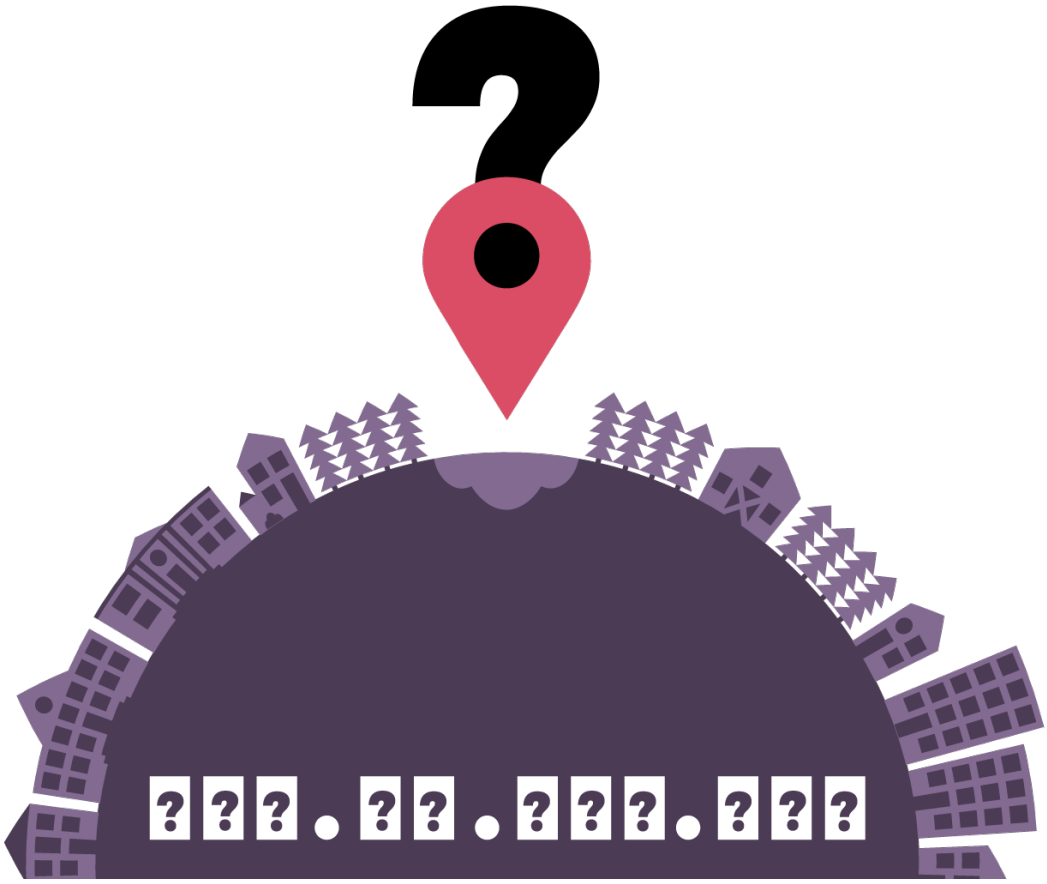

Unreliable Informants: IP Addresses, Digital Tips and Police Raids

How Police and Courts are Misusing Unreliable IP Address Information and What They Can Do to Better Verify Electronic Tips

Aaron Mackey, Frank Stanton Legal Fellow
Seth Schoen, Senior Staff Technologist
Cindy Cohn, Executive Director

September 2016

Table of Contents

Introduction

> They've been accused of being identity thieves, spammers, scammers and fraudsters. They've gotten visited by FBI agents, federal marshals, IRS collectors, ambulances searching for suicidal veterans, and police officers searching for runaway children. They've found people scrounging around in their barn. The renters have been doxxed, their names and addresses posted on the internet by vigilantes. Once, someone left a broken toilet in the driveway as a strange, indefinite threat.[1]
> *- How an internet mapping glitch turned a random Kansas farm into a digital hell*

> At 6 a.m. on March 30, Seattle police showed up at the Queen Anne apartment of Jan Bultmann and David Robinson with a search warrant to look for child porn, based on a tip that traced an illicit video to their IP address. Six officers arrived with two vans and spent over an hour doing forensic searches on the computers in the home. One officer stood in the bedroom and watched as Robinson got dressed.[2]
> *- Police go on fishing expedition, search the home of Seattle privacy activists who maintain Tor network*

> In 2012, he came home late one night to find the police about to break down his door. They said they were looking for a stolen government laptop with personal information on it. . . . He's gotten angry phone calls and Facebook messages from strangers who've been wronged by someone online. When they track the IP addresses associated with their assailants, they point to his house, so they assume its occupants are responsible.[3]
> *- 17 million IP addresses pointing to a house in Ashburn, Virginia*

The digital revolution has given law enforcement more tools to help track and identify us than ever before. Yet as law enforcement increasingly relies on electronic evidence to investigate crimes, one of the most readily available tools, Internet Protocol addresses (IP addresses), have become increasingly misused and misunderstood by law enforcement and judges alike. Law enforcement too often overstates the reliability of IP address information in seeking warrants and other process (such as subpoenas), using metaphors that create a sense of certainty where it does not always exist. Additionally, courts often don't know what questions to ask about IP address information or how to evaluate its reliability.

