64fogreveal-tierrahackers-ivoox91992992

Los departamentos de policía de Estados Unidos han estado utilizando la plataforma FOC Reveal para vigilar a usuarios móviles de forma masiva gracias a datos de aplicaciones móviles comunes que brokers de información han comprado y revendido por un precio anual de unos 7.500 dólares americanos. Viento en popa y a toda vela, os traemos otro episodio de Tierra de Hackers. ¡Comenzamos! Hola hola y bienvenidos a Tierra de Hackers, tu noticiero de ciberseguridad hecho podcast.

Hoy es el 4 de septiembre de 2022, este es el episodio número 64, yo soy Alexis Porros y en este episodio no tenemos al Gran Martín, ya que se encuentra fuera del ciberespacio, lamentablemente, pero lo vamos a tener de vuelta en el próximo episodio, así que quedaos sentados hasta que venga en el próximo. Así que en este episodio estamos tú y yo, querido oyente, bueno, y las noticias que te traigo. Pero primero de todo, como siempre, agradeceros a todos vosotros, nuestros queridos oyentes, el seguimiento que nos hacéis en redes sociales, donde nos comentáis y nos enviáis vuestras sugerencias y preguntas, si me refiero a Twitter, Instagram y Facebook, donde estamos como el handle arroba tierra de hackers, donde nos podéis seguir y escribir comentarios y lo que queráis.

También, si no estáis suscritos a nuestro podcast en vuestra plataforma de escucha favorita, id ahora mismo a suscribiros para que cuando salga el nuevo episodio lo tengáis, tengáis esa notificación de que ya está listo para escucharlo. También nos podéis seguir, nos podéis enviar vuestros mensajes y sugerencias en LinkedIn, YouTube y Twitch. Ahí estamos como tierra de hackers y, por supuesto, nos podéis enviar vuestros correos electrónicos a podcast arroba tierra de hackers punto com.

Bueno, y también tenemos un servidor de Discord al que podéis acceder vía tierra de hackers punto com barra Discord, donde tenemos ya una gran población cibernética, digámoslo así, de unos, no sé, 700 usuarios casi ya, así que muy, muy agradecidos por todos los que os habéis unido ahí a compartir vuestros conocimientos, enviar preguntas, dudas, está muy interesante la verdad, así que os invitamos a uniros también. Y finalmente, antes de entrar en el episodio en sí, comentar, agradeceros primero de todo vuestro apoyo a la pregunta del episodio que publicamos siempre en Twitter y comentarla brevemente. La pregunta del episodio anterior fue la siguiente ¿Quién crees que está diciendo la verdad en la confrontación entre Twitter y su ex responsable de seguridad Peter Mach Sadko? Con un aplastante 92% tenemos que nuestros oyentes han elegido a Mach como el que está diciendo la verdad y un 8% a Twitter.

La verdad es que hay que comentar que Mach tiene una reputación de ser bastante fiable, una persona con moral y ética, así que bueno, vamos a ver cómo se va

desarrollando la historia, pero así apuntan las votaciones. Agradecer también a nuestro patrocinador Monat que nos apoya y que nos permite seguir adelante con el podcast. Monat, una empresa que comparte los mismos valores que nosotros, hace la seguridad más accesible y transparente nosotros a través de un podcast y Monat a través de una herramienta de gestión y visualización de telemetría y datos de seguridad.

Una empresa fundada en Silicon Valley y que está buscando muchos ingenieros, sobre todo con algo de experiencia en seguridad para ayudarles a construir y hacer realidad su misión. Lo mejor de todo es que están contratando en todo el mundo y en remoto, así que ya sabéis, echadle un vistazo a su web monat.com y les podéis contactar al correo tierradehackers arroba monat.com para más información y así ellos saben que venís de nuestra parte. Y con todo esto y un bizcocho, comenzamos.

