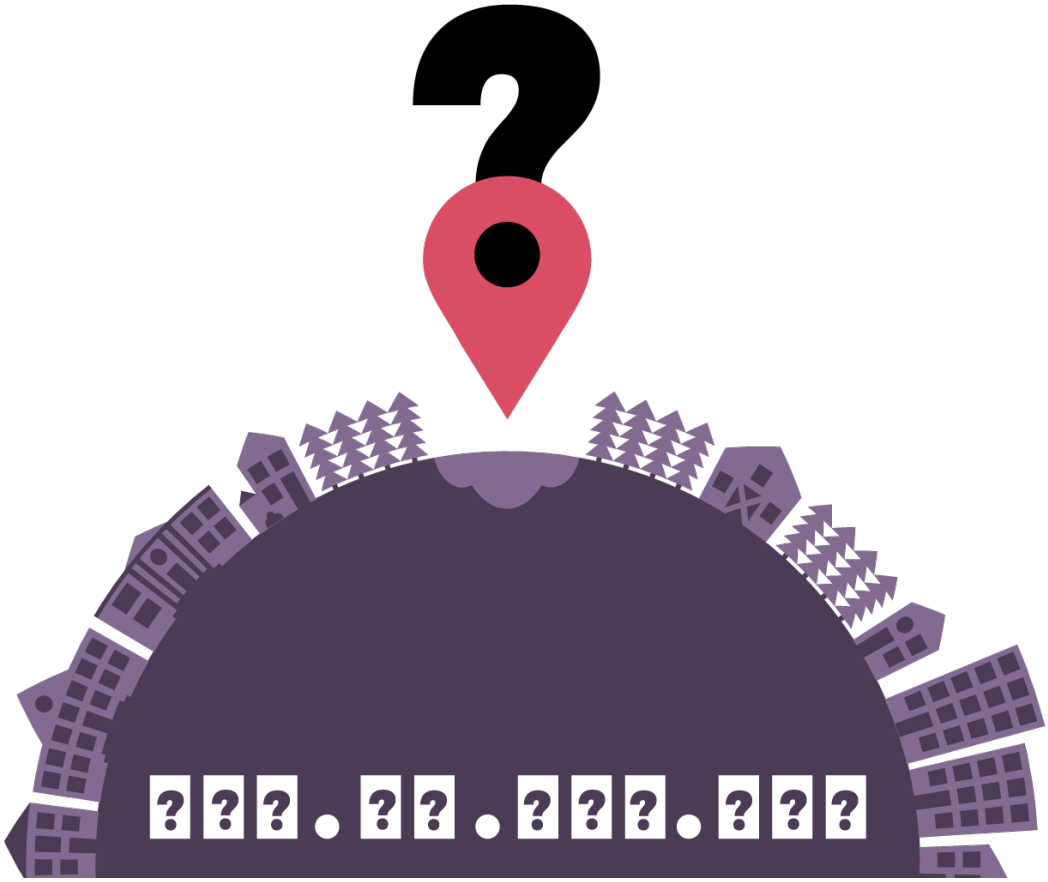

Informantes no fiables: direcciones IP, Consejos digitales e incursiones policiales

Cómo la policía y los tribunales fallan al usar la información poco fiable de las direcciones IP y consejos para verificar

Aaron Mackey, Frank Stanton Jurídico
Seth Schoen, Técnico Superior de Personal
Cindy Cohn, Directora Ejecutiva

Septiembre 2016

Sumario

Introducción

> Han sido acusados de ser ladrones de identidad, spammers y estafadores. Ellos han sido visitados por agentes del FBI, oficiales federales, recaudadores del IRS, ambulancias en busca de veteranos suicidas, y agentes de la policía en busca de niños fugitivos. Han encontrado la gente hurgando en su granero. La información personal de sus inquilinos ha sido difundida libremente; sus nombres y direcciones publicadas en Internet por vigilantes. Alguna vez, alguien dejó un inodoro roto en la calzada como una amenaza extraña e indefinida[1].
> *- Cómo un fallo en el mapeado de Internet convirtió una granja de Kansas cualquiera en un infierno digital*

> A las 6 am del 30 de marzo, la policía de Seattle apareció en el apartamento en Queen Anne de Jan Bultmann y David Robinson con una orden de registro para buscar pornografía infantil, basada en un dato obtenido desde un video ilícito ligado a su dirección IP. Seis oficiales llegaron con dos furgonetas y pasaron más de una hora haciendo búsquedas forenses en las computadoras de la casa. Un oficial se paró en el dormitorio y observó cómo Robinson se vestía[2].
> *- La policía va de pesca, buscando en la casa de los activistas de privacidad de Seattle que mantienen la red Tor*

> En 2012, llegó a casa tarde una noche para encontrar a la policía a punto de romper su puerta. Dijeron que estaban buscando una computadora portátil robada del gobierno con información personal en ella...Ha recibido llamadas telefónicas enojadas y mensajes de Facebook de extraños que han sido perjudicados por alguien en línea. Cuando rastrean las direcciones IP asociadas con sus agresores, apuntan a su casa, por lo que asumen que sus ocupantes son responsables[3].
> *- 17 millones de direcciones IP que apunta a una casa en Ashburn, Virginia*

La revolución digital ha dado a las fuerzas del orden más herramientas para ayudarnos a rastrear e identificarnos que nunca. Sin embargo, a medida que las fuerzas de seguridad recurren cada vez más a pruebas electrónicas para investigar los crímenes, una de las herramientas más accesibles, las direcciones de Protocolo de Internet (direcciones IP) se han vuelto cada vez más malinterpretadas por los agentes del orden y los jueces. La aplicación de la ley con demasiada frecuencia exagera la fiabilidad de la información de la dirección IP en la búsqueda de órdenes y otros procesos (como citaciones), utilizando metáforas que crean un sentido de certeza donde no siempre existe. Además, los tribunales a menudo no saben qué preguntas hacer acerca de la información de direcciones IP o cómo evaluar su fiabilidad.

Aunque las direcciones IP a veces pueden ser indicadores confiables de ubicaciones o

individuos cuando se combinan con otra información, como los registros de proveedores de servicios de Internet, el uso de la dirección IP por sí sola, sin más, con demasiada frecuencia puede dar lugar a redadas peligrosas, aterradoras y desperdiciadoras de recursos basadas en órdenes judiciales emitidas sin una investigación adecuada. Este riesgo es especialmente alto cuando: (1) determina la ubicación física de un sospechoso y (2) identifica a un sospechoso individual responsable de un crimen.

Este documento explica cómo las fuerzas del orden público y los tribunales pueden utilizar las direcciones IP de manera responsable en las investigaciones penales y proporciona sugerencias específicas para ayudar a cada una de ellas. Un cuerpo la ley, bien desarrollado en torno a la fiabilidad de los informantes anónimos, ofrece un buen modelo para policías y jueces que buscan confiar en direcciones IP. En resumen, cuando la policía confía en información de informantes anónimos para obtener una orden de registro, deben incluir detalles en sus solicitudes que demuestren tanto la confiabilidad del informante como el contexto similar y la comprobación que la policía haya obtenido.

