza en que realmente estuvo expuesto?

Además, estas aplicaciones sólo pueden registrar los contactos entre dos personas que tengan cada una un teléfono en su persona que esté habilitado para Bluetooth y que tenga la aplicación instalada. Esto pone de relieve otra condición necesaria para que una aplicación de proximidad sea efectiva: su adopción por un número suficientemente grande de personas. Las API de Apple y de Google intentan resolver este problema ofreciendo una plataforma común para que las autoridades sanitarias y los desarrolladores construyan aplicaciones que ofrezcan características y protecciones comunes. Estas empresas también aspiran a construir sus propias aplicaciones que interoperen de manera más directa y aceleren su adopción. Pero incluso así, un porcentaje considerable de la población mundial -incluida una buena parte de la población de los Estados Unidos- puede no tener acceso a un teléfono inteligente que ejecute la última versión de iOS o Android. Esto pone de relieve la necesidad de seguir empleando medidas de salud pública de probada eficacia, como las pruebas y el rastreo tradicional de contactos, para garantizar que no se pase por alto a las poblaciones ya marginadas.

No podemos resolver una pandemia codificando la aplicación perfecta. Los problemas sociales difíciles no se resuelven con tecnología mágica, entre otras razones porque no todo el mundo tendrá acceso a los teléfonos inteligentes y a la infraestructura necesaria para que esto funcione.

Por último, no debemos confiar excesivamente en la promesa de una aplicación no probada para tomar decisiones críticas, como decidir quién debe dejar de refugiarse y cuándo. Las aplicaciones fiables de este tipo suelen pasar por muchas rondas de desarrollo y capas de pruebas y garantía de calidad, todo lo cual lleva tiempo. E incluso entonces, las nuevas aplicaciones a menudo tienen errores. Una aplicación de rastreo de proximidad defectuosa podría conducir a falsos positivos, falsos negativos, o tal vez a ambos.

**¿Las aplicaciones de proximidad harían demasiado daño a nuestras libertades?**

Cualquier aplicación de proximidad crea nuevos riesgos para los usuarios de la tecnología. Un registro de la proximidad de un usuario con otros usuarios podría utilizarse para mostrar con quién se asocia e inferir lo que está haciendo. El temor a la divulgación de esa información sobre la proximidad podría enfriar a los usuarios para que no participen en actividades expresivas en lugares públicos. Los grupos vulnerables suelen tener una carga dispar por la tecnología de vigilancia, y el seguimiento de la proximidad puede no ser diferente. Y los datos de proximidad o los diagnósticos médicos pueden ser robados por adversarios como gobiernos extranjeros o ladrones de identidad.

Sin duda, algunas tecnologías de uso común crean riesgos similares. Muchos rastrean e informan de su ubicación, desde Fitbit a Pokemon Go. El simple hecho de llevar un teléfono móvil conlleva el riesgo de rastrear a través de la triangulación de la torre de telefonía móvil. Los comercios buscan minar el tráfico peatonal de los clientes [a través de Bluetooth](https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html?). Muchos usuarios "optan" por servicios como los servicios de localización de Google, que mantienen un registro detallado de todos los lugares a los que han ido. Facebook trata de cuantificar las asociaciones entre las personas a través de innumerables señales, entre ellas el uso del reconocimiento facial para extraer datos de fotografías, la vinculación de cuentas con datos de contacto y la extracción de interacciones digitales. Incluso los servicios de preservación de la privacidad como Signal pueden exponer asociaciones a través de metadatos.

Por lo tanto, la propuesta de añadir el rastreo de proximidad a estas otras formas de rastreo existentes no sería un vector de amenaza totalmente nuevo. Pero la escala potencialmente mundial del rastreo de contactos de los API y las aplicaciones, y su recopilación de información sensible sobre la salud y las asociaciones, presenta nuevos riesgos para un mayor número de usuarios.

El contexto importa, por supuesto. Nos enfrentamos a una pandemia sin precedentes. Decenas de miles de personas han muerto, y cientos de millones de personas han sido instruidas para refugiarse en su hogar. Se espera una vacuna en [12 a 18 meses](https://www.sciencealert.com/who-says-a-coronavirus-vaccine-is-18-months-away). Aunque esto da urgencia a los proyectos de aplicaciones de proximidad, también debemos recordar que esta crisis terminará, pero las nuevas tecnologías de rastreo tienden a quedarse. Por lo tanto, los desarrolladores de aplicaciones de proximidad deben estar seguros de que están desarrollando una tecnología que preservará la privacidad y la libertad que todos apreciamos, para no sacrificar los derechos fundamentales en una emergencia. Proporcionar suficientes salvaguardias ayudará a mitigar este riesgo. Es necesaria una total transparencia sobre el funcionamiento de las aplicaciones y las API, incluido el código fuente abierto, para que la gente entienda y dé su consentimiento informado a los riesgos.