Although IP addresses can sometimes be reliable indicators of locations or individuals when combined with other information, such as ISP records, use of the IP address alone, without more, can too often result in dangerous, frightening, and resource-wasting police raids based on warrants issued without proper investigation. This risk is especially high when: (1) determining a suspect's physical location and (2) identifying an individual suspect responsible for a crime.

This paper explains how law enforcement and courts can use IP addresses responsibly in criminal investigations and provides specific suggestions to assist each of them. The well-developed body of law around the reliability of anonymous informants provides a good model for cops and judges seeking to rely on IP addresses. In short, when police rely on information from anonymous informants to obtain a search warrant, they need to include details in their applications demonstrating both the 1) informant's reliability and similar context and 2) corroboration that the police have obtained.

We also strongly recommend that law enforcement stop using, and courts stop relying on metaphors like physical mailing addresses or license plates when describing IP addresses in warrant applications and elsewhere. The metaphors incorrectly characterize the function and reliability of IP addresses and they potentially operate to overstate the accuracy of IP address information.

This paper is divided into five sections. First, it explains what cops and courts need to know about IP address technology so that they can correctly use it in investigations. Second, it describes why IP addresses alone cannot reliably locate or identify a suspect using two recent high-profile examples. Third, it describes how the settled law concerning tips from informants provides a good model for how cops and courts should treat IP address information. Fourth, it shows how the informant rules can be applied to IP addresses. Fifth, it provides specific recommendations for both law enforcement and courts when IP addresses are used as part of criminal investigations.

1. The Limitations of IP Addresses Should Restrict How Police Use them in Investigations

Law enforcement's use of IP addresses to identify a particular location or individual is problematic because of the limited technical purpose of the technology. IP addresses are strings of numbers used to identify a device on the Internet and to route traffic to that address. By design, IP addresses were "specifically limited in scope to provide the functions necessary" for the Internet to properly deliver traffic, which today includes emails, websites, and streaming video.[4] The simplicity of IP addresses is in part what makes it possible for the Internet to quickly route traffic around the world. That simplicity, however, comes with limitations for using the technology in other contexts.

First, the technology was never designed to uniquely identify an exact physical location, only an electronic destination on the Internet. During the Internet's infancy, designers wanted to make sure traffic could be easily routed anywhere in the world. As part of the traffic routing, network operators can announce their ability to reach particular destinations, but these announcements are made on a numerical, not geographic, basis. A coordinating body has assigned blocks of IP addresses to regions throughout the world.[5] Below the regional level, ISPs are usually in charge of assigning IP addresses, but an IP address does not inherently "belong to" a particular country. Nor does it have to be used in or from a physical location or area or by an end user of a particular ISP.[6]

At a local level, similar IP addresses may be assigned based on geography, albeit only indirectly. ISPs make decisions to allocate blocks of IP addresses to particular locations for a variety of reasons, with the goal of creating a network that efficiently delivers Internet traffic. The result may be that locations near each other feature similar IP addresses, but that is more often the product of where the provider has physical links and routers to a network than geography. For example, if an ISP has a fiber-optic link between two distant cities, the IP addresses assigned to those cities may be similar because it creates a more efficient network. A third city near one of those towns geographically may not share the same connection and it would thus likely have completely different IP addresses assigned to it.

Although databases that track IP address allocations do exist, their comprehensiveness, contents, and the significance of an allocation can very widely. In short, there is no central map or phonebook that connects IP addresses to particular locations, particularly given that IP addresses are often reassigned to different Internet users over time. There's also no uniform way to systematically map physical locations based on IP addresses; although some mapping techniques may be extremely accurate for some addresses, the resulting maps are

not "official" and will not be completely comprehensive. Thus, IP address information, by itself, serves as an inconsistent tool for law enforcement or anyone to identify an exact location.

Second, using an IP address to identify a specific individual is problematic because there is nothing about the addresses themselves that make them personally identifiable. IP addresses identify particular devices or groups of devices on the Internet, not people using the Internet. In some cases, it may make sense to conclude that a single person is associated with a device connected to the Internet, but that is often not the case in real-world situations.

The difficulty of equating an IP address with any person is demonstrated by the fact that in developed, urbanized countries such as the United States, there are more devices connecting to the Internet today than there are available addresses in the most widely used version of the Internet Protocol, IPv4.[7] When the Internet was initially designed, the sequence used for IPv4 addresses allowed for 4.3 billion unique addresses, a total that seemed unimaginably high.[8] The incredible growth of the Internet combined with the development of personal and mobile computing – where most people in the United States use multiple devices daily – has outgrown the number of IPv4 addresses. And although there is a new version of the Internet Protocol, IPv6, with a dramatically larger pool of addresses than IPv4, the adoption rate of IPv6 addresses remains only 30 percent of users in the United States.[9]

As a result of demand for Internet connections outpacing the number of IPv4 addresses, Internet service providers are increasingly forced to split the limited pool of those IP addresses among their larger customer base. Thus when customers first use the service provider to access the Internet, they may connect through an IP address that was previously, or possibly even simultaneously, used by someone else. Depending on how frequently that individual uses the connection, the service provider may keep the same IP address assigned to that account or reassign it to another customer if there is demand elsewhere. And over time, the service provider may reassign the IP address for any number of reasons. In short, unlike street addresses, IP addresses are not static.

