

## *FBI Hacked a Tor-Hidden Site, Court Upholds 2013 Child Porn Conviction*

Legal Monitor Worldwide

January 28, 2016 Thursday

Copyright 2016 Legal Monitor Worldwide Provided by Syndigate Media Inc. All Rights Reserved



**Length:** 632 words

### **Body**

---

Earlier this month, the FBI hacked a child pornography site on the dark web, and ran it for over a week, collecting IP addresses from users, in the largest law enforcement hacking campaign to date. One defense team in that case has now argued that the FBI itself had peddled child porn. On January 21st, the 8th Circuit Court of Appeals upheld a conviction in a very similar case from 2013.

In *US v. Welch*, the FBI used a hacking tool on the site Pedobook, and captured the IP address of Brian Welch. Welch was later convicted of receiving, attempting to receive, and accessing with intent to view child pornography.

Although the conviction was upheld, the court did decide that the FBI had violated Federal Rule of Criminal Procedure 41(f). Rule 41 requires that a copy of the search warrant must be provided to the owner of the property seized. It's a rule that most people can't name, but are generally familiar with from movies and television frequently depict the police knocking on the door and brandishing pieces of paper.

Of course, the rules turn out a little differently when the police are, say, tapping phones or hacking Tor-hidden services. A statute can allow delaying showing the warrant for thirty days, or even longer if law enforcement seeks an extension.

In this case like in the law enforcement takedown of child pornography site Playpen last year the FBI left the site running and installed a hacking tool, which is known as a NIT, or Network Investigative Technique. The NIT provided agents with information about any user who accessed certain content on PedoBook.

The FBI used the NIT in November 2012, and arrested Brian Welch in April 2013 far more than thirty days after the execution of the warrant. The FBI believed that the thirty days began to count down the day that the agency identified Brian Welch as a suspect which it said was a few days prior to arrest. (On the other hand, the FBI had received the subscriber information for Welch's IP address from his internet service provider in December 122 days before they arrested him and showed him the warrant).

This is an extremely technical violation of the law, and one that didn't even rebound on investigators in this case, since their error was in good faith if it wasn't a reckless mistake, it can't be used to exclude evidence.

Amy Strickling

No one wants to side with child pornographers, but both the Playpen investigation and US v. Welch bring up troubling questions. These investigative techniques involve a government-sponsored hack, and have the potential to sweep up huge numbers of people. Yet whatever limits there are on these searches, they are meager.

The reason why can be illustrated in Rule 41, which is clearly designed around a basic case scenario where an officer knocks on a real-life door and searches a real-life location. And its not just Rule 41. This is an archetypal scene that much of the constitutional law around search and seizure is based on.

Yet the use of NITs is so different from a physical search that it might as well come from another universe. I mean, this is a story about hacking tools, the dark web, and a hidden child pornography distributor. Its even very different from wiretapping in general. In order to execute this search and the search in the Playpen case, the FBI not only hacked, but then arguably went on to run a child pornography site.

The limits there are to these searches are apparently just procedural issues like Rule 41. The law doesnt anticipate this kind of search, and apparently, cannot express whatever uneasiness the ordinary person might have about it. If the dark web spawns unprecedented kinds of crimes, it also spawns unprecedented kinds of police searches. It will be a while before constitutional limitations catch up if they ever catch up at all. 2016 Legal Monitor Worldwide.

## Classification

---

**Language:** ENGLISH

**Publication-Type:** Newspaper

**Journal Code:** 1258

**Subject:** LAW ENFORCEMENT (92%); CHILD PORNOGRAPHY (90%); CRIMINAL CONVICTIONS (90%); PORNOGRAPHY (90%); SPECIAL INVESTIGATIVE FORCES (90%); ARRESTS (89%); INVESTIGATIONS (89%); ARREST WARRANTS (88%); CRIMINAL INVESTIGATIONS (88%); SEARCH WARRANTS (78%); WIRETAPPING (78%); CRIMINAL LAW (77%); DECISIONS & RULINGS (77%); LAW COURTS & TRIBUNALS (71%); TRIAL & PROCEDURE (71%)

**Industry:** COMPUTER NETWORK SECURITY (90%); HIDDEN WEB (78%); COMPUTER NETWORKS (77%); INTERNET SERVICE PROVIDERS (61%)

**Load-Date:** January 28, 2016