¿Y qué os traigo? Pues nada más y nada menos que un caso más de abuso a nuestra privacidad, queridos oyentes. Sí, sí, así, tal y como lo escucháis. Y es que los departamentos de policía locales, estatales y federales de Estados Unidos han estado utilizando una herramienta llamada Fog Reveal, que sería traducido así como desvela la niebla o revela la niebla.

Es en plan, tenemos una cortina de humo, pues con esta herramienta se va el humo y ves la realidad claramente. Algo así, supongo, que se inspiraron en llamar a la herramienta Fog Reveal. Pero bueno, esta herramienta, como digo, la están utilizando los cuerpos de policía de Estados Unidos para vigilar a millones de personas en Estados Unidos, lo que les ha permitido rastrear dispositivos individuales sin una orden judicial.

Esto es muy importante. Gracias a información basada en datos recopilados de aplicaciones comunes de teléfonos móviles inteligentes que cualquiera, como vosotros, queridos oyentes, o como yo incluso, puede haber instalado en su teléfono. Estas aplicaciones incluyen aplicaciones del tiempo, incluso se mencionan un par bastante populares en la investigación, que son Starbucks, supongo que todo el mundo la conoce, para pedir, es de la cafetería de Starbucks, pedir café y similares.

Y Waze, esta aplicación que es, si no me equivoco, es propiedad de Google ahora y se utiliza para, bueno, para ubicarte en un mapa y tener la ruta a tu destino. Todo esto viene de investigaciones de la organización activista Electronic Frontier Foundation, la EFF, y el grupo de noticias Associated Press. Y es que estamos acostumbrados a escuchar sobre cómo la Agencia de Seguridad Nacional, la NSA, la Agencia Central de Inteligencia, la CIA, e incluso la Oficina Federal de Investigaciones, el FBI, todos estos han analizado ilegalmente cantidades masivas de datos sobre personas que viven en Estados Unidos e incluso en el mundo, con aliados en otros países, como hemos comentado en algún episodio anterior en Alemania y similares, pero bueno, la Organización del Conjunto de los Cinco Ojos Mundiales, ¿verdad? Pero de lo que no se habla tanto es de que la policía, al menos en Estados Unidos, está haciendo lo mismo.

Y ahora lo hemos podido comprobar gracias a correos electrónicos, documentos, que incluyen incluso manuales publicados al respecto de esta herramienta, FogReveal. Y bueno, antes de seguir, quiero hacer un inciso sobre FogReveal. ¿Quién ha creado esta herramienta? Pues una empresa que se llama FogDataScience, que es un bróker de información cuyo producto principal es, como digo, FogReveal.

Esta empresa, FogDataScience, tiene su sede en Virginia, en Estados Unidos, y también tiene entidades relacionadas en Nueva Jersey, Ohio y Texas. Fue fundada en 2016 por Robert Liskowski, quien dirigió la División de Seguridad Cibernética Nacional del Departamento de Seguridad Nacional en la administración del presidente George Bush. Su colega Broderick es un exgeneral de brigada de la Marina de Estados Unidos que dirigió el Centro Tecnológico del DHS, el Departamento de Seguridad Nacional, durante el huracán Katrina en 2005.

Bueno, ¿y cuál es el modelo de negocio de FogDataScience? Pues esta empresa lo que hace es comprar miles de millones de puntos de datos de unos 250 millones de dispositivos móviles en Estados Unidos, originalmente obtenidos de decenas de miles de aplicaciones móviles de iOS, iPhone, iPad y Android. Como he mencionado anteriormente, aplicaciones del tiempo, Starbucks y Waze, por mencionar unas de las más populares, los datos provienen de empresas de tecnología y torres de telefonía celular, y se recopilan en la herramienta FogReview. Luego, por una tarifa de suscripción anual de entre unos 7.000 y 9.000 dólares, bastante asequible para ciertos cuerpos de policía locales y estatales, los de, probablemente, las grandes ciudades, FogDataScience proporciona acceso a una base de datos masiva que permite realizar búsquedas de dónde se encuentran las personas gracias a una interfaz web amena y fácil de usar, y muchas veces, como digo, sin orden judicial, o bueno, creo que casi todos los escenarios que se han visto en base a los correos electrónicos y documentos obtenidos son todos sin orden judicial.