Further, given this IP address crunch, technologies have been created that allow multiple devices and users to share a single IP address. The most common example is Network Address Translation (NAT), which is used in household routers and by some ISPs (typically mobile carriers).[10] The technology essentially places the public IP address at a level above a specific individual or user.

Metaphors Can Compound the Problem

Given the limitations of IP addresses described above, analogies used to compare the technology to other types of personal or geographic identifiers often break down. For

example, police often include statements in warrant applications claiming that IP addresses are like physical street addresses. This is half true, in the sense that both IP addresses and street addresses are used for routing messages to their destinations. Yet the analogy implies that IP addresses are static and identify a particular house or location on a physical map, which is not always true. Police using this metaphor give a court the false impression that IP addresses are unique to exact places in the physical world, and that there is a permanence connecting the IP address to that location. It also wrongly suggests the existence of a clear, predictable procedure to be followed to determine the location in every case, as might be done for a street address given an authoritative map of a city.

The analogy also suggests that IP addresses can provide precise information about an individual associated with an IP address when, as discussed above, this is not always true. The street address metaphor breaks down further because IP addresses and physical addresses are assigned quite differently. Physical addresses are assigned based on geography, meaning that people living next to each other share some common address characteristics, such as the same street name. With IP addresses, two people living next to each other may be using IP addresses that have almost nothing in common because, for example, they use different ISPs (which have different pools of IP addresses) or they use proxy servers or Virtual Private Networks (VPNs).

Another faulty metaphor used by law enforcement is the notion that IP addresses are like vehicle license plates.[11] License plates serve vastly different purposes than IP addresses. License plates are designed to be uniquely identifiable and can be tracked by authorities for public safety and law enforcement. The government also assigns license plates to individuals, in contrast to private parties assigning IP addresses to their customers or users. It is generally illegal to change license plates without obtaining permission from the government or to hide them so law enforcement cannot readily identify vehicles. IP addresses, however, were not designed to be uniquely identifiable and can be shared by several people or devices simultaneously, or reused over time by different people accessing the Internet, as discussed above. It's also completely legal for Internet users to mask or share their IP addresses, unlike license plate numbers.

With the limitations of IP addresses to identify individuals and locations described here, the next section uses two recent cases that demonstrate why those limitations can cause severe invasions of individuals' privacy.

2. The Dangers of Using IP Addresses to Locate or Identify Suspects

As the three anecdotes provided in the introduction demonstrate, overreliance on the ability of IP address information, without more, to locate or identify criminal suspects is harming innocent people. A deeper dive into two of those cases helps flesh out the problem.

Before discussing those cases, it's important to emphasize that with proper corroboration, law enforcement's use of IP addresses to identify a particular location or individual can be quite reliable. For example, one method of corroboration of an IP address with a physical address or an individual is to obtain records from an Internet Service Provider (ISP). The corroboration comes from the additional information that an ISP has about users of an IP address, including billing records.[12] In many instances, of course, technically savvy police are already doing this. An alternative method of linking IP address to physical locations, known as IP geo-location and discussed in more detail below, can also be very reliable in some specific situations.

What the examples below demonstrate, however, is that there is no reliable formula that allows law enforcement to jump from a suspect IP address to a specific place or person. Instead, the reliability of using information derived from an IP address in investigations depends on a number of factors that are often outside of law enforcement's control and that some IP address investigative techniques might not be fruitful in particular situations.

Location: Why IP Addresses Alone are Not Always Location Proxies

The *Fusion* story describes how law enforcement and private parties' misuse of unreliable IP address information has subjected residents of a farm in the middle of the United States to nearly perpetual harassment.[13] This is because police are misinterpreting data that purports to identify specific physical locations based on IP addresses when the technology is actually telling cops that it has almost no idea where the IP address is physically located.

Private companies have built businesses off of matching IP addresses with physical locations. At a high level, the information is useful to many people and businesses. For instance, it can help a businesses see what country the most traffic to their websites appears to be coming from, which can help the business decide when to make a foreign-language version of the website available. These IP mapping companies have, over time, become much more accurate at linking particular IP addresses with physical locations in some circumstances, often as a result of combining IP addresses with other location data. This type of matching,

known as IP geo-location, can sometimes be a reasonable kind of corroboration, but the technique is still evolving. Examining the accuracy and reliability of all IP geo-location services used by law enforcement and private industries is beyond the scope of this paper. What media reports have shown, however, is that law enforcement's reliance on one geo-location service, MaxMind, is misplaced because police are overestimating the reliability of IP geo-location results provided by the service.