También recomendamos encarecidamente que las fuerzas del orden dejen de usar y que los tribunales dejen de confiar en metáforas como direcciones de correo físicas o placas de licencia al describir las direcciones IP en las solicitudes de autorización y en otros lugares. Las metáforas caracterizan incorrectamente la función y la confiabilidad de las direcciones IP y potencialmente operan para exagerar la precisión de la información de direcciones IP.

Este artículo se divide en cinco secciones. En primer lugar, explica lo que los policías y los tribunales necesitan saber acerca de la tecnología de direcciones IP para que puedan utilizarla correctamente en las investigaciones. En segundo lugar, describe por qué las direcciones IP por sí solas no pueden localizar o identificar de forma fiable a un sospechoso utilizando dos ejemplos recientes de alto perfil. En tercer lugar, describe cómo la ley establecida sobre la información de los informantes proporciona un buen modelo sobre cómo los policías y los tribunales deben tratar la información de direcciones IP. En cuarto lugar, muestra cómo se pueden aplicar las reglas de los informantes a las direcciones IP. En quinto lugar, ofrece recomendaciones específicas tanto para las fuerzas del orden como para los tribunales cuando se utilizan las direcciones IP como parte de las investigaciones penales.

1. Las limitaciones de las direcciones IP deberían restringir la forma en que la policía las usa en las investigaciones

El uso de direcciones IP por parte de las autoridades para identificar una ubicación o un individuo en particular es problemático debido al limitado propósito técnico de la tecnología. Las direcciones IP son cadenas de números utilizadas para identificar un dispositivo en Internet y para encaminar el tráfico a esa dirección. Por diseño, las direcciones IP estaban "específicamente limitadas en su alcance para proporcionar las funciones necesarias" para que Internet entregue correctamente el tráfico, que hoy incluye correos electrónicos, sitios web y videos en streaming[4]. La sencillez de las direcciones IP es en parte lo que hace posible que el Internet pueda enrutar el tráfico rápidamente en todo el mundo. Sin embargo, esa simplicidad viene con limitaciones para usar la tecnología en otros contextos.

Primeramente, la tecnología nunca fue diseñada para identificar de manera única una ubicación física exacta, sólo un destino electrónico en Internet. Durante la infancia de Internet, los diseñadores querían asegurarse de que el tráfico podría ser fácilmente enrutado en cualquier parte del mundo. Como parte del ruteo del tráfico los operadores pueden anunciar su capacidad para llegar a determinados destinos, pero estos anuncios se hacen sobre una base numérica, no geográfica. Un organismo coordinador ha asignado bloques de direcciones IP a regiones de todo el mundo[5]. Por debajo del nivel regional, los ISP están, por lo general, a cargo de asignar direcciones IP. Pero una dirección IP no lo hace inherentemente "pertenecer a" un país en particular como tampoco haber sido utilizados en o desde una ubicación física o área, o por un usuario final determinado o una ISP en especifico[6].

A nivel local, pueden asignarse direcciones IP similares basadas en la geografía, aunque sólo indirectamente. Los ISP toman la decisión de asignar bloques de direcciones IP a determinados lugares por una variedad de razones, con el objetivo de crear una red que entregue eficientemente el tráfico de Internet. El resultado puede ser que las ubicaciones cercanas unas a otras tienen direcciones IP similares, pero que es más a menudo es el producto de donde el proveedor tiene enlaces físicos y enrutadores a una red que la geografía. Por ejemplo, si un ISP tiene un enlace de fibra óptica entre dos ciudades distantes, las direcciones IP asignadas a esas ciudades pueden ser similares porque crea una red más eficiente. Una tercera ciudad cerca de una de esas ciudades geográficamente puede no compartir la misma conexión y por lo tanto, probablemente tendría completamente diferentes direcciones IP asignadas a ella.

Aunque existen bases de datos que rastrean las asignaciones de direcciones IP, su amplitud, su contenido y la importancia de una asignación pueden ser muy amplios. En resumen, no hay un mapa central ni una guía telefónica que conecte las direcciones IP a ubicaciones concretas, motivado, particularmente, por que las direcciones IP a menudo se reasignan a diferentes usuarios de Internet a lo largo del tiempo. Tampoco existe una forma uniforme de asignar de forma sistemática ubicaciones físicas basadas en direcciones IP; Aunque algunas técnicas de mapeo pueden ser extremadamente precisas para algunas direcciones, los mapas resultantes no son "oficiales" y no serán realmente completos. Por lo tanto, la información de direcciones IP, por sí misma, sirve como una herramienta inconsistente para la aplicación de la ley o cualquier persona para identificar una ubicación exacta.

En segundo lugar, el uso de una dirección IP para identificar a un individuo específico es problemático porque no hay nada sobre las propias direcciones que las haga identificables personalmente. Las direcciones IP identifican determinados dispositivos o grupos de dispositivos en Internet, no a las personas que utilizan Internet. En algunos casos, puede tener sentido concluir que una sola persona está asociada con un dispositivo conectado a Internet, pero que a menudo no es el caso en situaciones del mundo real.

La dificultad de asociar una dirección IP con cualquier persona se demuestra por el hecho de que en paises desarrollados, urbanizados como los Estados Unidos, existen más dispositivos de conexión a Internet, hoy en día, que direcciones disponibles en la versión más utilizada del protocolo de Internet, IPv4[7]. Cuando Internet fue inicialmente diseñado, la secuencia utilizada para IPv4 solo permitía 4,3 mil millones de direcciones únicas, un total que parecía inimaginablemente alta[8]. El increíble crecimiento de Internet junto con el desarrollo de la informática personal y móvil - donde la mayor parte de los estadounidenses usa múltiples dispositivos al día - ha superado el número de direcciones IPv4. Y aunque hay una nueva versión del Protocolo de Internet, IPv6, con una gama de direcciones IP dramáticamente más grande que IPv4, la tasa de adopción de direcciones IPv6 sigue siendo sólo el 30 por ciento de los usuarios en los Estados Unidos[9].

Como resultado de la demanda de conexiones de Internet superando el número de direcciones IPv4, los proveedores de servicios de Internet se ven cada vez más obligados a dividir ese limitado grupo de direcciones IP entre su mayor base de clientes. Así, cuando los clientes utilizan por primera vez el proveedor de servicios para acceder a Internet, pueden conectarse a través de una dirección IP que fue utilizada anteriormente – o incluso simultaneamente - por otra persona. Dependiendo de la frecuencia con la que el usuario utilice la conexión, el proveedor de servicios puede mantener la misma dirección IP asignada a esa cuenta o reasignarla a otro cliente si hay demanda en otra

parte. Y con el tiempo, el proveedor de servicios puede reasignar la dirección IP por cualquier número de razones. En resumen, a diferencia de las direcciones de las calles, las direcciones IP no son estáticas.