**¿Tiene una aplicación de proximidad suficientes salvaguardias?**

Instamos a los desarrolladores de aplicaciones a que proporcionen, y a los usuarios a que exijan, las siguientes salvaguardias necesarias:

**Consentimiento**

El consentimiento informado, "opt-in" y voluntario es el requisito fundamental para cualquier aplicación que rastree las interacciones de un usuario con otras personas en el mundo físico. Además, las personas que deciden utilizar la aplicación y luego se enteran de que están enfermas también deben tener la opción de compartir un registro de sus contactos. Los gobiernos no deben exigir el uso de ninguna aplicación de proximidad. Tampoco debe haber una presión informal para utilizar la aplicación a cambio del acceso a los servicios gubernamentales. Del mismo modo, las partes privadas no deben exigir el uso de la aplicación para acceder a espacios físicos u obtener otros beneficios.

Los individuos también deben tener la oportunidad de apagar la aplicación de rastreo de proximidad. Los usuarios que consientan en algún tipo de rastreo de proximidad podrían no consentir en otro tipo de rastreo de proximidad, por ejemplo, cuando participen en actividades particularmente delicadas como visitar a un proveedor de servicios médicos o participar en la organización política. Las personas pueden ocultar esta información en las entrevistas tradicionales de rastreo de contactos con los trabajadores de la salud, y el rastreo de contactos digitales no debe ser más intrusivo. Es más probable que las personas enciendan las aplicaciones de proximidad en primer lugar (lo que puede ser bueno para la salud pública) si saben que tienen la prerrogativa de apagarlas y volver a encenderlas cuando lo deseen.

Aunque puede ser tentador ordenar el uso de una aplicación de rastreo de contactos, la interferencia con la autonomía personal es inaceptable. La salud pública requiere confianza entre los funcionarios de salud pública y el público, y el temor a la vigilancia puede hacer que las personas eviten las pruebas y el tratamiento. Esta es una preocupación particularmente aguda en las comunidades marginadas que tienen razones históricas para desconfiar de la participación coercitiva en nombre de la salud pública. Si bien algunos gobiernos pueden hacer caso omiso del consentimiento de sus ciudadanos, instamos a los desarrolladores a que no trabajen con esos gobiernos.

**Minimización**

Cualquier aplicación de rastreo de proximidad para el seguimiento de contactos debe recoger la menor cantidad de información posible. Esto es probablemente sólo un registro de dos usuarios que están cerca el uno del otro, medido a través de la fuerza de la señal Bluetooth más los tipos de dispositivos, y un marcador único y giratorio para el teléfono de la otra persona. La aplicación no debería recopilar información de localización. Tampoco debería recopilar información de marca de tiempo, excepto quizás la fecha (si los funcionarios de salud pública piensan que es importante para el rastreo de contactos).

El sistema debe retener la información durante el menor tiempo posible, que probablemente se mide en días y semanas y no en meses. Los funcionarios de salud pública deberían definir el incremento de tiempo durante el cual los datos de proximidad podrían ser pertinentes para la localización de contactos. Todos los datos que ya no sean pertinentes deben ser eliminados automáticamente.

Toda autoridad central que mantenga o publique bases de datos de identificadores anónimos no debe recopilar ni almacenar metadatos (como las direcciones IP) que puedan vincular los identificadores anónimos con personas reales.

La solicitud debe recoger información con el único fin de localizar los contactos. Además, debería haber barreras rígidas entre a) la aplicación de rastreo de proximidad y b) cualquier otra cosa que un fabricante de aplicaciones esté recopilando, como datos de localización agregados o registros sanitarios individuales.

Por último, en la mayor medida posible, la información reunida debería residir en el propio dispositivo del usuario, en lugar de en los servidores administrados por el desarrollador de la aplicación o una entidad de salud pública. Esto presenta desafíos de ingeniería. Sin embargo, las listas de dispositivos con los que el usuario ha estado en proximidad deberían permanecer en el propio dispositivo del usuario, de modo que la comprobación de si un usuario se ha encontrado con alguien infectado se realice locálmente.

**Seguridad de la información**

Una aplicación que se ejecuta en segundo plano en un teléfono y que registra la proximidad de un usuario con otros usuarios presenta considerables riesgos para la seguridad de la información. Como siempre, la limitación de la superficie de ataque y la cantidad de información recogida disminuirá estos riesgos. Los desarrolladores deben abrir su código y someterlo a auditorías y pruebas de penetración de terceros. También deberían publicar detalles sobre sus prácticas de seguridad.

