NATIONAL PULSE

Inaccurate leads from IP addresses prompt police to serve warrants on innocent people

POSTED MAY 01, 2017 02:10 AM CDT

BY JASON TASHEA

On the morning of March 30, 2016, David Robinson and his partner, Jan Bultmann, were starting their day when six Seattle police officers knocked on their door with a search warrant. The police thought Robinson was trafficking child pornography. Still in bed when police arrived at 6:15 a.m., Robinson got dressed as an officer stood in the bedroom.

According to Robinson, the police spent 90 minutes searching his apartment and electronic devices. They also interrogated him and his partner in separate police vans parked in front of their building in the Queen Anne neighborhood.

The Seattle Police Department was working off a tip from the National Center for Missing & Exploited Children that an IP address, the unique identifier produced by every computer or computer network, was tied to Robinson's name and physical address and was used in the upload and transfer of child pornography.

After finding no evidence of child pornography, the police left without making an arrest. The incident left Robinson feeling "afraid" and "furious." Seattle police declined to comment for this story.

DAMAGED PROTECTIONS

Over the past 20 years, the internet has altered every aspect of society, including the challenges of obtaining a warrant. While police departments work to keep abreast of a technological landscape in flux, advocates worry that technology is outstripping procedure-and damaging the warrant process and its protections.

Tor is software that legally allows people to privately surf the internet by being randomly routed through various computers around the world. (Its name comes from the Tor Project's original name, "The Onion Router.")

Tor is promoted by the Department of State to help dissidents get access to the internet in repressive societies, such as China, Egypt and Russia. It's also used by privacy advocates to browse the internet without corporate or government tracking and can be used to disseminate illegal material, such as child pornography.

In Robinson's case, someone transferring child pornography was randomly routed through his IP address, similar to an illicit package through a random post office. The exit node, which Robinson says he set up as a service to people online who want to browse privately, allows a person being routed through Tor to connect to the internet.

The advent of Tor, along with proxy servers and mobile access to the internet, has made IP addresses less reliable for law enforcement investigating online crimes. "It's gotten more challenging," says Chuck Cohen, a captain with the Indiana State Police. He served his first subpoena for IP logs, the list of users who visit a website, in 1995. He was investigating the online sale of knockoff sunglasses.

"Back then it was easy," Cohen says. He says an IP address would lead him to the internet provider who would then release data about the customer tied to the address. This worked in the '90s because IP addresses were primarily static. Today, however, due largely to mobile access of the internet, Cohen says, IP logs are less useful.

CAUGHT UP IN THE SCENE

The combination of old tactics alongside new technology had led to innocent bystanders being caught up in criminal investigations. For more than a decade, MaxMind, an IP addressing company based in Waltham, Massachusetts, had been incorrectly and repeatedly leading law enforcement to a farm in Kansas in search of identity thieves, suicidal veterans and runaway children.

This happened because the farm's physical address was MaxMind's U.S. default location, a catchall for when the company knew an IP address was from the United States but could not get more specific. The family who moved to the farm in 2011 dealt with the IP addressing havoc for five years and filed a complaint last year.

This example informed the Electronic Frontier Foundation's September report that calls attention to the challenges that IP addresses create in criminal investigations.

"It's not just an education problem; it's also a constitutional problem," says Aaron Mackey, a legal fellow at the **EFF** and co-author of the paper. The education problem is that courts and law enforcement have to understand how IP addresses have changed, Mackey says. It is a constitutional issue because an IP address alone is often insufficient for a probable cause warrant, he says.

Both issues coalesce for Mackey in what he says is the incorrect use of certain analogies. He says it's misleading when police seek a warrant and try to equate IP addresses with physical locators, such as a street address or a vehicle license plate.

Mackey argues that an IP address is more analogous to an anonymous informant. "Anonymous tips can be right, but they can also be wrong," Mackey says. "In the same way, an IP address can sometimes identify an individual, but in a lot of circumstances they don't." Drawing out his preferred analogy, he says anonymous informants provide tips that require further police work to secure a warrant, and IP addresses should be no different.

The prevalence of this problem is hard to ascertain. For his research, Mackey says he examined several instances nationwide in which an IP address was used incorrectly to obtain a search warrant. However, he thinks this issue will become "more prevalent, as police are investigating more crimes online."

The inability to quantify this problem is a result of decentralized criminal justice data collection. Also, using an IP address to get a warrant is the exception rather than the rule, according to Cohen.

"On step one, we are going to see if [the IP address] is a Tor exit node," Cohen says. To help police differentiate between criminals and privacy activists such as Robinson, the Tor Project created the ExoneraTor service, which allows anyone to see whether an IP address was used as a Tor relay on the day in question. According to Robinson, the Seattle police knew he operated an exit relay.

Cohen says that if an IP address is shown to be a Tor exit node, then "that lead becomes a dead end" in the investigation.

He makes clear, however, "with 800,000 police officers [nationwide], it's not realistic for them to have that technical background." But, he says, this process and others are "widely known" among officers whom departments rely on to undertake these types of investigations.

'LUCKY' CRIMINALS

Offering a lawyer's perspective is Matthew Esworthy, a criminal defense and civil commercial litigator in Baltimore. Esworthy says he has seen Tor cases that involve child pornography in which criminals used computers to accomplish their crimes. But "that seems to be the exception to the rule," he says.

Also the co-chair of the ABA's cybercrime committee, Esworthy thinks online crime is so prolific that "law enforcement doesn't want to waste their time going after locations that aren't going to bear fruit."

From police officer Cohen's point of view, the challenge in using IP addresses to help obtain a warrant is about whether the address is collected at all. 'There is no federal law on retention of IP records," he says.

Federal lawmakers failed to create a standard for retention in 1999 and 2009. By comparison, the European Union passed the Data Retention Directive in 2006, requiring data to be kept for a minimum of six months and a maximum of two years.

Domestically, service providers can retain IP address information for as long as they want, if at all. One major internet provider, for example, keeps its records for 72 hours before it erases them. To this end, Cohen says that if you are a "lucky" criminal with a provider that does not retain IP information, then "you don't get caught."

This article originally appeared in the May 2017 issue of the ABA Journal *with this headline: "Net Search and Seizure: Inaccurate leads from IP addresses prompt police to serve warrants on innocent people.•*