Courts Pretty Much OK With FBI's Occasional Stints As Child Porn Distributors

Techdirt

January 27, 2016 Wednesday 8:59 PM EST

Length: 1544 words

Byline: Tim Cushing

Body

Jan 27, 2016(Techdirt: *http://www.techdirt.com* Delivered by Newstex) Law enforcement agencies commit criminal acts while conducting criminal investigations. It happens all the time. With the blessing of their handlers, confidential informants[1] routinely engage in criminal activity. Investigators act as co-conspirators[2] in the planning of terrorist attacks and the robbing of imaginary ″stash houses.″[3] But many people are taking issue with the FBI's decision to use seized servers loaded with child pornography as honeypots rather than immediately shut them down.

For some, this is the one unforgivable criminal act -- the possession and distribution of child porn. This is something the FBI has done twice (that we know of). The first time was back in 2012, when it seized a server in Bellevue, Nebraska linked to a website called ″PedoBook.″ It ran the site for three weeks[4] while it deployed a Network Investigative Tool to find out more info about its users. It did it again in 2015. Joseph Cox of Motherboard was the first to cover it[5], detailing the FBI's two-week stint[6] as the new hosts of ″Playpen,″ another child porn site accessible only to users utilizing the Tor browser. Again, the FBI deployed its NIT to gather information on the site's visitors. One of those caught in the latest sting is arguing[7] the FBI participated in criminal activity, tainting the evidence it seized. [T]he Government engaged in illegal conduct by aiding and abetting the distribution of child pornography; and, considering the Fourth Amendment's core reasonableness requirements and the totality of the circumstances, it obtained an unprecedently overbroad general warrant. This is one of several arguments Jay Michaud's attorney is raising. It's also being argued that the use of the NIT violated Rule 41, which governs the use of search warrants. Michaud claims the FBI violated Rule 41's territorial limits by using its control of a server in Virginia (where the NIT warrant was issued) to access Michaud's computer in Vancouver, Washington. The defense has never questioned the Government's authority to seize 'mere evidence,' assuming that other requirements of Rule 41 and the Constitution are complied with. Rather, this case involves the territorial limitations of Rule 41, a matter completely unaffected by the enactment of § 3103(a). Finally, it is important to note that the Government has not disputed that Rule 41 applies to the NIT warrant or argued that some other law alters or expands the Rule's requirement. Instead, the Government has argued that the Rule is 'flexible,' despite its plain language, and has proposed several novel and unpersuasive interpretations of the Rule that cannot be reconciled with that language. In sum, nothing in either of these statutes in any way alters or undercuts the territorial limitations of Rule 41 and thus have no relevance when applied to the facts of this case. The Rule 41 approach was also explored[8] by Joshua Welch, who was swept up in the FBI's 2012 operation. It was of limited success. While the Eighth Circuit Appeals Court found the NIT warrant fell under Rule 41's time limit of notification of search warrant targets (30 days), it was not enough to offset other evidence gathered by the FBI. We assume, without deciding, that Rule 41 applies to the NIT warrant. The statute authorizing the magistrate judge to delay