Las fuerzas del orden analizan estos datos de FogReview para crear patrones de vida de los usuarios geolocalizados, es decir, con estos, al fin y al cabo, una persona normalmente en su vida real, semana a semana, repite sus actividades, ¿no? Se puede crear un patrón de vida, por la mañana sale de casa y va al trabajo, al mediodía va a algún sitio a comer, pues, en una zona de restaurantes, luego vuelve al trabajo y a la tarde vuelve a su casa, y bueno, así es la vida, ¿no? Así se va repitiendo y las fuerzas del orden, como digo, pueden crear estos patrones de vida y bueno, y monitorizar a los usuarios. Según investigaciones de Associated Press, FogDataScience vendió su software en unos 40 contratos a casi dos docenas de agencias, según una empresa que se llama GopSpend, que en español sería algo como gastos gubernamentales, que controla los gastos del gobierno. Los registros y los informes de Associated Press muestran el primer relato público del uso extensivo de FogReveal por parte de la policía local.

Un dato curioso es que Associated Press intentó contactar a Starbucks e incluso a Waze

sobre estas revelaciones. Estas dos empresas denegaron cualquier relación con FogDataScience, así que estas empresas no dan directamente los datos a FogDataScience, como digo, les vienen, los compran estos datos a otra empresa tercera, que ahora voy a entrar en detalle en qué empresa es. Los oyentes de Tierra de Hackers no se deberían sorprender de este tipo de empresas, ya que hemos comentado noticias similares en episodios anteriores.

Y ya en el episodio 52 tenemos el caso del bróker de información AnomalySix. En el episodio 61 tenemos el caso de los brókers de información Safegraph y Placer AI. Vamos, que no paran de surgir empresas que venden nuestra información para que otras empresas o cuerpos de la ley nos rastreen.

Hoy en día lo que más vale, incluso yo creo más que el oro y el petróleo, son nuestros datos, así que tendríamos que protegerlos bastante bien, o que nos compensaran si los utilizan sin nuestro consentimiento, ¿verdad? Y con esto voy a... ¿está esto permitido? Alguien se preguntará, supongo. Pues claramente la respuesta es no. En Estados Unidos, de hecho, está la Cuarta Enmienda, que es un grupo de leyes que protege a los ciudadanos americanos sobre búsquedas o incautaciones de forma no justificada o de forma forzada.

Y esto, todo lo que comento, FOC Reveal, FOC Data Science, y el uso de estos datos por parte de los grupos policiales en Estados Unidos, es una clara violación de la Cuarta Enmienda. No solo si se busca un individuo en particular, que esto sería obvio, sino que la Cuarta Enmienda prohíbe las búsquedas generales y no particulares de los datos de ubicación de todas las personas que estén presentes en un lugar en particular. Por esta razón, los tribunales, de hecho, dicen que las búsquedas mediante el concepto de geovalla, geofencing en inglés, también violan la Cuarta Enmienda.

El tema del geofencing lo hemos comentado anteriormente, pero brevemente comentar que es definir una zona geográfica en la que quieres buscar datos sobre personas que están en esa zona. En 2018, la Corte Suprema de Estados Unidos dictaminó que la Cuarta Enmienda requiere que la policía obtenga una orden judicial antes de incautar datos de ubicación históricos, llamados Información de Ubicación de Sitio Celular, de las empresas telefónicas. También se teme que el seguimiento de la ubicación que ofrece FOC Data Services pueda tener otros usos más aplicados a la vida real o más concretos, como controlar a las personas que buscan abortos en estados donde ahora es ilegal.

