Courts, DOJ: Using Tor Doesn't Give You A Greater Expectation Of Privacy

Techdirt

February 29, 2016 Monday 8:11 PM EST

Length: 1440 words

Byline: Tim Cushing

Body

Feb 29, 2016(Techdirt: *http://www.techdirt.com* Delivered by Newstex) When is a reasonable expectation of privacy unreasonable? When the government says it is. In this month alone, we've had two federal judges and the DOJ state that there's no expectation of privacy in IP addresses. This would normally be something covered by the Third Party Doctrine -- where an IP address is part of the records retained by ISPs, and therefore, can be accessed with subpoenas rather than warrants.

The twist, though, is that all of these statements were made in reference to people who made an active effort to obscure their IP addresses by using Tor. On February 1st, the judge presiding over the Jay Michaud case -- the one where the FBI (for the second time in recent history) ran a child porn website[1] for two weeks in order to gather evidence on visitors to the site -- stated that Tor users had no reasonable expectation of privac[2]y, despite their privacy-protecting efforts. Michaud was challenging the FBI's use of a standard warrant to deploy its NIT (Network Investigative Technique) -- a piece of malware that gathered information about computers connecting to the child porn website. US district judge Robert J. Bryan denied the motion[3], noting that while the warrant technically violated the rule, a higher court's interpretation provides an exception for when the information sought could have been discovered by 'other lawful means." To prove this, the judge bizarrely argued that Tor doesn't give its users complete anonymity because a user has to give their IP address to their Internet Service Provider to connect to the Tor network. Therefore, he concluded, Michaud's IP address was 'public information, like an unlisted telephone number' that 'eventually could have been discovered.' In doing this, the judge agreed with the assertions the DOJ made in its earlier motion[4]. The DOJ claimed Michaud's IP address was something he shared with third parties -- despite his use of Tor -- and was info the government would have eventually discovered one way or another, even without the use of its controversial hacking tool. '[E]ven if a defendant wants to seek to hide his Internet Protocol address through the use of Tor, that does not cloak the IP address with an expectation of privacy,' the government wrote, in a statement very similar to the opinion later written by Judge Bryan. 'While Michaud may have a reasonable expectation of privacy in stored information contained on his computer, he lacks a reasonable expectation of privacy in IP address information that belongs to an internet service provider and that is voluntarily shared with others in the course of Internet communications.' The interesting thing about this assertion is that Michaud voluntarily shared his IP address with others. It would seem fairly obvious there was nothing "voluntary" about this exposure. While it's true that IP addresses are "shared" with Tor when connecting, that information is stripped from communications as they travel through the Tor network. The government argued the NIT merely rerouted this information to the FBI before Tor stripped it. Michaud apparently should have known his use of a privacy-protecting network would perhaps expose his IP address to others, including the FBI. But as Tor itself states[5], without intervention from other parties, this information would not be

