Ya es sabido que Google te rastrea en todos lados, aún cuando tienes deshabilitada la función de historial de ubicaciones de Google.

Según una investigación de Associated Press en 2018, otras aplicaciones de Google como Maps o el servicio de actualización meteorológica diaria en Android, permiten que Google recoja continuamente tu ubicación precisa.

De acuerdo con Google, la compañía utiliza estas funciones de seguimiento de ubicación con el objetivo de mejorar la experiencia de los usuarios, como *«mapas personalizados, recomendaciones basadas en lugares que has visitado, ayuda para encontrar tu teléfono, actualizaciones de tráfico en tiempo real y anuncios más útiles».*

Además, también se sabe que Google podría compartir tus datos de ubicación con las autoridades federales en investigaciones criminales cuando se te solicite con una orden judicial.

La base de datos «SensorVault» de Google ayuda a la policía a resolver crímenes

Un dato que no muchos sabían, es que Google también ayuda a las autoridades federales a identificar sospechosos de delitos compartiendo el historial de ubicación de todos los dispositivos que pasaron cerca de escenas de crímenes por un periodo de tiempo predeterminado.

Cabe mencionar que Google no comparte información personal de los usuarios cercanos, sino que pide a la policía que primero analice el historial de ubicación de todos los usuarios y reduzca los resultados a solo unos pocos usuarios seleccionados para recibir sus nombres, direcciones de correo electrónico y otros datos personales de Google.

Un nuevo informe del The New York Times reveló que Google mantiene una base de datos, conocida internacionalmente como SensorVault, que ha funcionado por casi diez años y contiene registros detallados de ubicación de cientos de millones de teléfonos en todo el

mundo, y comparte con las autoridades de los países.

Según algunos empleados anónimos de Google citados en el informe, dichas solicitudes para investigar en la base de datos de SensorVault de Google se han disparado en los últimos seis meses, recibiendo Google hasta 180 solicitudes en solo una semana.

¿Cómo utiliza la ley la base de datos de Google SensorVault?

Para poder buscar datos de ubicación, las autoridades policiales deben obtener una orden llamada «geofence».

A continuación se observa una lista de cómo Google comparte los datos de ubicación cuando se requiere *«legalmente»:*

- Las autoridades se acercan a Google con una orden de goefence en busca de smartphones que Google registró cerca de la escena del crimen.
- Luego de recibir la orden, Google recopila información de ubicación de su base de datos SensorVault y la envía a los investigadores, con cada dispositivo identificado por un código de identificación anónimo y no la identidad real de los dispositivos.
- Después, los investigadores revisan los datos, buscan patrones de los dispositivos cerca de la escena del crimen y solicitan más datos de ubicación en los dispositivos de Google que parezcan relevantes para ver el movimiento particular del dispositivo más allá del área original definida en la orden.
- Cuando los investigadores limitan los resultados a unos pocos dispositivos, que creen que pudieron pertenecer a sospechosos o testigos, Google revela el nombre real, dirección de correo electrónico y otros datos asociados con los dispositivos.

El informe del NYT explicó todo el proceso cuando los agentes federales solicitaron los datos de ubicación para investigar una serie de atentados en Austin, Texas.

Los agentes federales utilizaron por primera vez esta técnica de captura de delincuentes en 2016, que desde entonces se ha extendido a los departamentos locales de todo el país,

incluyendo California, Florida, Minnesota y Washington.

Algunos casos destacados por el informe del diario mostraron cómo la policía utilizó dichos datos para acusar a inocentes, con un hombre encarcelado durante una semana el año pasado en una investigación de asesinato luego de ser registrado cerca del lugar de la muerte y luego liberado después de que los investigadores señalaron y arrestaron a otro sospechoso.

Cada vez es más común que las autoridades busquen la ayuda de compañías tecnológicas durante investigaciones criminales, pero el uso de base de datos de historial de ubicación como SensorVault ha generado inquietudes referentes a la privacidad de los usuarios, recopilación de datos e incluso, temor a ser inocente y acusado como implicado.