Y esto, como digo, lo hemos comentado en el episodio 61, así que si queréis refrescar vuestra memoria escuchando esos episodios. ¿Y cómo se consiguieron estos correos electrónicos y documentos reveladores? La Electronic Frontier Foundation, esta organización activista, realizó su investigación a través de más de 100 solicitudes de registros públicos presentados durante varios meses y se consiguieron correos electrónicos y documentos de FOC Data Science. Entre estos documentos también se

consiguió el manual de usuario de 30 páginas de la herramienta FOC Reveal.

Luego comento algunos detalles del manual que son interesantes, pero quería comentar una conclusión que obtuvieron los investigadores. Decían literalmente que esos registros muestran que FOC Data Science y algunas fuerzas del orden, policías, no creían que la vigilancia de FOC Data Science violara los derechos de la Cuarta Enmienda de las Personas y que hiciera falta que las autoridades obtuvieran una orden judicial para poder utilizar la herramienta FOC Reveal. Me parece una conclusión bastante interesante para reflexionar sobre la capacidad de lógica de estas entidades del orden, de no saber si la información que están tratando necesita una orden judicial o no, pero bueno, ahí lo dejo.

FOC Data Science menciona que tiene un socio de información y de hecho es desde esta empresa desde donde obtiene la información para ofrecerla a sus clientes y esta empresa se llama Ventel con dos Ns, V-E-N-T-E-L, que provee de datos que consume y vende a sus clientes. Ventel obtiene datos publicitarios globales de su empresa matriz llamada Gravy Analytics. Los datos en sí proveen, como he dicho antes, de aplicaciones instaladas en los teléfonos inteligentes de las personas.

Los desarrolladores de hecho de estas aplicaciones a menudo firman acuerdos para vender la información de ubicación de sus usuarios a terceros y de hecho este es digamos el modelo de negocio que utilizan los desarrolladores que ofrecen aplicaciones gratuitas. De alguna forma supongo que tienen que ganarse el pan de cada día y en lugar de cobrar a los usuarios, que a veces es una entrada bastante difícil para usuarios que se descarguen la aplicación o que la compren, pues la ofrecen de forma gratuita y a cambio sin que el usuario se dé cuenta, o bueno, o algunos aunque se den cuenta, se está compartiendo la ubicación. Y es lo que estos desarrolladores recopilan de sus aplicaciones y esto lo pasan a empresas como digo Ventel barra Gravy Analytics y Ventel luego lo vende a otras empresas como FogDataScience.

La información de geolocalización se basa en números de identificación publicitarios, lo que se llama en inglés Advertising ID por ejemplo en los sistemas IOS, que según los funcionarios de FogDataServices se extraen de aplicaciones populares, como he dicho anteriormente. Esta información luego se vende a empresas como FogDataScience, como he dicho, pero también interesante es que se vende a agencias gubernamentales, incluida la oficina de aduanas y protección fronteriza. De hecho sobre Ventel, si nos habéis seguido cada episodio, ya hablamos por primera vez en el episodio 16, allá en noviembre de 2020, cuando cubríamos la noticia que ponían entre dichos si la oficina de aduanas y protección fronteriza de Estados Unidos pudiera estar abusando de los datos de ubicación de los residentes americanos para ubicarlos y arrestarlos.

De nuevo, si no os acordáis de esta noticia, podéis ir a refrescar vuestra memoria y escuchar el episodio 16. Por poner un poquito en perspectiva en tema de precio de licencias, hemos comentado que una licencia anual de FogReveal cuesta entre 7.000 y

9.000 dólares. Pues la oficina de aduanas y protección fronteriza de Estados Unidos pagó a Ventel casi medio millón de dólares en agosto de 2020 por su software para poder geolocalizar a personas en Estados Unidos.

