



AUGUST 24, 2011 | BY [MARCIA HOFMANN \(/ABOUT/STAFF/MARCIA-HOFMANN\)](#)

## 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](#) ([https://secure.wikimedia.org/wikipedia/en/wiki/IP\\_address](https://secure.wikimedia.org/wikipedia/en/wiki/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](#) (<http://boingboing.net/2006/09/10/report-german-police.html>) [countries](#) (<http://www.techdirt.com/articles/20110530/22003714465/austrian-police-seize-computers-tor-exit-node.shtml>), we weren't aware of any seizures in the United States until ICE showed up at Mr. King's home.

(UPDATE: A reader points us to this [blog post](#) (<http://toddsnotes.blogspot.com/2009/11/because-i-ran-tor-police-took-all-my.html>) detailing a Tor exit relay seizure in the United States in 2009.)

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](#) (<https://metrics.torproject.org/exonerator.html>) 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](#) (<https://www.eff.org/cases/government-demands-twitter-records>) 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.

[Donate to EFF](#)

(<https://supporters.eff.org/do>)

---

### Stay in Touch

Email Address

Postal Code (optional)

**SIGN UP NOW**

---

### NSA Spying



[eff.org/nsa-spying](#)

([/nsa-spying](#))

EFF is leading the fight against the NSA's illegal mass surveillance program. [Learn more \(/nsa-spying\)](#) about what the program is, how it works and what you can do.

---

### Follow EFF

Trolls should be clear about which product is infringing which patent. The Innovation Act makes sure of it: <https://eff.org/r.c9hf> (<https://eff.org/r.c9hf>)

OCT 31 @ 12:23PM

It's almost time for @EFF's SF Bay Area member meetup! Check your inbox for details on our fall Speakeasy.

<https://eff.org/r.3chd> (<https://eff.org/r.3chd>)

OCT 31 @ 11:59AM

Senate Finance leaders call for #TPP to get fast-tracked through Congress without any proper hearings.

<https://eff.org/r.c6hc> (<https://eff.org/r.c6hc>)

OCT 31 @ 10:42AM

[Twitter](#) (<https://twitter.com/eff>)

[Facebook](#) (<https://www.facebook.com/eff>)  
[Identi.ca](#) (<https://identi.ca/eff>)

---

### Projects

[Bloggers' Rights \(/bloggers\)](#)

This means an IP address is nothing more than a piece of information, a clue. An IP address alone 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](#) (<https://metrics.torproject.org/data.html#exitlist>) of exit relays published on the Tor Project's web site. The [ExoneraTor](#) (<https://metrics.torproject.org/exonerator.html>) 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](#) (<https://trac.torproject.org/projects/tor/wiki/doc/GoodBadISPs>) 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](#) (<https://blog.torproject.org/blog/tips-running-exit-node-minimal-harassment>) 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](#) (<https://www.eff.org/torchallenge/legal-faq>).

[Privacy \(/issues/privacy\)](#) [Anonymity \(/issues/anonymity\)](#)

[Follow EFF \(/social-networks\)](#)

[Free Speech Weak Links \(/free-speech-weak-link\)](#)

[Global Chokepoints \(https://globalchokepoints.org/\)](#)

[HTTPS Everywhere \(/https-everywhere\)](#)

[Open Wireless Movement \(https://openwireless.org\)](#)

[Patent Busting \(https://w2.eff.org/patent/\)](#)

[Surveillance Self-Defense \(https://ssd.eff.org\)](#)

[Takedown Hall of Shame \(/takedowns\)](#)

[Teaching Copyright \(http://www.teachingcopyright.org/\)](#)

[Transparency Project \(https://www.eff.org/issues/transparency\)](#)

[Trolling Effects \(https://trollingeffects.org\)](#)

[Ways To Help \(/helpout\)](#)

## MORE DEEPLINKS POSTS LIKE THIS

MAY 2012

[UPDATE: With May First/Riseup Server Seizure, FBI Overreaches Yet Again \(/deeplinks/2012/04/may-first-riseup-server-seizure-fbi-overreaches-yet-again\)](#)

JULY 2011

[EFF Campaign Increases the Number of Tor Relays by 13.4% \(/deeplinks/2011/07/eff-campaign-increases-number-tor-relays-13-4\)](#)

JUNE 2011

[Achievement Unlocked: Set Up Tor Relays, Get a Molly Crabapple Poster \(/deeplinks/2011/06/achievement-unlocked-set-up-tor-relays-get-a-molly-crabapple-poster\)](#)