Además, dado este cruce de direcciones IP, se han creado tecnologías que permiten a múltiples dispositivos y usuarios compartir una sola dirección IP. El ejemplo más común es la traducción de direcciones de red (Network Address Translation, NAT), que se utiliza en los routers domésticos y en algunos ISP (generalmente los operadores móviles)[10]. La tecnología pone esencialmente la dirección IP pública en un nivel superior que un individuo o usuario específico.

Las metáforas pueden articular el problema

Dados los limites de las direcciones IP descritas anteriormente, las analogías usadas para comparar la tecnología con otros tipos de identificadores personales o geográficos a menudo se descomponen. Por ejemplo, la policía a menudo incluye declaraciones en las solicitudes de autorización que afirman que las direcciones IP son como las direcciones físicas de las calles. Esto es a medias cierto, en el sentido de que tanto las direcciones IP como las direcciones de calle se utilizan para enrutar mensajes a sus destinos. Sin embargo, la analogía implica que las direcciones IP son estáticas e identifican una casa o ubicación en un mapa físico, lo que no siempre es cierto. La policía que usa esta metáfora da a un tribunal la falsa impresión de que las direcciones IP son exclusivas de los lugares exactos del mundo físico y que hay una permanencia que conecta la dirección IP a esa ubicación. También sugiere – erróneamente - la existencia de un procedimiento claro y predecible a seguir para determinar la localización en cada caso, como se podría hacer para una dirección de calle dada un mapa autoritario de una ciudad.

La analogía también sugiere que las direcciones IP pueden proporcionar información precisa acerca de un individuo asociado con una dirección IP cuando, como se discutió anteriormente, esto no siempre es cierto. La metáfora de la dirección de la calle se descompone aún más porque las direcciones IP y las direcciones físicas se asignan de manera muy diferente. Las direcciones físicas se asignan en función de la geografía, lo que significa que las personas que viven al lado del otro comparten algunas características comunes de la dirección, como el mismo nombre de la calle. Con las direcciones IP, dos personas que viven al lado del otro pueden estar usando direcciones IP que no tienen casi nada en común porque, por ejemplo, utilizan diferentes ISP (que tienen diferentes grupos de direcciones IP) o utilizan servidores proxy o redes privadas virtuales VPNs).

Otra metáfora defectuosa utilizada por la aplicación de la ley es la noción de que las direcciones IP son como placas de matrícula de vehículos[11]. Las placas sirven muy diferentes propósitos que las direcciones IP. Las matrículas están diseñadas para ser identificadas de

manera única y pueden ser rastreadas por las autoridades para la seguridad pública y la aplicación de la ley. El gobierno también asigna placas de licencia a las personas, en contraste con las partes privadas que asignan direcciones IP a sus clientes o usuarios. Es generalmente ilegal cambiar las matrículas sin obtener permiso del gobierno o ocultarlas para que la policía no pueda identificar fácilmente los vehículos. Las direcciones IP, sin embargo, no fueron diseñadas para ser identificables de forma única y pueden ser compartidas por varias personas o dispositivos simultáneamente o reutilizadas en el tiempo por diferentes personas que acceden a Internet, como se mencionó anteriormente. También es completamente legal que los usuarios de Internet enmascaren o compartan sus direcciones IP, a diferencia de los números de matrículas.

Con las limitaciones de las direcciones IP para identificar individuos y lugares descritos aquí, la siguiente sección usa dos casos recientes que demuestran por qué esas limitaciones pueden causar invasiones severas de la privacidad de los individuos.

2. Los peligros de usar direcciones IP para localizar o identificar sospechosos

Como demuestran las tres anécdotas presentadas en la introducción, la excesiva dependencia de la capacidad de la información de direcciones IP, sin más, para localizar o identificar sospechosos de delitos, está causando daño a personas inocentes. Una inmersión más profunda en dos de esos casos ayuda a dilucidar el problema.

Antes de discutir estos casos, es importante enfatizar que con una correcta corroboración, el uso de direcciones IP, por parte de las fuerzas del orden, para identificar una ubicación o individuo en particular puede ser bastante confiable. Por ejemplo, un método de corroboración de una dirección IP con una dirección física o un individuo es obtener registros de un proveedor de servicios de Internet (ISP). La corroboración proviene de la información adicional que un ISP tiene acerca de los usuarios de una dirección IP, incluidos los registros de facturación[12]. En muchos casos, por supuesto, la policía con conocimientos técnicos ya están haciendo esto. Un método alternativo de vincular direcciones IP a ubicaciones físicas, conocidas como geo-ubicación IP y discutidas con más detalle a continuación, también puede ser muy fiable en algunas situaciones específicas.

Sin embargo, lo que los ejemplos a continuación demuestran es que no existe una fórmula fiable que permita a las fuerzas del orden público pasar de una dirección IP sospechosa a un lugar o persona específica. En cambio, la fiabilidad del uso de la información derivada de una dirección IP en las investigaciones depende de una serie de factores que no suelen estar bajo el control de la policía, es más; algunas técnicas de investigación de direcciones IP podrían no ser fructíferas en situaciones particulares.

Ubicación: ¿Por qué las direcciones IP solo no son proxies de ubicación siempre

La historia de *Fusión* describecomo las fuerzas del orden y el mal uso de la poco fiable información de las dirección IP de los particulares ha sometido a los residentes de una granja en el centro de los Estados Unidos a un acoso casi perpetuo[13]. Esto se debe a que la policía está malinterpretando los datos que apuntan a identificar las ubicaciones físicas específicas en función de las direcciones IP cuando la tecnología realmente le está diciendo a los policías que casi no tienen idea de dónde se encuentra físicamente la dirección IP.

Las empresas privadas han construido negocios a partir de hacer que las direcciones IP coincidan con ubicaciones físicas. A un nivel alto, la información es útil para muchas personas y empresas. Por ejemplo, puede ayudar a las empresas a ver de qué país parece venir

la mayoría del tráfico de sus sitios web,lo que puede ayudar a tomar la decisión de negocios de cuando debe crearse una versión en idioma extranjero de dicho sitio web. Con el tiempo, estas compañías de mapeo IP se han vuelto mucho más precisas al vincular direcciones IP particulares con ubicaciones físicas en algunas circunstancias, a menudo como resultado de combinar direcciones IP con otros datos de ubicación. Este tipo de coincidencia, conocido como geo-ubicación IP, a veces puede ser un tipo razonable de corroboración, pero la técnica sigue evolucionando. Examinar la exactitud y fiabilidad de todos los servicios de localización geográfica de IP utilizados por las fuerzas de seguridad y las industrias privadas está fuera del alcance de este documento. Sin embargo, lo que los informes de los medios han demostrado es que la dependencia de la ley en un servicio de geolocalización, MaxMind, está fuera de lugar porque la policía sobreestima la confiabilidad de los resultados de localización geográfica IP proporcionados por el servicio.