Se entiende que los cuerpos de policía prefieran ir con FogReveal, que es mucho más barato que con Ventel directamente. Y por eso creo que en el futuro van a seguir surgiendo empresas de este tipo que venden datos de geolocalización porque van a competir supongo que en precio y bueno, van a seguir surgiendo de estas empresas hasta que se regularice un poco el tema. Bueno, y aparte de dar seguimiento, poder determinar dónde se encuentra un usuario en tiempo real, qué es lo que ofrece digamos FogReveal? Pues según los materiales de marketing obtenidos, FogDataScience también ha promocionado su herramienta FogReveal con la capacidad de ofrecer análisis predictivos a la policía.

Una palabra, un concepto de moda últimamente que se usa para describir herramientas de alta tecnología, digamos, utilizando Machine Learning, inteligencia artificial y similares que para predecir los puntos críticos del crimen. Con esto lo que se puede hacer es determinar casi en tiempo real los movimientos diarios de las personas y estar un paso adelante de ellas. Como he dicho anteriormente, no se puede determinar un patrón de vida de estas personas.

Personas pueden ser criminales, no? Pues se podría incluso decir, oye, pues en base a su historia, hoy lunes suponemos que va a ir a esta zona para cometer un crimen o no, o ahí lo podemos ir a interceptar y arrestar. Así que esta función predictiva también es muy atractiva para los policías. FogReveal se ha utilizado desde al menos el 2018 en investigaciones criminales, algunas con resoluciones exitosas como casos de protección infantil y abusos de menores y también como el asesinato de una enfermera de 25 años en Newport, Arkansas.

Se pudieron encontrar los teléfonos de personas que habían estado cerca de ella cuando se la vio por última vez y de alguna forma identificaron al criminal. Y también se ha utilizado en otras investigaciones criminales como el rastreo de los movimientos de un posible participante en la insurrección del 6 de enero en el Capitolio. La herramienta FogReveal rara vez o nunca se menciona en los registros judiciales durante las investigaciones legales, algo que los abogados defensores dicen que les dificulta defender adecuadamente a sus clientes en los casos en los que se utilizó esta tecnología.

FogReveal permite a la policía y a otros de sus clientes interactuar con la herramienta para realizar distintas tareas, por ejemplo, dibujar un cuadro, una geovalla o una geofence y ver identificadores que representan cada dispositivo dentro de esa área geográfica en un periodo de tiempo determinado y también usar la identificación de un dispositivo para rastrear el historial de ubicación preciso de ese dispositivo durante

hasta cinco años en el pasado. FogReveal en sus documentos menciona que sigue, rastrea los dispositivos a través del ID de publicidad, del Advertising ID. Estos son números únicos asignados a cada dispositivo que, de todas formas, se pueden resetear de tanto en cuando desde las opciones del teléfono móvil, pero si no las reseteas, es fácil seguir a estos identificadores.

Estos números de identificación de publicidad no contienen el nombre del usuario del teléfono, pero se pueden rastrear hasta los hogares y lugares de trabajo para ayudar a la policía a establecer análisis de patrones de vida y determinar al menos el tipo de persona que está detrás de este dispositivo móvil rastreando. Bueno, y sobre el manual, unas pinceladas. ¿Qué dice? Cuando inician sesión por primera vez en la interfaz web de FogReveal, los usuarios reciben un mensaje que les recuerda que los datos a los que están a punto de acceder son confidenciales y que deben protegerse adecuadamente.

A partir de ahí, un usuario puede comenzar a buscar datos históricos sobre qué dispositivos se encontraban en un área en particular a través de un cuadro de búsqueda que acepta direcciones y coordenadas de latitud y longitud. Como he dicho, los usuarios también pueden dibujar geobayas, geofences, para ver qué dispositivos estaban en un área. El manual indica que es posible vigilar a una gran cantidad de personas a la vez, aunque esto puede no ser útil por la gran cantidad de datos que devuelve la herramienta.

Entonces vas a tener muchos datos y no puedes identificar cuál es tu objetivo. Luego, los usuarios pueden etiquetar un dispositivo en concreto para marcarlo como un dispositivo de interés. A partir de ahí, pueden consultar ese dispositivo en particular y el sistema mostrará un patrón de actividad de unos 180 días o unos seis meses en el pasado.