JUNE 2009

[Help Protesters in Iran: Run a Tor Bridge or a Tor Relay \(/deeplinks/2009/06/help-protesters-iran-run-tor-relays-bridges\)](#)

MAY 2012

[EFF is Joining the Transition to IPv6 \(/deeplinks/2012/05/eff-joining-transition-ipv6\)](#)

## RECENT DEEPLINKS POSTS

OCT 31, 2013

[Six Good Things About the Innovation Act: Part One, Heightened Pleading \(/deeplinks/2013/10/six-good-things-about-innovation-act-part-one-heightened-pleading\)](#)

OCT 31, 2013

[Congress Must Not Fast Track TPP to Ratification \(/deeplinks/2013/10/congress-must-not-fast-track-tpp-ratification\)](#)

OCT 30, 2013

[EFF Urge a la Comision Inter-Americana que Tome Acción Contra los Programas de Vigilancia Masiva de los Estados Unidos \(/es/deeplinks/2013/10/eff-CIDH-vigilancia-NSA\)](#)

OCT 30, 2013

[Fifth Amendment Prohibits Compelled Decryption, New EFF Brief Argues \(/deeplinks/2013/10/new-eff-amicus-brief-argues-fifth-amendment-prohibits-compelled-decryption\)](#)

OCT 30, 2013

[Trolls, Watch Out: Senator Hatch Introduces New Patent Legislation \(/deeplinks/2013/10/trolls-watch-out-senator-hatch-introduces-new-patent-legislation\)](#)

# date visited 10/31/13

[Analog Hole \(/deeplinks/analog-hole\)](#)  
[Anonymity \(/deeplinks/anonymity\)](#)  
[Anti-Counterfeiting Trade Agreement \(/deeplinks/anti-counterfeiting-trade-agreement\)](#)  
[Biometrics \(/deeplinks/biometrics\)](#)  
[Bloggers Under Fire \(/deeplinks/bloggers-under-fire\)](#)  
[Bloggers' Rights \(/deeplinks/bloggers%27-rights\)](#)  
[Broadcast Flag \(/deeplinks/broadcast-flag\)](#)  
[Broadcasting Treaty \(/deeplinks/broadcasting-treaty\)](#)  
[CALEA \(/deeplinks/calea\)](#)  
[Cell Tracking \(/deeplinks/cell-tracking\)](#)  
[Coders' Rights Project \(/deeplinks/coders%27-rights-project\)](#)  
[Computer Fraud And Abuse Act Reform \(/deeplinks/computer-fraud-and-abuse-act-reform\)](#)  
[Content Blocking \(/deeplinks/content-blocking\)](#)  
[Copyright Trolls \(/deeplinks/copyright-trolls\)](#)  
[Council of Europe \(/deeplinks/council-of-europe\)](#)  
[Cyber Security Legislation \(/deeplinks/cyber-security-legislation\)](#)  
[CyberSLAPP \(/deeplinks/cyberslapp\)](#)  
[Development Agenda \(/deeplinks/development-agenda\)](#)  
[Digital Books \(/deeplinks/digital-books\)](#)  
[Digital Radio \(/deeplinks/digital-radio\)](#)  
[Digital Video \(/deeplinks/digital-video\)](#)  
[DMCA \(/deeplinks/dmca\)](#)  
[DMCA Rulemaking \(/deeplinks/dmca-rulemaking\)](#)  
[Do Not Track \(/deeplinks/do-not-track\)](#)  
[DRM \(/deeplinks/drm\)](#)  
[E-Voting Rights \(/deeplinks/e-voting-rights\)](#)  
[EFF Europe \(/deeplinks/eff-europe\)](#)  
[EFF Software Projects \(/deeplinks/eff-software-projects\)](#)  
[Encrypting the Web \(/deeplinks/encrypting-the-web\)](#)