En la actualidad, aunque la mayoría de los servicios de geo-localización pueden identificar con precisión que una dirección IP es originaria de un país o región del mundo en particular, su precisión puede variar drásticamente al intentar localizar con precisión una dirección IP en un estado particular, ciudad o dirección física. Compañías como MaxMind generalmente proporcionan información sobre las limitaciones de sus servicios, de manera que la medida contextual y de confiabilidad está disponible para la policía y los tribunales. También es probable que las empresas proporcionen estimaciones de la precisión de su información de ubicación para cualquier dirección IP o rango de direcciones. Por ejemplo, a partir de la fecha de publicación de este documento en setiembre de 2016, MaxMind afirma que sus datos de ubicación es, en promedio, el 87 por ciento de precisión cuando se trata de identificar que una dirección IP en particular se encuentra en los Estados Unidos[14], pero Sólo entre 28-44 por ciento de precisión para hacer coincidir una dirección IP con una ubicación exacta[15]. Una vez más, esto no quiere decir que los datos de MaxMind pueden ser mucho más preciso para las consultas particulares, sólo se usa como un ejemplo de las limitaciones generales inherentes a servicios de geolocalización IP.

El especifico, preocupante, acoso que sufren los habitantes de la finca descrita en el relato de Fusion, es un resultado de lo MaxMind hace con las direcciones IP para los que no tiene datos de ubicación razonable en absoluto. Para los más de 600 millones de direcciones IP para las que MaxMind no tiene información específica que no sea probable que se encuentran en algún lugar de los Estados Unidos[16], El servicio hace por defecto la dirección física de una IP con las coordenadas GPS en la mitad del país. Esa ubicación, hasta un cambio reciente, resultó ser la única granja en la pequeña ciudad de Potwin, Kansas[17].

Esta característica del servicio de localización geográfica IP de MaxMind es el por que la policía ha llegado a la conclusión errónea de que los residentes de la granja son responsables de una gran cantidad de crímenes durante la última década. La policía está malinterpretando un resultado nulo para 600 millones de direcciones IP con que la ubicación precisa de

cientos de dispositivos conectados a Internet es esta granja. Pero los datos realmente dicen todo lo contrario - que el servicio no tiene idea de dónde está situada la dirección dentro de los Estados Unidos.

La historia de *Fusion* subraya por qué la policía tiene que utilizar la información de ubicación geográfica IP como punto de partida - y no la conclusión - para localizar a un sospechoso y apoya la necesidad de corroboración. Como se mencionó anteriormente, muchas policías usan las direcciones IP sólo como una pista inicial. El paso siguiente más común es uno que recomendamos: que la policía entonces proceso el solicitar al ISP para emparejar una dirección IP particular con una localización física[18]. A diferencia de servicios de geolocalización IPcomo MaxMind, los ISP son generalmente capaces de proporcionar una dirección de cliente correspondiente que coincida con una dirección IP utilizada en un momento determinado, dado que la mayoría ha tomado la decisión de negocios de registrar esa informacióncomo una cuestión de rutina. Cuando la información de ubicación se obtiene de un ISP para conectar una dirección física particular de un suscriptor con una dirección IP, esa información puede ser un indicador muy fiable de la ubicación de un suscriptor de un suscriptor particular de banda ancha de un ISP, aunque no necesariamente de un usuario específico, como se describe más adelante.

Las compañías de telefonía móvil que proporcionan servicios de Internet a los clientes pueden tener información adicional sobre la ubicación de un individuo basada en las características de su servicio, en comparación con los ISP de banda ancha fija. Por ejemplo, los carriers pueden ser capaces de identificar dispositivos individuales usando su red en lugar de suscriptores particulares. Los operadores móviles también pueden ser capaces de obtener una imagen más precisa de la ubicación de un individuo en el tiempo. Pero esto sólo refuerza el punto de que la policía y los jueces deben entender la naturaleza de la información que reciben.

MaxMind realmente hace algo de este seguimiento en la actualidad y puede hacer más en el futuro. Otras compañías de Geolocalización pueden y utilizan otros medios técnicos más complejos para hacer coincidir las direcciones IP con ubicaciones físicas. Estos métodos incluyen rastreo de ruteo (trace routing), teniendo dispositivos que reportan arreglos al GPS de parte de direcciones IP particulares, o usar investigaciones físicas en el mundo real para hacer coincidir una dirección IP con una ubicación física[19]. Incluso entonces, sin embargo, la información puede no identificar una dirección exacta de la calle o número de unidad y probablemente no habrá un identificador fiable de una persona en particular.

Identidad: El problema con depender de direcciones IP como equivalentes de identidad o por qué las direcciones IP no son Proxy de Identidad

La policía también está sobrestimando la capacidad de la información de direcciones IP para identificar realmente que un individuo específico es responsable de un crimen cometido en línea, una creencia que ha dañado a personas completamente inocentes. Para ser claro, hay algunas circunstancias en las que una dirección IP puede ser suficiente para identificar una persona usando un dispositivo. Sin embargo, como se analiza a continuación, por lo menos algunas pruebas corroborantes adicionales normalmente son necesarias.

A principios de este año, la policía de Seattle invadió la casa de dos activistas de la privacidad después de recibir una indicación de que una dirección IP asociada con el proveedor de Internet de la pareja fue utilizada en un crimen[20]. Resulta que los activistas eran hacían funcionar un relé de salida de Tor en su casa, lo que significaba que la policía allanó personas inocentes.

Tor es un servicio de anonimato diseñado para proteger la privacidad del individuo que oculta las direcciones IP de sus usuarios y luego a través eruta el tráfico de salida a través de relés de salida gestionados por voluntarios Tor[21] y sus operadores voluntarios de relé de salida proporcionan un servicio público importante para los disidentes políticos, activistas, o cualquier persona que quiera navegar por la web de forma anónima[22]. Una característica clave de Tor es que los individuos que operan sus relés de salida, que son los últimos equipos del tráfico Tor atraviesa antes de llegar a su destino final, no tienen ningún control o conocimiento de la actividad de Internet viene a través de los relés[23].

Así que cuando la policía se entera de un crimen conectado a una dirección IP de un relé de salida de Tor, hay pocas posibilidades de que el delincuente esté realmente asociado con esa dirección IP. La policía no ha reconocido esta realidad en múltiples casos en los que han buscado en los hogares de los anfitriones del relé de salida de Tor y se han apoderado de sus dispositivos[24].

Lo que los casos subrayan es que la policía a menudo toma la información de dirección IP para significar que una persona asociada con una dirección es la parte que cometió un crimen. Por muchas razones, la conexión de un individuo a un delito relacionado con una dirección IP, sin ninguna investigación adicional, es irresponsable y amenaza las libertades civiles de personas inocentes.

El problema de usar una dirección IP como un proxy de identidad para la delincuencia atribuida a la persona asociada con una dirección particular no se limita a Tor. Con empresas e individuos que operan redes inalámbricas abiertas fuera de sus hogares, cafés,

bibliotecas públicas y negocios, a menudo tienen muy poco control o conocimiento de las actividades de Internet de las personas que usan su conexión[25]. Otros servicios, como Redes Privadas Virtuales (VPN) y servidores proxy, también pueden hacer que las direcciones IP no sean indicadores confiables de la identidad y / o ubicación de una persona en particular[26].