Y de hecho, según uno de los fundadores en la documentación y en los correos electrónicos intercambiados, como digo, puede permitir búsquedas de hasta cinco años en el pasado. El manual también incluye una captura de pantalla que enumera lo que describe como grupos de usuarios, mostrando diferentes usuarios. Estos incluyen Arkansas, el Departamento de Policía de Atlanta, el Departamento de Policía de Massachusetts, Barnstable, el Departamento de Policía del Estado de Connecticut, el Departamento de Policía del Estado de Delaware y algunos más.

Algunos dicen la FFI Associated Press, que ya se conocían, pero otros son nuevos y es una revelación. Esta lista también incluye una referencia a una empresa privada que se llama iWorks Corp, que según dicen, podría referirse a iWork Corporation, que es un contratista del gobierno federal. Hasta incluso el gobierno federal directamente está abusando, pudiera estar abusando de esta información.

Algunos departamentos de policía les gusta mucho la rapidez con la que pueden acceder a estos datos, ya que no requieren órdenes judiciales, como he dicho. Por lo general, se ha demostrado que Google podría proporcionar información sobre qué dispositivos

estaban presentes en un área en particular en un momento específico, pero las autoridades necesitarían obtener la llamada orden judicial de ubicación inversa que puede llevar tiempo. Con FOC Reveal es tan simple como hacer login y buscar a tu objetivo.

Y esto marca un antes y un después, porque según Bennett Cyphers, que dirigió el trabajo de registros públicos de la Electronic Frontier Foundation en contra de FOC Data Science, dijo que no ha habido ningún registro oficial anterior de empresas que vendan este tipo de datos granulares directamente a las fuerzas del orden local. Así que esto es una gran revelación. Y esto viene sobre todo por el precio de lo gratuito, ¿no? ¿Cuál es este precio? Pues, bien, querido oyente, tu privacidad.

Tenemos que pensárnoslo bien dos veces antes de utilizar aplicaciones gratuitas que puedan poner en peligro nuestra privacidad, sobre todo esas que piden información de geolocalización. Gratuitas y no gratuitas también, algunas que pagues incluso pueden ser tan malas como las gratuitas. En conclusión, piénsatelo dos veces, querido oyente, antes de darles permiso o si no, y de vez en cuando puedes analizar los permisos que has otorgado a las aplicaciones y deshabilitar los que pienses que no son necesarios.

Igual te preguntas, querido oyente, ¿tiene FOC Data Science mis datos? ¿Y cómo lo detengo si es así? Pues es bastante difícil saber si FOC Data Science, y por extensión, la policía, tiene acceso a tus datos. Si descargaste una aplicación de terceros, bueno, cualquier aplicación, digámoslo así, en tu móvil y otorgaste acceso a los datos de ubicación en los últimos cinco años, es posible que la respuesta sea sí, es bastante posible. Aunque bueno, como digo, mencionan 250 millones de dispositivos, ¿no? Hay muchos más dispositivos en Estados Unidos, así que podrías calcular la probabilidad en función a todos los dispositivos móviles que hay en Estados Unidos.

Los residentes en California pueden enviar una solicitud de derecho a saber, en base a la ley de privacidad del consumidor en California, a la fuente de datos de FOC Data Science y Ventel para saber qué es lo que tienen sobre vosotros. Y si lo sé y no lo sé, si sospecho que igual tienen mi información, ¿qué puedo hacer al respecto? Pues lo primero, deshabilitar el seguimiento de anuncios y identificador de anuncios móviles, este en iOS, por ejemplo, se llama Advertising ID. Esto se puede desactivar o resetear de vez en cuando, así se rompe un poco el seguimiento.