[Export Controls \(/deeplinks/export-controls\)](#)  
[FAQs for Lodsyst Targets \(/deeplinks/faqs-for-lodsyst-targets\)](#)  
[File Sharing \(/deeplinks/file-sharing\)](#)  
[Free Speech \(/deeplinks/free-speech\)](#)  
[FTAA \(/deeplinks/ftaa\)](#)  
[Hollywood v. DVD \(/deeplinks/hollywood-v.-dvd\)](#)  
[How Patents Hinder Innovation \(Graphic\) \(/deeplinks/how-patents-hinder-innovation-%28graphic%29\)](#)  
[Innovation \(/deeplinks/innovation\)](#)  
[Intellectual Property \(/deeplinks/intellectual-property\)](#)  
[International \(/deeplinks/international\)](#)  
[International Privacy Standards \(/deeplinks/international-privacy-standards\)](#)  
[Internet Governance Forum \(/deeplinks/internet-governance-forum\)](#)  
[Legislative Solutions for Patent Reform \(/deeplinks/legislative-solutions-for-patent-reform\)](#)  
[Locational Privacy \(/deeplinks/locational-privacy\)](#)  
[Mandatory Data Retention \(/deeplinks/mandatory-data-retention\)](#)  
[Mandatory National IDs and Biometric Databases \(/deeplinks/mandatory-national-ids-and-biometric-databases\)](#)  
[Mass Surveillance Technologies \(/deeplinks/mass-surveillance-technologies\)](#)  
[National Security Letters \(/deeplinks/national-security-letters\)](#)  
[Net Neutrality \(/deeplinks/net-neutrality\)](#)  
[No Downtime for Free Speech \(/deeplinks/no-downtime-for-free-speech\)](#)  
[NSA Spying \(/deeplinks/nsa-spying\)](#)  
[OECD \(/deeplinks/oecd\)](#)  
[Online Behavioral Tracking \(/deeplinks/online-behavioral-tracking\)](#)  
[Open Access \(/deeplinks/open-access\)](#)  
[Open Wireless \(/deeplinks/open-wireless\)](#)  
[Patent Busting Project \(/deeplinks/patent-busting-project\)](#)  
[Patent Trolls \(/deeplinks/patent-trolls\)](#)  
[Patents \(/deeplinks/patents\)](#)  
[PATRIOT Act \(/deeplinks/patriot-act\)](#)

[Pen Trap \(/deeplinks/pen-trap\)](#)  
[Policy Analysis \(/deeplinks/policy-analysis\)](#)  
[Printers \(/deeplinks/printers\)](#)  
[Privacy \(/deeplinks/privacy\)](#)  
[Reading Accessibility \(/deeplinks/reading-accessibility\)](#)  
[Real ID \(/deeplinks/real-id\)](#)  
[RFID \(/deeplinks/rfid\)](#)  
[Search Engines \(/deeplinks/search-engines\)](#)  
[Search Incident to Arrest \(/deeplinks/search-incident-to-arrest\)](#)  
[Section 230 of the Communications Decency Act \(/deeplinks/section-230-of-the-communications-decency-act\)](#)  
[Security \(/deeplinks/security\)](#)  
[Social Networks \(/deeplinks/social-networks\)](#)  
[SOPA/PIPA: Internet Blacklist Legislation \(/deeplinks/sopa/pipa%3A-internet-blacklist-legislation\)](#)  
[State Surveillance & Human Rights \(/deeplinks/state-surveillance-%26-human-rights\)](#)  
[State-Sponsored Malware \(/deeplinks/state-sponsored-malware\)](#)  
[Surveillance Drones \(/deeplinks/surveillance-drones\)](#)  
[Terms Of \(Ab\)Use \(/deeplinks/terms-of-%28ab%29use\)](#)  
[Test Your ISP \(/deeplinks/test-your-isp\)](#)  
[The "Six Strikes" Copyright Surveillance Machine \(/deeplinks/the-%22six-strikes%22-copyright-surveillance-machine\)](#)  
[The Global Network Initiative \(/deeplinks/the-global-network-initiative\)](#)  
[Trans-Pacific Partnership Agreement \(/deeplinks/trans-pacific-partnership-agreement\)](#)  
[Transparency \(/deeplinks/transparency\)](#)  
[Travel Screening \(/deeplinks/travel-screening\)](#)  
[Trusted Computing \(/deeplinks/trusted-computing\)](#)  
[Uncategorized \(/deeplinks/uncategorized\)](#)  
[Video Games \(/deeplinks/video-games\)](#)  
[Wikileaks \(/deeplinks/wikileaks\)](#)  
[WIPO \(/deeplinks/wipo\)](#)  
[Broadcast Flag \(/deeplinks/broadcast-flag\)](#)

# date visited 10/31/13



<https://www.eff.org/copyright>

[Thanks \(/thanks\)](#) | [RSS Feeds \(/rss\)](#) | [Copyright Policy \(/copyright\)](#)

| [Privacy Policy \(/policy\)](#) | [Contact EFF \(/about/contact\)](#)