La policía ha allanado locales que ofrecen redes inalámbricas abiertas tras concluir erróneamente que el titular de la cuenta fue responsable de un crimen, como el casode un hombre de Buffalo, Nueva York donde la policía allanó su casa y lo aresto de manera similar[27] después de rastrear pornografía infantil a su red doméstica, sin embargo, resultó que un vecino estaba usando la conexión inalámbrica abierta para descargar el contenido ilegal.

Todas estas tecnologías ponen de relieve cómo la dirección IP pública asociada a un dispositivo cambiará generalmente cuando se utiliza ese dispositivo en una conexión a Internet diferente. Es importante que la policía y los tribunales comprendan esta evolución en la forma en que la gente se conecta a Internet, porque significa que la dirección IP asignada a un abonado en particular puede incluir el tráfico de muchas otras personas y algunas de ellas pueden estar a miles de millas de la ubicación física del abonado.

Tal vez una de las explicaciones de por que las personas no pueden equivaler a una dirección IP vinieron de la orden del juez federal Gary Brown en *BitTorrent Adult Film Copyright Infringement Cases*[28]. En la concesión de varias mociones para anular subpoenas pidiendo la información del abonado ligado a direcciones IP identificadas en varias demandas por violación de derechos de autor, el juez Brown sostuvo que "el supuesto de que la persona que paga por el acceso a Internet en un lugar determinado es el mismo individuo que presuntamente descargó una sola película sexualmente explícita es tenue, y uno que ha crecido más que el tiempo." [29] el juez Brown continuó "Por lo tanto, hay más probabilidades de que el suscriptor a una dirección IP lleva a cabo una función aquí en particular el ordenador la descarga ilegal supuesta de un película pornográfica que solo quiere decir una persona que paga la factura de teléfono hizo una llamada de teléfono específico" [30].

Por lo tanto, la policía debe pensar en las direcciones IP como pistas útiles que pueden localizar la actividad delictiva dentro de una región geográfica en particular o conducir a un sospechoso individual. También deben reconocer que hay pasos rápidos y sencillos que pueden realizar para aprender más acerca de una dirección IP particular. Un ejemplo sencillo es realizar una búsqueda inversa de DNS (Domain Name System) de una dirección IP. :Los DNS son una enorme base de datos que compila la dirección IP y los nombres de dominio del sitio web de Internet, permitiendo a todos encontrar sitios web basados en sus nombres en lugar de la cadena de números que componen una dirección IP[31]. Una búsqueda DNS inversa puede revelar información útil e información de contacto de la parte que registró el dominio. Conectar una dirección IP en un servicio de búsqueda DNS inversa puede

proporcionar información adicional sobre la dirección.

EFF reconoce que muchos policías ya tratan las dirección IP como el punto de inicio de sus investigaciones y hacen mucho más trabajo antes de buscar una orden de búsqueda. . Pero para otros en las fuerzas del orden, este no es siempre el caso. Por lo tanto, la policía debe entender que las direcciones IP por sí solas no siempre son lo suficientemente confiables para localizar una ubicación exacta o individual porque la tecnología nunca fue construida para esas funciones. Con una mejor comprensión de por qué las direcciones IP por sí solas no pueden ser confiables, el documento ahora proporciona un marco legal para que los tribunales y la policía utilicen cuando usen la información en órdenes judiciales.

3. La información de la dirección de IP es muy parecida a los datos de los informantes a la policía

La información de direcciones IP no es confiable para identificar ubicaciones o identidades específicas y esta falta de fiabilidad debe tratarse también bajo la ley. Un modelo jurídico útil es la jurisprudencia relativa a los informantes anónimos, donde la ley ha reconocido desde hace mucho tiempo que pueden ser útiles para la policía, pero también que hay peligros de la Cuarta Enmienda inherentes a confiar en consejos anónimos demasiado pesadamente o sin una comprensión adecuada de la más amplia contexto.

En virtud de la Cuarta Enmienda, los tribunales han reconocido desde hace mucho tiempo que la policía no puede obtener órdenes basadas únicamente en rumores o consejos anónimos que reciben de los informantes[32]. A pesar de la carga de la prueba requerida por la policía para obtener una orden, necesaria para llevar a cabo una incursión en el hogar o la oficina de alguien, es mucho menor que lo que se necesita para condenar a alguien, las fuerzas del orden todavía tienen que demostrar que tienen una causa probable. Determinar lo que equivale a causa probable no es un análisis científico riguroso; Más bien, es una conclusión de sentido común que se sigue del análisis de todos los hechos y circunstancias que la policía ha incluido en sus solicitudes de autorización.

En una línea de casos del Tribunal Supremo que tratan de problemas de confiabilidad y corroboración que surgen cuando terceros proporcionan consejos a la policía, el tribunal ha dejado claro que la policía debe hacer más para confirmar los consejos proporcionados por informantes anónimos antes de solicitar una orden u otro proceso, Y esbozó una serie de requisitos[33].

Por ejemplo, en *Aguilar v. Estado de Texas*, el Tribunal Supremo dictaminó que la orden no debe haber sido emitido debido a la declaración del informante no proporcionó ninguna información adicional para corroborar la punta del informante[34].

Más tarde, en *Spinelli v. Estados Unidos*, el Tribunal Supremo dictaminó que una orden de registro es inconstitucional cuando no proporciona al juez que la emite información para evaluar si el informante era fiable[35]. El tribunal dictaminó que la policía necesita proporcionar información que corrobore que la información entregada por el informante, como es requerido por *Aguilar*, o incluir más detalles sobre el informante que muestran que él o ella es fiable.

En un caso posterior, *Illinois v. Gates*, el Tribunal Supremo, una vez más, hizo hincapié en

que la fiabilidad y la base del conocimiento de un informante es altamente relevante para determinar si la policía tiene causa probable para apoyar una orden[36]. Aunque el tribunal se apartó de la aplicación rígida de lo que se conoce como la prueba de *Aguilar-Spinelli* para informantes anónimos en una solicitud de orden de búsqueda, reafirmó que un comunicado escueto de un informante acerca de la existencia de evidencia para un crimen en una locación determinada no constituía, en si misma, causa probable para una orden de registro.

La ley también reconoce que un informante anónimo puede ser confiable en algunas circunstancias, pero no en otros. La policía debe revelar las limitaciones del informante, ya que, como ha dicho el Tribunal Supremo de los Estados Unidos v. Franks, la Cuarta Enmienda requiere sinceridad "para permitir al magistrado una evaluación independiente de la cuestión" [37].

Por ejemplo, el Cuarto Circuito emitió recientemente una orden de búsqueda después de que la policía no reveló información sobre la falta de fiabilidad de un informante. En Estados Unidos v. Lull, la policía no informa al juez que dicta la orden de registro que su informante había robado el dinero que la policía le había dado para la compra de drogas[38]. La policía admitió que el informante era fiable para la identificación del vendedor de drogas, pero no era fiable debido al robo. Pero determinar la fiabilidad del informante, el Cuarto Circuito sostuvo, era una evaluación que debía realizar el magistrado y no la policía. El mismo principio debería aplicarse a las direcciones IP porqueel hecho de que las fuerzas del orden no revelen plenamente las limitaciones de la tecnología debería ser motivo similar para anular una orden judicial.