notice is perfectly clear-the thirty day extension runs from the execution of the warrant. 18 U.S.C. § 3103a(b)(3). This occurred on November 19, 2012, meaning notice was to be provided within thirty days of that date. Moreover, the ″notice″ provided by the government was insufficient. The government points to a hearing Welch attended in which an agent testified about the NIT and to the entry of the residential search warrant into evidence as notice ″provided during the discovery process.″ But under Rule 41 Welch should have been given a copy of the NIT warrant. Of course it is plainly true that if agents were required to send a copy of the warrant to the subscriber address they obtained before they could search the premises and identify the individual user, Welch would have had ample time to flee prosecution, destroy or tamper with evidence, and otherwise seriously jeopardize the investigation. But these special considerations would have allowed for the magistrate judge to either specify a later date certain, which he did not do, or for the government to return for extensions of time under § 3103a(c), which it did not do. Therefore, the notice given Welch failed to comport with Rule 41. If the FBI's use of NITs, especially in conjunction with its decision to act as interim administrators for seized child porn websites, is going to be challenged, Rule 41 seems to be the angle to take. The other route -- challenging the FBI's forays into child porn distribution -- seems far less likely to succeed. The courts have granted a lot of leeway to law enforcement agencies who engage in illegal activities during the course of investigations, as USA Today's Brad Heath has been pointing out on Twitter[9]. The FBI ″hired a heroin-addicted prostitute″ to become intimate with a suspect and get him to sell drugs. Court: OK. pic.twitter.com/0MbaBJu3xn[10] — Brad Heath (@bradheath) January 21, 2016[11] The FBI ″hired a heroin-addicted prostitute″ to become intimate with a suspect and get him to sell drugs. Court: OK. Federal courts have given the government wide latitude to break the law in pursuit of criminals. From a #DOJ[12] brief: pic.twitter.com/pZ8WiNtqJm[13] — Brad Heath (@bradheath) January 21, 2016[14] The footnote pictured in the tweet reads: E.g., United States v. Esch, 832 F.2d 531 (10th Cir. 1987) (holding that it was not outrageous government conduct to create a pedophilic organization, advertise for members, and encourage those members to create child pornography). The latter would seem to be even more reprehensible than simply running an existing child porn site and allowing users to upload and download child porn. In the 1987 case, the FBI actually encouraged the production of child pornography. Yet the court found no reason to question or discourage this behavior. ; And there will always be other examples of highly-questionable activity engaged in by law enforcement during criminal investigations. An entire cottage industry of sting operations is predicated on pushing potential suspects towards committing criminal behavior and arresting them before the imaginary scheme can be carried out. In stash house robbery cases, the contents of the house to be robbed are limited only to creativity of the agents participating in the sting. Prison terms are predicated on these nonexistent items, allowing the government to send someone away for decades for almost robbing an empty house. While it is undoubtedly true the FBI would not have been able to uncover the identities of these child porn site visitors without allowing the site to run, one has to question whether it was all worth it. In the two weeks it participated in the hosting and distribution of child porn, 100,000 visitors were logged. But so far, it has only resulted in 137 arrests and far fewer indictments[15]. Its 2012 investigation led to far less: 25 criminal complaints -- nine of which are still only identified as ″Doe.″ Permalink[16] | Comments[17] | Email This Story[18] [1]: *https://www.techdirt.com/articles/20150722/22575031731/deas-confidential-informant-program-basically-being-run-with-no-oversight-whatsoever.shtml* [2]: *https://www.techdirt.com/articles/20140318/17221226618/government-g-men-bust-another-handcrafted-terrorist-crime-thinking-about-supporting-terrorist-organization.shtml* [3]: *https://www.techdirt.com/articles/20140319/07345226624/judge-otis-wright-slams-made-up-government-plot-designed-to-ensnare-gullible-non-criminals.shtml* [4]: *http://www.theregister.co.uk/2014/*

08/27/former_cybersecurity_czar_convicted_of_involvement_in_online_child_abuse_ring/ [5]: *http://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers* [6]: *https://www.techdirt.com/articles/20160107/06414333264/fbi-deploying-large-scale-hacking-with-little-to-no-judicial-oversight.shtml* [7]: *https://assets.documentcloud.org/documents/2698486/Us-v-Michaud.pdf* [8]: *http://media.ca8.uscourts.gov/opndir/16/01/151993P.pdf* [9]: *https://twitter.com/bradheath/status/690267758467137536* [10]: *https://t.co/0MbaBJu3xn* [11]: *https://twitter.com/bradheath/status/690269074610372608* [12]: *https://twitter.com/hashtag/DOJ?src=hash* [13]: *https://t.co/pZ8WiNtqJm* [14]: *https://twitter.com/bradheath/status/690267758467137536* [15]: *http://www.usatoday.com/story/news/2016/01/21/fbi-ran-website-sharing-thousands-child-porn-images/79108346/* [16]: *https://www.techdirt.com/articles/20160126/14535433436/courts-pretty-much-ok-with-fbis-occasional-stints-as-child-porn-distributors.shtml* [17]: *https://www.techdirt.com/articles/20160126/14535433436/courts-pretty-much-ok-with-fbis-occasional-stints-as-child-porn-distributors.shtml#comments* [18]: *https://www.techdirt.com/articles/20160126/14535433436/courts-pretty-much-ok-with-fbis-occasional-stints-as-ch*

Classification

Language: English

Publication-Type: Web Blog

Journal Code: DIRT-0001

Subject: CRIMINAL INVESTIGATIONS (90%); LAW ENFORCEMENT (90%); PORNOGRAPHY (90%); INVESTIGATIONS (90%); CHILD PORNOGRAPHY (89%); INTERNET CRIME (78%); CONSPIRACY (78%); SEARCH WARRANTS (77%); LAWYERS (75%); TERRORIST ATTACKS (57%); TERRORISM (57%)

Organization: FEDERAL BUREAU OF INVESTIGATION (94%)

Industry: INTERNET CRIME (78%); HIDDEN WEB (77%); LAWYERS (75%)

Geographic: NEBRASKA, USA (79%); WASHINGTON, USA (79%); UNITED STATES (79%)

Load-Date: January 27, 2016