Why IP Addresses Alone Don't Identify Criminals

This spring, agents from Immigration and Customs Enforcement (ICE) executed a search warrant at the home of Nolan King and seized six computer hard drives in connection with a criminal investigation. The warrant was issued on the basis of an Internet Protocol (IP) address that traced back to an account connected to Mr. King's home, where he was operating a Tor exit relay.

An exit relay is the last computer that Tor traffic goes through before it reaches its destination. Because Tor traffic exits through these computers, their IP addresses may be misinterpreted as the source of the traffic, even though the exit node operator is neither the true origin of that traffic nor able to identify the user who is. While law enforcement officers have seized exit relays in other countries, we weren't aware of any seizures in the United States until ICE showed up at Mr. King's home.

After the computers were seized, EFF spoke with ICE and explained that Mr. King was running a Tor exit relay in his home. We pointed out that ICE could confirm on the Tor Project's web site that a computer associated with the IP address listed in the warrant was highly likely to have been running an exit relay at the date and time listed in the warrant. ICE later returned the hard drives, warning Mr. King that "this could happen again." After EFF sent a letter, however, ICE confirmed that it hadn't retained any data from the computer and that Mr. King is no longer a person of interest in the investigation.

While we think it's important to let the public know about this unfortunate event, it doesn't change our belief that running a Tor exit relay is legal. And it's worth highlighting the fact that these unnecessary incidents are avoidable, and law enforcement agents and relay operators alike can take measures to avoid them in the future.

First, an IP address doesn't automatically identify a criminal suspect. It's just a unique address for a device connected to the Internet, much like a street address identifies a building. In most cases, an IP address will identify a router that one or more computers use to connect to the Internet. Sometimes a router's IP address might correspond fairly well to a specific user—for example, a person who lives alone and has a password-protected wireless network. And tracking the IP addresses associated with a person over time can create a detailed portrait of her movements and activities in private spaces, as we've pointed out in a case in which the government is seeking IP addresses of several Twitter users in connection with the criminal investigation of Wikileaks.

But in many situations, an IP address isn't personally identifying at all. When it traces back to a router that connects to many computers at a library, cafe, university, or to an open wireless network, VPN or Tor exit relay used by any number of people, an IP address alone doesn't identify the sender of a specific message. And because of pervasive problems like botnets and malware, suspect IP addresses increasingly turn out to be mere stepping stones for the person actually "using" the computer—a person who is nowhere nearby.
This means an IP address is not probable cause that a person has committed a crime. Furthermore, search warrants executed solely on the basis of IP addresses have a significant likelihood of wasting officers' time and resources rather than producing helpful leads.

In the case of Tor, the police can avoid mistakenly pursuing exit relay operators by checking the IP addresses that emerge in their investigations against publicly available lists of exit relays published on the Tor Project's website. The ExoneraTor is another tool that allows anyone to quickly and easily see whether a Tor exit relay was likely to have been running at a particular IP address during a given date and time. The Tor Project can also help law enforcement agencies set up their own systems to query IP addresses easily. These simple checks will help officers concentrate their investigative resources on tracking down those actually committing crimes and ensure that they don't execute search warrants at innocent people's homes.

If you run an exit relay, consider operating it in a Tor-friendly commercial facility instead of your home to make it less likely that law enforcement agents will show up at your door. Also follow the Tor Project's advice for running an exit relay, which includes setting up a reverse DNS name for your IP address that makes it clear your computer is running an exit relay.

To learn more about the legal issues surrounding Tor, read EFF's Legal FAQ for Tor Relay Operators.

---

**MORE DEEPLINKS POSTS LIKE THIS**

**MAY 2012**

**UPDATE: With May First/Riseup Server Seizure, FBI Overreaches Yet Again**

**JULY 2011**

**EFF Campaign Increases the Number of Tor Relays by 13.4%**

**JUNE 2011**

**Achievement Unlocked: Set Up Tor Relays, Get a Molly Crabapple Poster**

**JUNE 2009**

**Help Protesters in Iran: Run a Tor Bridge or a Tor Relay**

**MAY 2012**

**EFF is Joining the Transition to IPv6**

---

**RECENT DEEPLINKS POSTS**

**OCT 31, 2013**

**Six Good Things About the Innovation Act: Part One, Heightened Pleading**

**OCT 31, 2013**

**Congress Must Not Fast Track TPP to Ratification**

**OCT 30, 2013**

**EFF Urga a la Comisión Inter-Americana que Tome Acción Contra los Programas de Vigilancia Masiva de los Estados Unidos**

**OCT 30, 2013**

**Fifth Amendment Prohibits Compelled Decryption, New EFF Brief Argues**

---