4. Aplicación de las reglas del informante anónimo a las direcciones IP

Los tribunales y la policía deben aplicar el mismo escepticismo frente a los informantes anónimos a las direcciones IP. En su conjunto, los casos de la sección anterior requieren que cuando la policía se base en información de informantes anónimos para obtener una orden de registro, deben incluir detalles en sus solicitudes que demuestren tanto 1) la confiabilidad del informante como 2) la corroboración que la policía haya obtenido. Como el Tribunal Supremo falló en Spinelli, es necesario presentar información adicional y el trabajo policial para que los tribunales emitan órdenes sobre la base de que la policía está "confiando en algo más sustancial que un rumor ocasional que circula en el mundo subterráneo o una acusación basada simplemente en reputación general de un individuo."

Al igual que ocurre con los informantes, la información de la dirección IP que la policía proporciona en las solicitudes de autorización requiere explicar el contexto y la corroboración, incluyendo: dónde se obtuvo la información de la dirección, cómo se asignó a una ubicación física o una persona y si existen otros hechos que afecten su fiabilidad, como el listado de la dirección IP en una lista de servidores Tor. Por lo tanto, estos casos pueden proporcionar una guía para la policía, los fiscales y los tribunales en el pensamiento sobre cómo examinar la información de direcciones IP contenida en las solicitudes de búsqueda.

En el caso de la granja de Kansas que está sujeto a búsquedas policiales perpetuas, la información de localización IP proporcionada a la policía es absolutamente no fiable para unos 600 millones de direcciones, dadas las limitaciones del servicio utilizado por la policía. Como se mencionó anteriormente, incluso en lo que respecta a las direcciones que no se asignan arbitrariamente a una granja de Kansas, el sitio web de MaxMind afirma que sus diversos servicios de geolocalización tienen una precisión entre el 28 y el 44 por ciento de precisión para identificar una ubicación exacta[39]. Esas limitaciones se dan a conocer en el sitio web y deben darse a conocer a la corte. Por otra parte, incluso sin descargo de responsabilidad del sitio web, dado el gran número de delitos que antes eran "asignados" a la ubicación de la granja[40], la policía debería haber investigado más a fondo para determinar por qué esta dirección aparece continuamente, si una sola llamada de un periodista pudo revelar que era una ubicación predeterminada, sin duda una llamada de la policía pudo hacer lo mismo.

En el caso de los operadores del nodo de retransmisión de salida Tor en Seattle, la policía obtuvo una orden de registro basado casi exclusivamente en el hecho de que la pornografía infantil pasó a través de la dirección IP asociada a su hogar. Ese hecho en si, sin más corroboración, es análogo a una llamada anónima alegando que algún crimen está

ocurriendo en casa de alguien, pero no proporciona más información que corroborando esta imputación El resultado en Seattle es tanto más problemático porque Tor ofrece una lista de búsqueda de direcciones IP que se utilizan para albergar los relés de salida de la red[41]. Una búsqueda rápida habría revelado que la dirección IP bajo sospecha era poco probable que haya sido el lugar donde se originó la pornografía infantil, y la carga de la policía para hacer esta sencilla prueba es baja. Si la policía no llevará a cabo este importante paso voluntariamente, los tribunales deben exigir que se haga antes de emitir una orden.

Por lo tanto, no es correcto - y una violación de la Cuarta Enmienda - registrar la casa de un individuo basándose en simples afirmaciones de que un crimen se cometió usando una dirección IP asociada a un lugar o una persona. Las fuerzas del orden deben ser obligadas a investigar más a fondo, incluyendo la identificación de otras evidencias electrónico o físico que corroboren su teoría acerca de quela evidencia del crimen se encuentre en la ubicación física asociada con una dirección IP en particular. Y los tribunales deben ser informados de las limitaciones tecnológicas de las pruebas con el fin de evaluar de forma independiente y asegúrese de que la dirección IP es fiable antes de autorizar la intrusión de aplicación de la ley en la privacidad individual.

5. Lo que la policías y los tribunales deben hacer de manera diferente cuando se utiliza información de dirección IP

Dado que la información de la dirección IP puede ser poco fiable o no corroborada, las fuerzas del orden y los tribunales pueden necesitar cambiar sus prácticas actuales para prevenir el daño a personas inocentes y el desperdicio de recursos judiciales. Como se señaló anteriormente, la información de direcciones IP puede ser un indicador útil para la aplicación de la ley y, una vez corroborada, puede ser una pieza importante para ayudar a localizar o identificar a un sospechoso. A continuación se presentan varias recomendaciones sobre cómo la policía y los tribunales deben tratar la información de la dirección IP de manera que no impidan a la policía la investigación de los delitos, pero protegiendo los derechos de las personas, especialmente los que garantiza la Cuarta Enmienda. Para hacer más fácil la navegación, tanto para la policía y los tribunales, hemos creado listas separadas para cada uno a pesar de que las recomendaciones se superponen.

Las recomendaciones de EFF para la Policía

1. *Localización :* realizar una investigación adicional para verificar y corroborar la ubicación física de un dispositivo en particular conectado a Internet cada vez que la policía tiene información sobre la ubicación física de una dirección IP, y proporcionar está información a la cancha con la aplicación orden. Esto debe incluir:

    a. Consulta del servicio de localización que se utiliza para entender cómo funciona y donde se puede estar utilizando una ubicación predeterminada en lugar de uno real. También incluiría el aprendizaje de la fuente de los datos, la forma precisa, completa, cuan actualizada es y cómo el servicio pretende usar la información.

    b. La obtención de los registros de un proveedor de servicio local que podría proporcionar una dirección más precisa y/o

    c. Cuando sea posible, la vigilancia física de la propiedad para ver si hay indicios de delito.

2. *Identidad :* Investigar si es probable que más de una persona use la dirección IP asociada con el crimen. Es la dirección IP asociada con una cafetería, biblioteca, empresa, organización, apartamento de varias habitaciones o casa compartida

por varias personas? ¿El abonado asociado con la dirección IP proporciona una conexión inalámbrica abierta al público? Estas son cuestiones esenciales que deben ser contestadas antes de que la policía tenga una causa probable para creer que una persona asociada con una dirección IP es el sospechoso.

3. *La identidad y ubicación* : Determinar si la dirección IP está siendo utilizado como un servidor Tor salida, VPN, o un servidor proxy. Además, ¿hay alguna indicación de que alguien haya puesto en peligro el dispositivo utilizando la dirección IP en un esfuerzo por ocultar su ubicación o identidad real?. Un buen primer paso sería utilizar un servicio de búsqueda DNS inversa, que puede proporcionar información útil sobre la dirección IP. Para Tor, la policía siempre deben consultar cualquier dirección IP que se han asociado con un delito con una base de datos de todos los relés de salida Tor conocidos como ExoneraTor. Si la dirección IP sospechoso también se usa como un relé de salida de Tor, este hecho constituye información de descargo, demostrando que las pruebas del delito muy probablemente no se encuentran en la ubicación del relé. Además, dado que los nodos Tor de salida no retienen información que pueda identificar a los usuarios anteriores, no almacena información que podría ayudar en las investigaciones policiales. Sin más pruebas incriminatorias, una coincidencia entre la dirección IP sospechoso y un relé de salida de Tor debería ser una señal de alerta que no hay causa probable para buscar un lugar determinado o arrestar a cualquier persona asociada con la dirección. Como mínimo, la información de descargo debe ser incluido y explicada en una aplicación de orden para que el tribunal pueda determinar si existe una causa probable para apoyar la orden.