Currently, although most geo-location services can accurately identify that an IP address is originating from a particular country or region of the world, their accuracy can vary dramatically when attempting to precisely locate an IP address in a particular state, city, or physical address. Companies like MaxMind generally do provide information about the limitations of their services, so that contextual and reliability measure is readily available for the police and courts. The companies are also likely to give estimates for how precise its location information is for any particular IP address or range of addresses. For instance, as of the date of publication of this paper in September, 2016, MaxMind states that its location data is, on average, 87 percent accurate when it comes to identifying that a particular IP address is located in the United States,[14] but only between 28-44 percent accurate for matching an IP address with an exact location.[15] Again, this is not to say that MaxMind's data may be much more precise for particular queries – it is only used as an example of the general limitations inherent in IP geo-location services.

The specific, troubling harassment suffered by inhabitants of the farm described in the *Fusion* story results from what MaxMind does with IP addresses for which it has no reasonable location data at all. For the more than 600 million IP addresses for which MaxMind has no specific information other than they are likely located somewhere in the United States,[16] the service defaults to matching the address' physical location with the GPS coordinates in the middle of the country. That location, until a recent change, turned out to be the single farm in the small town of Potwin, Kansas.[17]

This feature of MaxMind's IP geo-location service is why police have time and again erroneously concluded that residents of the farm are responsible for a bevy of crimes over the past decade. Police are misconstruing a null result for 600 million IP addresses to mean that the precise location of hundreds of devices connected to the Internet is this farm. But the data is actually telling them the complete opposite – that the service has no idea where the addresses are actually located inside the United States.

The *Fusion* story underscores why police need to use IP geo-location information as the starting place – and not the conclusion – for locating a suspect and supports the need for corroboration. As noted above, many police actually do use IP addresses only as an initial clue. The most common next step is one we recommend: that police then issue process to an ISP to match a particular IP address with a physical location.[18] Unlike IP geo-location

services like MaxMind, ISPs are generally able to provide a corresponding customer address that matches to an IP address used at a particular time, given that most have made a business decision to record such information as a matter of course. When location information is obtained from an ISP to connect a particular physical address of a subscriber with an IP address, that information can be a very reliable indicator of location of a fixed broadband ISP subscriber, albeit not necessarily of a specific user, as described further below.

Mobile carriers providing Internet services to customers may have additional information about an individuals' location based on features of its service, compared to fixed broadband ISPs. For example, carriers may be able to identify individual devices using its network rather than particular subscribers. Mobile carriers may also be able to gain a more precise picture of an individual's location over time. But this just reinforces the point that police and judges must understand the nature of the information they receive

MaxMind actually does some of this follow up itself currently and it may do more in the future. Other IP geo-location companies can and do use other, more complex technical means to more precisely match IP addresses with physical locations. These methods include trace routing, having devices report GPS fixes from particular IP addresses, or using real-world physical investigations to actually match an IP address more closely with a physical location.[19] Even then, however, the information may not identify an exact street address or unit number and likely won't be a reliable identifier of a particular person.

Identity: The Problem with Relying on IP Addresses as Identity Equivalents or Why IP Addresses are Not Identity Proxies

Police are also overestimating the ability of IP address information to actually identify that a specific individual is responsible for a crime committed online, a leap that has harmed completely innocent people. To be clear, there are some circumstances in which an IP address may be enough to identify a person using a device. But as discussed below, at least some additional corroborating evidence is usually needed.

Earlier this year, Seattle police raided the home of two privacy activists after getting a tip that an IP address associated with the couple's Internet provider was used in a crime.[20] It turns out that the activists were hosting a Tor exit relay in their home, which meant that the police raided innocent people.

Tor is an anonymizing service designed to protect individual privacy that masks the IP addresses of its users and then routes traffic through exit relays operated by volunteers.[21] Tor and its volunteer exit relay operators provide an important public service for political dissidents, activists, or anyone who wants to browse the web anonymously.[22] A key feature

of Tor is that the individuals operating its exit relays, which are the last computers the Tor traffic goes through before reaching its final destination, have no control or knowledge of the Internet activity coming through the relays.[23]

So when police learn of a crime connected to an IP address from a Tor exit relay, there is little chance that the criminal is actually associated with that IP address. Police have failed to recognize this reality in multiple cases in which they have searched the homes of Tor exit relay hosts and seized their devices.[24]

What the cases underscore is that police too often take IP address information to mean that a person associated with an address is the party who committed a crime. For many reasons, connecting an individual to a crime linked to an IP address, without any additional investigation, is irresponsible and threatens the civil liberties of innocent people.