collected by Tor, nor passed along its network. It is clear that the court does not understand how the Tor network works. The entire purpose of the network is to enable users to communicate privately and securely. While it is true that users ″disclose information, including their IP addresses, to unknown individuals running Tor nodes,″ that information gets stripped from messages as they pass through Tor's private network pathways. This statement is in response to another judge's declaration that people who utilize additional privacy protections when browsing the web still have no expectation of privacy in their IP addresses. This nearly-identical assertion was made by the judge presiding over the Silk Road 2.0 prosecution of Brian Farrell. In this case, the Defense Department (home of the NSA!) paid Carnegie Mellon[6] researchers to attack the Tor network in order to expose identifying info about its users. The FBI followed along behind the DoD, firing off subpoenas to obtain this newly-discovered information. The judge in this case wrote[7]: From the record, it appears the only information passed on to law enforcement about the defendant was his IP address. There is nothing presented by the defense, other than rank speculation, that anything more was obtained by SEI and provided to law enforcement to identify the defendant. The Court agrees with the government that applicable Ninth Circuit authority precludes the defendant's success on his motion. SEI's identification of the defendant's IP address because of his use of the Tor network did not constitute a search subject to Fourth Amendment scrutiny. The Court reaches this conclusion primarily upon reliance on United States v. Forrester, 512 F.2d 500 (9th Cir. 2007). In Forrester, the court clearly enunciated that: 'Internet users have no expectation of privacy in …the IP address of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.' The court goes on to say it's too bad Tor users expected more protection from the service, but their expectations are not ″reasonable″ under the Fourth Amendment. In the instant case, it is the Court's understanding that in order for a prospective user to use the Tor network they must disclose information, including their IP addresses, to unknown individuals running Tor nodes, so that their communications can be directed toward their destinations. Under such a system, an individual would necessarily be disclosing his identifying information to complete strangers. Again, according to the parties' submissions, such a submission is made despite the understanding communicated by the Tor Project that the Tor network has vulnerabilities and that users might not remain anonymous. Under these circumstances Tor users clearly lack a reasonable expectation of privacy in their IP addresses while using the Tor network. In other words, they are taking a significant gamble on any real expectation of privacy under these circumstances. A subjective expectation of privacy is in no way comparable to the historic view of the objective, reasonable expectation of privacy. Tor users may be taking extra steps to obscure their IP addresses, but two court rulings clearly state the judicial system won't be granting them any ″extra″ protection from government subpoenas. In fact, these rulings simply make it easier for the government to defend the intrusive techniques it deploys to unmask Tor users by declaring that, underneath it all, it's all about IP addresses, rather than users taking proactive steps to better protect their privacy. It's not quite a blank check for hacking, but it's close. As long as the target is information not historically awarded Fourth Amendment protections, courts will be hard-pressed to question the means used to achieve these ends. Permalink[8] | Comments[9] | Email This Story[10] [1]: *https://www.techdirt.com/articles/20160126/14535433436/courts-pretty-much-ok-with-fbis-occasional-stints-as-child-porn-distributors.shtml* [2]: *http://motherboard.vice.com/read/confused-judge-says-you-have-no-expectation-of-privacy-when-using-tor-playpen-fbi-michaud* [3]: *https://assets.documentcloud.org/documents/2699886/140-Michaud-Order-Denying-Mtn-to-Suppress.pdf* [4]: *http://motherboard.vice.com/read/justice-department-to-judge-tor-users-have-no-expectation-of-privacy-playpen* [5]: *https://*

blog.torproject.org/blog/statement-tor-project-re-courts-february-23-order-us-v-farrell [6]: *https://www.techdirt.com/articles/20160225/07295633707/silk-road-20-court-docs-show-us-government-paid-carnegie-mellon-researchers-to-unmask-tor-users.shtml* [7]: *https://assets.documentcloud.org/documents/2721237/Order-Denying-Motion-to-Compel.pdf* [8]: *https://www.techdirt.com/articles/20160228/15011333749/courts-doj-using-tor-doesnt-give-you-greater-expectation-privacy.shtml* [9]: *https://www.techdirt.com/articles/20160228/15011333749/courts-doj-using-tor-doesnt-give-you-greater-expectation-privacy.shtml#comments* [10]: *https://www.techdirt.com/articles/20160228/15011333749/courts-doj-using-tor-doesnt-give-you-greater-expectati*

Classification

Language: English

Publication-Type: Web Blog

Journal Code: DIRT-0001

Subject: JUDGES (90%); PRIVACY RIGHTS (90%); SPECIAL INVESTIGATIVE FORCES (90%); INVESTIGATIONS (77%); PORNOGRAPHY (73%); SUBPOENAS (70%); CHILD PORNOGRAPHY (68%); EDITORIALS & OPINIONS (50%)

Organization: FEDERAL BUREAU OF INVESTIGATION (83%)

Industry: COMPUTER NETWORKS (89%); NETWORK PROTOCOLS (77%); INTERNET & WWW (77%); HIDDEN WEB (77%); INTERNET SERVICE PROVIDERS (76%); MALICIOUS SOFTWARE (73%)

Geographic: UNITED STATES (79%)

Load-Date: February 29, 2016