Tal vez sea necesaria una mayor ingeniería para garantizar que los adversarios no puedan comprometer la eficacia de un sistema de rastreo por proximidad o derivar información reveladora sobre los usuarios de la aplicación. Ello incluiría impedir que las personas denuncien falsamente las infecciones como una forma de rastreo o de denegación de servicio, así como garantizar que los adversarios bien dotados de recursos que vigilan los metadatos no puedan identificar a las personas que utilizan la aplicación o registrar sus conexiones con otras.

Los identificadores "anónimos" no deben ser vinculables. La rotación regular de los identificadores utilizados por el teléfono es un comienzo, pero si un adversario puede enterarse de que varios identificadores pertenecen al mismo usuario, aumenta en gran medida el riesgo de que pueda vincular esa actividad con una persona real. Según entendemos la propuesta de Apple y Google, se pide a los usuarios que den positivo que suban claves que vinculen todos sus identificadores durante un período de 24 horas. (Hemos pedido a Apple y Google una aclaración.) Esto podría permitir a los rastreadores recoger identificadores rotativos si tuvieran acceso a una amplia red de lectores bluetooth, y luego rastrear los movimientos de los usuarios infectados a lo largo del tiempo. Esto rompe las salvaguardas creadas por el uso de identificadores rotativos en primer lugar. Por esa razón, los identificadores rotativos deben cargarse a cualquier autoridad central o base de datos de manera que no revele el hecho de que muchos identificadores pertenecen a la misma persona. Esto puede requerir que la carga de las fichas de un solo usuario se agrupe con otros datos del usuario o se extienda a lo largo del tiempo.

Por último, los gobiernos podrían tratar de obligar a los desarrolladores de tecnología a subvertir los límites que establecen, por ejemplo, cambiando la aplicación para informar de las listas de contactos a una autoridad central. La transparencia mitigará estos riesgos, pero siguen siendo inherentes a la construcción y el despliegue de una aplicación de este tipo. Esta es una de las razones por las que pedimos a los desarrolladores que establezcan líneas claras sobre los usos de sus productos y que se comprometan a resistir a los esfuerzos del gobierno por entrometerse en el diseño, como hemos visto hacer a empresas como [Apple en el caso de San Bernardino.](https://www.apple.com/customer-letter/)

**Transparencia**

Las entidades que desarrollan estas aplicaciones deben publicar informes sobre lo que hacen, cómo lo hacen y por qué lo hacen. También deben publicar código de fuente abierta, así como políticas que aborden los problemas de privacidad y seguridad de la información mencionados anteriormente. Éstas deben incluir compromisos para evitar otros usos de la información recogida por la aplicación y un compromiso para evitar la interferencia del gobierno en la medida en que lo permita la ley. Declarado como política de la aplicación, esto también debería permitir la aplicación de las violaciones a través de las leyes de protección del consumidor.

**Abordar el Sesgo**

Como ya se ha dicho, las aplicaciones de rastreo de contactos dejarán fuera a los individuos sin acceso a la tecnología más avanzada. También favorecerán a aquellos predispuestos a contar con las empresas de tecnología y el gobierno para atender sus necesidades. Debemos asegurarnos de que los desarrolladores y el gobierno no dejen fuera directa o indirectamente a los grupos marginados al confiar en estas aplicaciones con la exclusión de otras intervenciones.

Por otro lado, estas aplicaciones pueden dar lugar a muchos más falsos positivos para ciertos tipos de usuarios, como los trabajadores del sector de la salud o de los servicios. Esta es otra razón por la que las aplicaciones de rastreo de contactos no deben utilizarse como base para excluir a las personas del trabajo, las reuniones públicas o los beneficios del gobierno.

**Expiración**

Cuando la crisis de COVID-19 termine, cualquier aplicación construida para luchar contra la enfermedad debería terminar también. Definir el final de la crisis será una cuestión difícil, por lo que los desarrolladores deben asegurarse de que los usuarios puedan optar por no participar en cualquier momento. También deberían considerar la posibilidad de incluir límites de tiempo en sus aplicaciones, junto con comprobaciones periódicas con los usuarios para saber si quieren seguir emitiendo. Además, como los grandes proveedores como Apple y Google apoyan estas aplicaciones, deberían articular las circunstancias en las que construirán y no construirán productos similares en el futuro.

La tecnología tiene el poder de amplificar los esfuerzos de la sociedad para abordar problemas complejos, y esta pandemia ya ha inspirado a muchos de los mejores y más brillantes. Pero también estamos muy familiarizados con la capacidad de los gobiernos y entidades privadas para desplegar tecnologías de rastreo dañinas. Sobre todo, incluso mientras luchamos contra COVID-19, debemos asegurarnos de que la palabra "crisis" no se convierta en un talismán mágico que pueda ser invocado para construir nuevos y cada vez más inteligentes medios de limitar las libertades de las personas a través de la vigilancia.