The problem of using an IP address as an identity proxy for criminality ascribed to the person associated with a particular address is not limited to Tor. With companies and individuals operating open wireless networks out of their homes, cafés, public libraries, and businesses, they often have very little control or knowledge of the Internet activities of the people using their connections.[25] Other services, such as Virtual Private Networks (VPNs) and proxy servers, also can make IP addresses unreliable indicators of the identity and/or location of a particular person.[26]

Police have similarly raided locations providing open wireless networks after erroneously concluding that the account holder was responsible for a crime. In Buffalo, N.Y., police raided a man's home and arrested him after tracing child pornography to his home network.[27] It turned out, however, that a neighbor was using the open wireless connection to download the illegal content.

All of these technologies underscore how the public IP address associated with a device will generally change when that device is used on a different Internet connection. It is important for law enforcement and courts to understand this evolution in how people connect to the Internet, because it means that the IP address assigned to a particular subscriber may include the traffic of many other people, and some of them may be thousands of miles away from the physical location of the subscriber.

Perhaps one of the most cogent explanations of why individuals cannot be equated with IP addresses came from U.S. Magistrate Judge Gary Brown's order in *BitTorrent Adult Film Copyright Infringement Cases*.[28] In granting several motions to quash subpoenas for subscriber information linked to IP addresses identified in several copyright infringement lawsuits, Judge Brown held that "the assumption that the person who pays for Internet access at a given location is the same individual who allegedly downloaded a single sexually

explicit film is tenuous, and one that has grown more so over time."[29] Judge Brown continued "Thus, it is no more likely that the subscriber to an IP address carried out a particular computer function—here the purported illegal downloading of a single pornographic film—than to say an individual who pays the telephone bill made a specific telephone call."[30]

Police should therefore think about IP addresses as helpful clues that may locate criminal activity within a particular geographic region or lead to an individual suspect. They should also recognize that there are quick, easy steps they can take to learn more about a particular IP address. One easy example is to use a reverse Domain Name System (DNS) lookup of an IP address. DNS is a massive database that compiles the Internet's IP address and website domain names, enabling everyone to find websites based on their names rather than the string of numbers that comprise an IP address.[31] A reverse DNS lookup can reveal useful information, such as name and contact information of the party who registered the domain. Plugging an IP address into a reverse DNS lookup service may thus provide additional information about the address.

EFF recognizes that many police already treat IP addresses as the starting point in their investigations and do more work before seeking a warrant. But for others in law enforcement, this is not always the case. Police must therefore understand that IP addresses alone are not always reliable enough to pinpoint an exact location or individual because the technology was never built for those functions. With a better understanding of why IP addresses alone can be unreliable, the paper now provides a legal framework for courts and police to use when using the information in warrants.

3. IP Address Information is a Lot Like Informants' Tips to Police

IP address information is unreliable in identifying specific locations or identities and this unreliability should be addressed under the law as well. A helpful legal model is the case law regarding anonymous informants, where the law has long recognized both that they can be useful to police but also that there are Fourth Amendment dangers inherent in relying upon anonymous tips too heavily or without a proper understanding of the broader context.

Under the Fourth Amendment, courts have long recognized that police cannot obtain warrants based solely on rumors or anonymous tips they receive from informants.[32] Although the burden of proof needed by police to obtain a warrant necessary to conduct a raid on someone's home or office is much lower than what is needed to convict someone, law enforcement must still demonstrate that they have probable cause. Determining what amounts to probable cause is not a rigorous scientific analysis; rather, it a common-sense conclusion that follows from analyzing all the facts and circumstances police have included in their warrant applications.

In a line of Supreme Court cases dealing with reliability and corroboration problems that arise whenever third parties provide tips to law enforcement, the court has made clear that police must do more to confirm the tips provided by anonymous informants before seeking a warrant or other process, and it outlined a series of requirements.[33]

For example, in *Aguilar v. State of Texas*, the Supreme Court ruled that the warrant should not have been issued because the informant's statement did not provide any additional information to corroborate the informant's tip.[34]

Later, in *Spinelli v. United States*, the Supreme Court ruled that a search warrant is unconstitutional when it does not provide the issuing judge with information to assess whether the informant was reliable.[35] The court ruled that police either needed to provide corroborating information that supported the informant's tip as required by *Aguilar* or include more details about the informant that would show he or she was reliable.

In a subsequent case, *Illinois v. Gates*, the Supreme Court once more stressed that an informant's reliability and basis of knowledge remain highly relevant in determining whether police have probable cause to support a warrant.[36] Although the court backed away from rigid application of what became known as the *Aguilar-Spinelli* test for anonymous informant information in a warrant application, it reaffirmed that a bare-bones statement from an informant that there was evidence of a crime at a particular location would not, by

itself, create probable cause for a search warrant.

The law also recognizes that an anonymous informant may be reliable in some circumstances but not in others. Police must disclose the informant's limitations because, as the Supreme Court said in *U.S. v. Franks*, the Fourth Amendment requires candor "to allow the magistrate to make an independent evaluation of the matter."[37]

For example, the Fourth Circuit recently tossed a search warrant after the police failed to disclose information about an informant's unreliability. In *United States v. Lull,* police did not tell the judge issuing the search warrant that their informant had stolen money that police had given him to purchase drugs.[38] Police admitted that the informant was reliable for identifying the drug dealer but was not reliable because of the theft. But determining the informant's reliability, the Fourth Circuit held, was an assessment for the magistrate – and not the police – to make. The same principle should apply to IP addresses: law enforcement's failure to fully disclose the technology's limitations should similarly be grounds for voiding a warrant.