No es que sea infalible y perfecto, porque probablemente igual, viendo el mismo patrón en dos distintos Advertising IDs, podrían correlar y decir, estos dos Advertising IDs son el mismo, la misma persona, el mismo dispositivo móvil, pero bueno, es una forma de ponérselo más difícil a esta gente, a estas empresas que venden nuestros datos y los recopilan. En segundo lugar, se puede intentar limitar cuántas aplicaciones en el teléfono tienen permiso a recopilar datos de geolocalización, como he dicho antes, deshabilita las aplicaciones que no lo necesiten y permíteles a las que lo necesiten,

como por ejemplo, aplicaciones de mapas para orientarse en el espacio. Aunque como ya he dicho, una de esas aplicaciones que ha proporcionado datos a este tipo de empresas es Waze, que según mi experiencia, la utilizan muchísimos taxistas, al menos en Nueva York y en todo Estados Unidos, así que, bueno, no es tan fácil aplicar esta recomendación.

Pero lo más importante es que todos podemos hacer, bueno, al menos desde Estados Unidos, pero también en cualquier otro país, es hacer presión al Congreso y al gobierno en sí para que protejan nuestra privacidad. La supervisión federal de empresas como Fog Data Science es un panorama legal en evolución y de hecho, recientemente, un caso relacionado. La Comisión Federal de Comercio demandó a un bróker de información llamado Kochava, que al igual que Fog Data Science, ofrece información de usuarios móviles en base a identificaciones publicitarias.

Los tribunales también están sopesando el uso que hace el gobierno de los datos de ubicación y de hecho, ahora ya hay proyectos de ley ante el Congreso que, de ser aprobados, regularían la industria. Recordemos que en 2018, la Corte Suprema dictaminó que la policía generalmente necesita una orden judicial para revisar los registros que revelan dónde han estado los usuarios de teléfonos celulares. Esto, bueno, esto es normal, ¿verdad?, que lo necesiten, pero vemos cómo estos cuerpos de policía se los saltan un poco a la torera, así, digámoslo, utilizando FogReveal.

Y con esto, queridos oyentes, llego a la pregunta del episodio. ¿Cuál crees que sería la medida más efectiva para evitar el abuso de información de geolocalización de usuarios obtenida a partir de aplicaciones móviles que siguen tus movimientos? Os vamos a ofrecer cuatro opciones de respuesta. La primera es, pues bueno, el gobierno, con la legislación, debería tratar este tema.

La segunda sería que los fabricantes deberían aplicar más restricciones aún para evitar qué aplicaciones pudieran acceder de forma ilimitada a accesos de ubicación. La tercera es que los desarrolladores deberían tener un poquito más de moral y decidir no vender toda esta información de geolocalización a otras empresas. Y la última somos nosotros, queridos oyentes, los usuarios de estas aplicaciones móviles, que podríamos intentar, bueno, de alguna forma enviar ubicaciones falsas o no utilizar el GPS, como he dicho, desactivarlo, resetear el Advertising ID este, que he dicho, es todo más desde la parte del consumidor, del usuario.

Así que ahí planteamos la pregunta del episodio y votad, por favor, en Twitter. Y bueno, antes de acabar el episodio también quería comentar brevemente una noticia que me ha parecido muy interesante y bastante relacionada sobre este tema de geolocalización. No es tan relacionada con un tema a nivel global o a nivel de todo un país como Estados Unidos, es un tema más concreto.

Pero bueno, durante la conferencia de la Black Hat de este año en Las Vegas, a la que

pudimos asistir Martín y yo en calidad de prensa, en representación de Tierra de Hackers, los investigadores de seguridad de Nozomi Networks, que es una empresa que se enfoca en seguridad de sistemas de control industrial, mostraron un nuevo ataque contra los sistemas de localización en tiempo real construidos con tecnología de radio de banda ultra ancha, ultra wideband en inglés. Lo que consiguieron los investigadores fue, uno, monitorizar estos dispositivos de rastreo sin el conocimiento de su objetivo, de la persona que lo lleva, y dos, incluso hacer que cualquier dispositivo de rastreo en tiempo real pareciera que se moviera a voluntad de sus atacantes.