4. *Metáforas :* Eliminar analogías imprecisas sobre las direcciones IP de las solicitudes de ordenes de búsqueda. Analogías y metáforas del mundo real son útiles para explicar la tecnología a los tribunales y el público, pero en el contexto de las direcciones IP, la policía no debe usar analogías que exageran las capacidades de información de la dirección IP. Como mínimo, la policía debe dejar de representar las direcciones IP como suficientemente similares a direcciones fisicas de calles o placas de matrícula para justificar una orden, ya que no son asi.

5. *Exageraciones* : dejar de incluir declaraciones en solicitudes de búsqueda implicando que todos los dispositivos electrónicos conectados a Internet se identifican únicamente a través de una dirección IP. Como se discutió anteriormente, hay muchos más dispositivos conectados a Internet que direcciones IP existentes, lo que significa que los dispositivos a menudo comparten una dirección IP asociada a un router o punto de acceso a Internet. Además, estas declaraciones a menudo dan la impresión de que un solo

dispositivo y, por extensión, un individuo, está conectado a una dirección IP en particular cuando esto no es necesariamente cierto.

Los tribunales también deben desempeñar un papel más activo en el control tanto información de la dirección IP incluida en aplicaciones asimilados y afirmaciones hechas sobre la capacidad de la tecnología para identificar una ubicación o individuo en particular.

Las recomendaciones de EFF para los jueces/tribunales

1. *Localización* : cuestionar las declaraciones acerca de la exactitud de la información de localización de IP. Específicamente; ¿la policía llevó a cabo investigaciones adicionales para verificar y corroborar la ubicación física de un determinado dispositivo conectado a Internet? ¿Se obtienen la información a través de un proceso legal a un proveedor de servicios de Internet o a través de un servicio de geolocalización de IP? ¿ha entregado, la policía, esta información adicional con la solicitud de la orden? Esa información debe incluir:

    a. Descripciones de si la policía cuestionó el servicio de localización para entender cómo funciona y donde se puede estar utilizando una ubicación predeterminada en lugar de uno real. La descripción también incluiría el aprendizaje de la fuente de los datos, que tan precisa, completa, y actualizada está, y cómo la compañía pretende usar la información.

    b. Declaraciones que muestran que la policía obtuvo legalmente los registros de un proveedor de servicio local que proporcionan una dirección más precisa y / o

    c. Descripciones de si la policía llevó a cabo la vigilancia física de la propiedad y encontraron indicios del crimen o por qué habría sido poco práctico hacerlo.

2. *Identidad* : Pregunta si es probable que más de una persona haya utilizado la dirección IP proporcionada en la solicitud de orden. Un ISP podría haber reasignado la dirección IP a través del tiempo; algunos ISP podrían haberla asignado a más de un cliente a la vez; o podría estar asociado con una cafetería, biblioteca, empresa, organización, apartamento de varias habitaciones o casa compartida por varias personas. El abonado asociado con la dirección IP también podría proporcionar una conexión inalámbrica abierta al público. Estas son cuestiones esenciales que deben ser contestadas antes de que la policía tenga causa probable para creer que una persona asociada con una dirección IP es

sospechosa.

3. *Localización e Identidad* : preguntar a la policía si se comprueba si la dirección IP está siendo utilizado como un relé de salida Tor, VPN, o un servidor proxy. Como seguimiento, preguntar si existe algún indicio de que alguien ha puesto en peligro el dispositivo utilizando la dirección IP en un esfuerzo por ocultar la ubicación o la identidad real de ese individuo o si han realizado una búsqueda inversa de DNS y cuales son sus resultados. Con respecto a Tor, en ausencia de las circunstancias más exigentes, la policía debería haber dirigido la dirección IP a través de una base de datos de todos los relés de salida Tor conocidos como ExoneraTor. Preguntar si la tienen. Si la dirección está asociada con un relé de salida de Tor, este hecho es la información de descargo lo que demuestra que es poco probable que las pruebas del delito se encuentran en la ubicación del relé. La coincidencia entre la dirección IP en la solicitud de orden de búsqueda y ExoneraTor debe ser una señal de alerta de que no hay causa probable a menos que la policía tenga otra información incriminatoria. Además, dado que los nodos Tor de salida no retienen información que pueda identificar a los usuarios anteriores, que no almacena información que podría ayudar en las investigaciones policiales. Como mínimo, el tribunal debe garantizar que la policía incluyen la información de descargo en la solicitud de autorización, junto con una explicación de por qué la policía todavía creen que existe una causa probable para emitir una orden de registro.

4. *Metáforas* : Exigir a la policía explicar la tecnología y las limitaciones de las direcciones IP sin que remitirse a analogías imprecisas. En particular, los tribunales deben ser escépticos de analogías y metáforas que definen a las direcciones IP como suficientemente similares a una dirección física de calles o placas de matrícula, ya que no lo son. Estas analogías y potencialmente otras, exageran las capacidades de información de la dirección IP. Los tribunales deben rechazarlas como base para determinar si existe causa probable para emitir una orden.

5. *Exageraciones* : *rechazar las declaraciones en las aplicaciones de solicitudes de búsqueda que implican que todos los dispositivos electrónicos conectados a Internet se identifican únicamente a través de una dirección IP.* Estas declaraciones, a menudo, dan la impresión de que un solo dispositivo y, por extensión, un individuo, está conectado a una dirección IP en particular cuando esto no es necesariamente cierto. Debido a que hay muchos más dispositivos conectados a Internet que direcciones IPv4 existentes, los dispositivos a menudo comparten una dirección IP asociada a un router o punto de acceso a Internet.

[1] Kashmir Hill, *Cómo un problema técnico mapeo Internet convirtió una granja de Kansas al azar en un infierno digital*, Fusión (10 de abril, 2016), http://fusion.net/story/287592/internet-mapping-glitch-kansas-farm/ (*Historia en Fusión*)

[2] Ansel Hirsh, *Policía sale en jornada de pesca, registra la casa de defensores de la privacidad en Seattle que mantienen una Tor*, The Stranger (30 de marzo, 2016), http://www.thestranger.com/slog/2016/04/08/23914735/judge-who-authorized-police-search-of-seattle-privacy-activists-wasnt-told-they-operate-tor-network (Tor raid).

[3] *Fusión* Story, *supra*, n. 1.

[4] DOD Standard Internet Protocol, Information Sciences Institute – University of Southern California (January 1980), https://tools.ietf.org/html/rfc760#page-iii.

[5] La Internet Assigned Numbers Authority (IANA) "es responsable de la coordinación global del Protocolo de Internet frente a los sistemas, así como los Números de Sistema Autónomo utilizados para enrutar el tráfico de Internet."