4. Applying the Anonymous Informant Rules to IP Addresses

Courts and police must apply the same skepticism of anonymous informants to IP addresses. Taken together, the cases in the previous section require that when police rely on information from anonymous informants to obtain a search warrant, they need to include details in their applications demonstrating both the 1) informant's reliability and 2) corroboration that the police have obtained. As the Supreme Court ruled in *Spinelli*, additional information and police work is necessary so that courts issuing warrants know that police are "relying on something more substantial than a casual rumor circulating in the underworld or an accusation based merely on an individual's general reputation."

As with informants, the IP address information that police provide in warrant applications requires explaining the context and corroboration, including: where the address information was obtained, how that was mapped to a physical location or a person, and whether there are other facts that bear on its reliability, such as the listing of the IP address on a Tor server list. Thus, these cases can provide a guide for police, prosecutors and courts in thinking about how to scrutinize IP address information contained in warrant applications.

In the case of the Kansas farm that is subject to perpetual police searches, the IP location information provided to police is completely unreliable for some 600 million addresses, given the limitations of the service used by the police. As mentioned above, even as to addresses that are not arbitrarily assigned to a Kansas farm, MaxMind's website states that its various geo-location services are between 28-44 percent accurate for identifying an exact location.[39] Those limitations are disclosed on the website and should be disclosed to the court. Moreover, even without the website's disclaimer, given the vast numbers of crimes that were previously "mapped" to the farm's location,[40] the police should have investigated further to determine why this address came up – if a single call from a reporter can reveal that this is a default location, surely a call from the police could uncover the same.

In the case of the Tor exit relay operators in Seattle, police obtained a search warrant based almost entirely on the fact that child pornography came across the IP address associated with their home. That fact alone, without further corroboration, is analogous to an anonymous tip that alleges some criminality is occurring at someone's home but provides no further information to corroborate the claim. The result in Seattle is all the more problematic because Tor provides a searchable list of IP addresses that are used to host the network's exit relays.[41] A quick search would have revealed that the suspected IP address was unlikely to have been the place where the child porn originated, and the burden on the

police in doing this simple check is low. If the police won't undertake this important step voluntarily, courts should demand it be done prior to issuing a warrant.

Thus, it is wrong – and a Fourth Amendment violation – to search an individual's home based on bare assertions that some crime was committed using an IP address associated with a location or a person. Law enforcement must be required to investigate further, including identifying other electronic or physical evidence that corroborates their theory that evidence of the crime is likely to be found at the physical location that is associated with a particular IP address. And courts must be informed of the technological limitations of the evidence so that they can independently ensure that IP address information is reliable before authorizing law enforcement intrusion into individual privacy.

5. What Cops and Courts Should Do Differently When Using IP Address Information

Given that IP address information can be unreliable or uncorroborated, law enforcement and courts may need to change their current practices to prevent harm to innocent parties and wasting judicial resources. As noted above, IP address information can be a useful indicator for law enforcement and, with corroboration, can be an important piece in helping locate or identify a suspect. Below are several recommendations for how police and the courts should treat IP address information in ways that do not prevent police from investigating crime but still protects people's rights, especially those guaranteed by the Fourth Amendment. To make this easier for police and courts to navigate, we've created separate lists for each, although the recommendations overlap.

EFF's recommendations for Police:

1. *Location*: Conduct additional investigation to verify and corroborate the physical location of a particular device connected to the Internet whenever police have information about an IP address' physical location, and providing that information to the court with the warrant application. This should include:

    a. Querying the location service that is being used to understand how it works and where it may be using a default location rather than an actual one. It would also include learning the source of the data, how precise, complete, and up to date they are, and how the service intended the data to be used.

    b. Obtaining records from a local service provider that could provide a more precise address and/or

    c. When practical, conducting physical surveillance of the property to see if there are indicia of a crime.

2. *Identity*: Investigate whether it is likely that more than one person uses the IP address associated with the crime. Is the IP address associated with a café, library, business, organization, multi-room apartment, or house shared by several people? Does the subscriber associated with the IP address provide an open wireless connection to the public? These are essential questions that must be answered before police have probable cause to believe that an individual

associated with an IP address is the suspect.

