Apple y Google se unieron para trabajar en un borrador de especificación para toda la industria que está diseñado para abordar los riesgos de seguridad y alertar a los usuarios cuando están siendo rastreados sin su conocimiento o permiso usando dispositivos como AirTags.

> *«La primera especificación de su tipo permitirá que los dispositivos de rastreo de ubicación Bluetooth sean compatibles con la detección y alertas de rastreo no autorizados en las plataformas Android e iOS»*, dijeron las compañías.

Aunque estos rastreadores están diseñados principalmente para controlar pertenencias personales como llaves, billeteras, equipaje y otros artículos, estos dispositivos también han sido objeto de abuso por parte de atacantes con fines delictivos o maliciosos, incluyendo casos de acecho, acoso y robo.

El objetivo es estandarizar los mecanismos de alerta y minimizar las oportunidades de uso indebido en los dispositivos de rastreo de ubicación Bluetooth de diferentes proveedores. Con ese fin, Samsung, Tile, Chipolo, eufy Security y Pebblebee se han unido.

Al hacerlo, los dispositivos de seguimiento fabricados por las compañías deben cumplir con un conjunto de instrucciones y recomendaciones, así como notificar a los usuarios sobre cualquier seguimiento no autorizado en dispositivos iOS y Android.

> *«La formalización de un conjunto de mejores prácticas para los fabricantes permitirá una compatibilidad escalable con las tecnología de detección de seguimiento no deseado en varias plataformas de teléfonos inteligentes y mejorará la privacidad y la seguridad de las personas»,* según la especificación.

> *«La detección de seguimiento no deseado puede detectar y alertar a las personas*

> *de que un rastreados de ubicación separado del dispositivo del propietario viaja con ellos, así como proporcionar medios para encontrar y desactivar el rastreador».*

Un aspecto crucial de la especificación propuesta es el uso de un registro de emparejamiento, que contiene información de identidad verificable (pero ofuscada) del propietario de un accesorio (por ejemplo, número de teléfono o dirección de correo electrónico) junto con el número de serie del accesorio.

Además de retener los datos durante un período mínimo de 25 días después de que se haya desemparejado el dispositivo (momento de eliminación), el registro de emparejamiento se pone a disposición de las fuerzas del orden al enviar una solicitud válida.

Además, la especificación exige que los rastreadores pasen de un modo *«casi propietario»* a un modo *«separado»* en caso de que ya no esté cerca del dispositivo emparejado de un propietario durante más de 30 minutos.

Las compañías están solicitando comentarios de las partes interesadas durante los próximos tres meses, después de lo cual se espera que se publique una implementación de producción de la especificación para alertas de seguimiento no deseadas en algún momento antes de fin de año en ambos ecosistemas móviles.

La última vez que Apple y Google se unieron fue para diseñar una plataforma a nivel de sistema que usa balizas Bluetooth de baja energía (BLE) para permitir el rastreo de contactos durante la pandemia de COVID-19 sin usar datos de ubicación.