[6] Por ejemplo, el grupo regional que supervisa las direcciones IP en los Estados Unidos es el Registro Americano de Números de Internet (ARIN). Ver https://www.arin.net/.

[7] *The Washington Post* tiene un gráfico informativo para explicar la distribución geográfica de las direcciones IP. Darla Cameron y Nancy Scola, *Mapeo de 4.3 mil millones de direcciones de Internet del mundo*, The Washington Post (7 Ene, 2015) https://www.washingtonpost.com/graphics/business/world-ip-addresses/.

[8] ljitsch van Beijnum, *Con las Américas terminándose el IPv4, es oficial: Internet está lleno,* ArsTechnica (June 12, 2014) http://arstechnica.com/information-technology/2014/06/with-the-americas-running-out-of-ipv4-its-official-the-internet-is-full/.

[9] Lanzamiento Mundial de IPv6, http://www.worldipv6launch.org/measurements/.

[10] NAT esencialmente crea una red privada en la que todos los dispositivos comparten una única dirección IP pública. *Ver ¿Qué es la traducción de direcciones de red?* , ¿Cuál es mi dirección IP? http://whatismyipaddress.com/nat.

[11] Esta metáfora fue usada en la solicitud de orden de búsqueda que condujo a la incursión de la activista de privacidad de Seattle que operaba un relé de salida de Tor desde su casa. Una copia de la solicitud está disponible en https://www.thestranger.com/images/blogimages/2016/04/08/1460142130-search_warrant_redacted3.pdf.

[12] Este abonado, sin embargo, puede ser que no sea necesariamente la parte responsable del tráfico de Internet en particular, por las razones discutidas en más detalle, más adelante , en la sección 2.b

[13] *Fusión* historia, *supra*, n. 1.

[14] MaxMind, GeoIP2 City Accuracy, https://www.maxmind.com/en/geoip2-city-database-accuracy (last visited August 19, 2016).

[15] MaxMind, GeoIP2 City Accuracy, https://www.maxmind.com/en/geoip2-city-database-accuracy?country=United+States&resolution=postal (last visited August 19, 2016).

[16] *Fusión* historia, *supra*, n. 1.

[17] Después de MaxMind supo de los problemas con su base de datos, se restablece la ubicación predeterminada de direcciones IP sobre las que se tiene poca información para que correspondan con las coordenadas GPS de la mitad de un lago cerca de Wichita, Kansas, en lugar de la granja en Potwin. Pero esa actualización puede no alcance a todos los usuarios de Maxmind, incluyendo agencias de la ley, ya que no actualizan sus datos con regularidad. Kashmir Hill, este es el nuevo centro digital de los Estados Unidos , Fusión (12 de abril, 2016),

http://fusion.net/story/290772/ip-mapping-maxmind-new-us-default-location/ (Digital Centrar). Los propietarios de la finca recientemente presentó una demanda contra MaxMind. Olivia Solon, familia de Kansas demanda a empresa de mapas por los años de 'infierno digital,' The Guardian (9 de agosto, 2016), https://www.theguardian.com/technology/2016/aug/09/maxmind-mapping-lawsuit-kansas-farm-ip-address.

[18]Debido a que las demandas de información de cumplimiento de la ley pueden revelar información personal sobre los individuos, EFF cree que, en algunos casos, la policía debería estar obligado a obtener una orden o, como mínimo, una orden judicial en virtud de la Ley de Comunicaciones Almacenadas, 18 USC § 2703 (d).

[19] Una empresa de geo-localización; Skyhook, utiliza datos de puntos de acceso Wi-Fi, GPS, antena y torres de telefonía celular, para mapear las ubicaciones de direcciones IP. Ver Skyhook, precisión de la ubicación,http://www.skyhookwireless.com/products/precision-location.

[20] Tor incursión, *supra* , n. 2.

[21] Tor general, Tor, https://www.torproject.org/about/overview.html.en.

[22] La gente normal usa Tor, Tor, https://www.torproject.org/about/torusers.html.en.

[23] Para un gráfico que muestra cómo funciona Tor, ver Cómo Tor funciona , Electronic Frontier Foundation https://ssd.eff.org/files/tor.png.

[24] Marcia Hoffman, *¿Por qué las direcciones IP por sí solas, no identifican a los criminales*, Electronic Frontier Foundation (24 de agosto, 2011) https://www.eff.org/deeplinks/2011/08/why-ip-addresses-alone-dont-identify-criminals.

[25] Muchas organizaciones y compañías, incluyendo EFF, están apoyando el Movimiento Inalámbrico Abierto, (OpenWireless Movement) que está diseñado para crear redes WI-FI abiertas y ubicuas para el uso público. OpenWireless Movement https://openwireless.org/.

[26]*Eligiendo la VPN que sea adecuada para usted*, Autodefensa contra la Vigilancia- Electronic Frontier Foundation, https://ssd.eff.org/en/module/choosing-vpn-thats-right-you.

[27] Federales "Se disculpan" por confundir hombre de Buffalo con sospechoso de pornografía infantil , WGRZ (Mar. 18 de, 2011), disponible en http://westside.wgrz.com/news/news/feds-apologize-mistaking-buffalo-man-kiddie-porn-suspect/53488.

[28] 296 80 FRD (EDNY 2012).

[29] *Id*. en 84.

[30] *Id*.

[31] La diferencia entre DNS y los servidores de nombres, PCNames.com (last visited Sept. 20, 2016), disponible en http://www.pcnames.com/Articles/The-Difference-Between-DNS-and-Name-Servers.

[32] El Tribunal Supremo lo resumió en Spinelli v. Estados Unidos , 393 Estados Unidos 410 (1969), abrogada en parte por *Illinois v. Gates* , 416 Estados Unidos 213 (1983), las llamadas anónimas deben ser presentados con el contexto y la corroboración de modo que la corte que emita la orden sepa que "se basa en algo más sustancial que un rumor ocasional que circula en el mundo subterráneo o una acusación basada simplemente en la reputación general de un individuo." *Spinelli*, 393 de Estados Unidos en 416.

[33] Además, dadas las limitaciones técnicas de las direcciones IP discutidos anteriormente, no debe darseles la credibilidad de informantes civiles.

[34] 378 Estados Unidos 108 (1964), https://www.law.cornell.edu/supremecourt/text/378/108.

[35] 393 Estados Unidos 410 (1969), http://caselaw.findlaw.com/us-supreme-court/393/410.html.

[36] 462 Estados Unidos 213 (1983), https://www.law.cornell.edu/supremecourt/text/462/213.

[37]438 Estados Unidos 154 (1978), https://www.law.cornell.edu/supremecourt/text/438/154.

[38] No. 15-4216 (4th Cir. May 25, 2016), http://law.justia.com/cases/federal/appellate-courts/ca4/15-4216/15-4216-2016-05-25.html.
[39] *Supra*, n. 7.
[40] Digital Center, *supra*, n. 9.
[41] ExoneraTor, https://exonerator.torproject.org/.