3. *Identity and Location*: Determine whether the IP address is being used as a Tor exit relay, VPN, or proxy server. Additionally, is there any indication that someone has compromised the device using that IP address in an effort to obscure their actual location or identity? A good first step would be use a reverse DNS lookup service, which may provide useful information about the IP address. For Tor, police should always check whatever IP address they have associated with a crime with a database of all Tor exit relays known as ExoneraTor. If the suspect IP address is also used as a Tor exit relay, that fact is exculpatory information demonstrating that evidence of the crime is unlikely to be found at the location of the relay. Further, because Tor exit nodes do not retain information that would identify previous users, it does not store information that could assist police investigations. Without more incriminating evidence, a match between the suspect IP address and a Tor exit relay should be a red flag that there is not probable cause to search a particular location or arrest anyone associated with the address. At minimum, the exculpatory information must be included and explained in a warrant application to allow the court to determine whether there is probable cause to support the warrant.

4. *Metaphors*: Remove imprecise analogies about IP addresses from warrant applications. Real-world analogies and metaphors are useful to explaining technology to courts and the public, but in the context of IP addresses, police should not use analogies that overstate the capabilities of IP address information. At minimum, police should stop representing IP addresses as sufficiently similar to a physical street addresses or license plates to justify a warrant, since they are neither.

5. *Overstatements*: Stop including statements in warrant applications implying that every electronic device connected to the Internet is uniquely identifiable via an IP address. As discussed above, there are many more devices connected to the Internet than there are IP addresses, meaning that devices often share an IP address associated with a router or other Internet access point. Further, the statements often give the impression that a single device and, by extension, an individual, is connected to a particular IP address when that is not necessarily true.

Courts also must play a more active role in scrutinizing both IP address information included in warrant applications and claims made about the technology's ability to identify a particular location or individual.

EFF's recommendations for Judges/Courts:

1. *Location*: Question claims about the accuracy of IP location information. Specifically, did police conduct additional investigation to verify and corroborate the physical location of a particular device connected to the Internet? Did they obtain the information via legal process to an Internet Service Provider or through an IP geo-location service? Did police provide that additional information to the court with the warrant application? That additional information should include:

    a. Descriptions of whether the police queried the location service to understand how it works and where it may be using a default location rather than an actual one. The description would also include learning the source of the data, how precise, complete, and up to date they are, and how the service intended the data to be used.

    b. Statements showing that police lawfully obtained records from a local service provider that provide a more precise address and/or

    c. Descriptions of whether police conducted physical surveillance of the property and found indicia of the crime or why it would have been impractical to do so.

2. *Identity*: Ask whether it is likely that more than one person will have used the IP address provided in the warrant application. An ISP could have reassigned the IP address over time; some ISPs could have assigned it to more than one customer at a time; or it could be associated with a café, library, business, organization, multi-room apartment, or house shared by several people. The subscriber associated with the IP address could also provide an open wireless connection to the public. These are essential questions that must be answered before police have probable cause to believe that an individual associated with an IP address is the suspect.

3. *Location and Identity*: Ask police if they checked whether the IP address is being used as a Tor exit relay, VPN, or proxy server. As follow ups, ask if there is any indication that someone has compromised the device using that IP address in an effort to obscure that individual's actual location or identity, or if they conducted a reverse DNS lookup (and what the results were). With respect to Tor, absent the most exigent circumstances, police should have run the IP address through a database of all Tor exit relays known as ExoneraTor. Ask if

they have. If the address is associated with a Tor exit relay, that fact is exculpatory information demonstrating that evidence of the crime is unlikely to be found at the location of the relay. The match between the IP address in the warrant application and ExoneraTor should be a red flag that there is not probable cause unless police have other incriminating information. Further, because Tor exit nodes do not retain information that would identify previous users, it does not store information that could assist police investigations. At minimum, the court should ensure that police included the exculpatory information in the warrant application, along with an explanation as to why police still believe there is probable cause to issue a search warrant.

4. *Metaphors*: Require police to explain the technology and limitations of IP addresses without resulting to imprecise analogies. In particular, courts should be skeptical of analogies and metaphors that compare IP addresses as sufficiently similar to a physical street addresses or license plates, since they are neither. These analogies, and potentially others, overstate the capabilities of IP address information. Courts should reject them as a basis for determining whether there is probable cause to issue a warrant.

5. *Overstatements*: Push back against statements in warrant applications implying that every electronic device connected to the Internet is uniquely identifiable via an IP address. The statements often give the impression that a single device and, by extension, an individual, is connected to a particular IP address when that is not necessarily true. Because there are many more devices connected to the Internet than there are IPv4 addresses, devices often share an IP address associated with a router or other Internet access point.

---

[1] Kashmir Hill, *How an internet mapping glitch turned a random Kansas farm into a digital hell*, Fusion (April 10, 2016), http://fusion.net/story/287592/internet-mapping-glitch-kansas-farm/ (*Fusion* Story).

[2] Ansel Herz, *Police Go on Fishing Expedition, Search the Home of Seattle Privacy Activists Who Maintain Tor Network*, The Stranger (March 30, 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] *Fusion* 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] The Internet Assigned Numbers Authority (IANA) "is responsible for global coordination of the Internet Protocol addressing systems, as well as the Autonomous System Numbers used for

routing Internet traffic." Number Resources, Internet Assigned Numbers Authority, https://www.iana.org/numbers.

[6] For example, the regional group overseeing IP addresses in the United States is the American Registry for Internet Numbers (ARIN). *See* https://www.arin.net/.

[7] *The Washington Post* has an informative graphic to explain the geographic breakdown of IP addresses. Darla Cameron & Nancy Scola, *Mapping the world's 4.3 billion Internet addresses*, The Washington Post (Jan 7, 2015) https://www.washingtonpost.com/graphics/business/world-ip-addresses/.

[8] Iljitsch van Beijnum, *With the Americas running out of IPv4, it's official: the Internet is full*, 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] World IPv6 Launch, http://www.worldipv6launch.org/measurements/.

[10] NAT essentially creates a private network in which all devices share a single public IP address. *See What is Network Address Translation?*, What is my IP Address? http://whatismyipaddress.com/nat.

[11] This metaphor was used in the warrant application that led to the raid of the Seattle privacy activist who operated a Tor exit relay from his home. A copy of the application is available at https://www.thestranger.com/images/blogimages/2016/04/08/1460142130-search_warrant_redacted3.pdf.

[12] That subscriber, however, may still not necessarily be the party responsible for particular Internet traffic, for the reasons discussed in more detail, *infra*, in Section 2.B.

[13] *Fusion* story, *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] *Fusion* Story, *supra*, n. 1.

[17] After MaxMind learned about the problems with its database, it reset the default location for IP addresses it has little information on to correspond with the GPS coordinates of the middle of a lake near Wichita, Kansas, rather than the farm in Potwin. But that update may not trickle down to all of MaxMind's users, including law enforcement agencies, because they do not update their data regularly. Kashmir Hill, *This is the new digital center of the United States*, Fusion (April 12, 2016), http://fusion.net/story/290772/ip-mapping-maxmind-new-us-default-location/ (Digital Center). The owners of the farm recently filed a lawsuit against MaxMind. Olivia Solon, *Kansa family sues mapping company for years of 'digital hell,'* The Guardian (Aug. 9, 2016), https://www.theguardian.com/technology/2016/aug/09/maxmind-mapping-lawsuit-kansas-farm-ip-address.

[18] Because law enforcement information demands may reveal personal information about individuals, EFF believes that in some instances, law enforcement should be required to obtain a warrant or, at minimum, a court order under the Stored Communications Act, 18 U.S.C. § 2703(d).

[19] One geo-location firm, Skyhook, uses data from Wi-Fi access points, GPS antenna, and cell phone towers, to map the locations of IP addresses. *See* Skyhook, Precision Location, http://www.skyhookwireless.com/products/precision-location.

[20] Tor raid, *supra*, n. 2.

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

[22] Normal People Use Tor, Tor, https://www.torproject.org/about/torusers.html.en.

[23] For a graphic showing how Tor works, see *How Tor Works*, Electronic Frontier Foundation https://ssd.eff.org/files/tor.png.
[24] Marcia Hoffman, *Why IP Addresses Alone Don't Identify Criminals*, Electronic Frontier Foundation (Aug. 24, 2011) https://www.eff.org/deeplinks/2011/08/why-ip-addresses-alone-dont-identify-criminals.
[25] Many organizations and companies, including EFF, are supporting the Open Wireless Movement, which is designed to create ubiquitous open Wi-Fi networks for public use. Open Wireless Movement https://openwireless.org/.
[26] *Choosing the VPN That's Right for You*, Surveillance Self-Defense – Electronic Frontier Foundation, https://ssd.eff.org/en/module/choosing-vpn-thats-right-you.
[27] *Feds "Apologize" For Mistaking Buffalo Man For Kiddie Porn Suspect*, WGRZ (Mar. 18, 2011), *available at* http://westside.wgrz.com/news/news/feds-apologize-mistaking-buffalo-man-kiddie-porn-suspect/53488.
[28] 296 F.R.D. 80 (E.D.N.Y. 2012).
[29] *Id.* at 84.
[30] *Id.*
[31] *The Difference Between DNS and Name Servers*, PCNames.com (last visited Sept. 20, 2016), *available at* http://www.pcnames.com/Articles/The-Difference-Between-DNS-and-Name-Servers.
[32] The Supreme Court put it succinctly in *Spinelli v. United States*, 393 U.S. 410 (1969), *abrogated in part by Illinois v. Gates*, 416 U.S. 213 (1983), that anonymous tips must be presented with context and corroboration so that the court issuing the warrant knows that it "is relying on something more substantial than a casual rumor circulating in the underworld or an accusation based merely on an individual's general reputation." *Spinelli*, 393 U.S. at 416.
[33] Moreover, given the technical limitations of IP addresses discussed above, they should not be given the credibility of civilian informants.
[34] 378 U.S. 108 (1964), https://www.law.cornell.edu/supremecourt/text/378/108.
[35] 393 U.S. 410 (1969), http://caselaw.findlaw.com/us-supreme-court/393/410.html.
[36] 462 U.S. 213 (1983), https://www.law.cornell.edu/supremecourt/text/462/213.
[37] 438 U.S. 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/.