# *How the FBI became the world's largest distributor of child sex abuse imagery*

TheNextWeb.com

January 28, 2016 Thursday 11:13 PM EST



**Length:** 1758 words

**Byline:** Bryan Clark

## Body

Jan 28, 2016( TheNextWeb.com: *http://thenextweb.com* Delivered by Newstex) For 12 days between February and March, 2014, the FBI was the world's largest peddler of images and video depicting child sexual abuse on the internet. In an attempt to catch criminals uploading, viewing, sharing and downloading these files, the US government authorized members of the FBI to run an operation — 'Operation Pacifier' — of dubious legality to catch pedophiles visiting Playpen, the world's largest child sexual abuse site. 'There is something tawdry and sick about FBI agents peddling porn,' says famed civil rights trial attorney Norm Pattis. In speaking with attorneys about Operation Pacifier, I heard words like: 'shocking,' 'disgusting,' and 'vile'; they weren't talking about the pedophiles. PlaypenPlaypen launched in August of 2014 as a dark web site only accessible by 'The Onion Router', commonly known as TOR.

Through use of TOR[1], users are able to access the Deep Web while routing web traffic around the world in an attempt to anonymize their browsing. It's not foolproof, but it's the best weapon a Web user has to remain anonymous online. And anonymity, when peeking into the darkest corners of the web, is paramount. Due to the nature of the site in question, I didn't want to dig too far, but from FBI testimony on the topic, it contained files — mainly images and video — of some of the most extreme child abuse imagery one could imagine as well as advice on how sexual abusers could perpetrate their crimes without being caught. For all intents and purposes, Playpen was amongst the darkest of the dark corners of the web.Operation PacifierFebruary 20, 2015 was an unremarkable day for Playpen's users. At the surface, the site was operating as usual, but behind the scenes its server had been seized by FBI agents at a web host in North Carolina and moved to a secure government-controlled facility in Virgina. No one noticed. And really, how could they? For fear of raising suspicions amongst Playpen's users, the FBI left the site fully operational while they sought a warrant to track users through what it refers to as 'network investigative techniques' or NIT. NIT, is a vague term for an exploit the FBI uses to gain access to a network or device. In this case, malware. To be clear, 'fully operational' means just that. For two weeks, users had the ability to upload new files, view existing images or video and communicate with other pedophiles. Basically, it was business as usual, only the FBI was piloting the ship. From February 20 until March 4, 2015, the FBI continued to operate Playpen[2] while infecting users computers with malware in hopes that it would lead to identifying information, such as an internet protocol (IP) address. During its 12 day reign as the king of all child sexual abuse sites, the FBI garnered some 1,300 of these IP addresses. Sting operations featuring Deep Web honeypots aren't new to the FBI. In 2011, the bureau used NIT — albeit a different type of exploit — on three hidden services (Deep Web websites) hosting lewd images and of minors. Users of these services were targeted through a Flash application that would ping a users real IP address back to an FBI-controlled server rather than routing the traffic through TOR, as intended. But this operation, in comparison, was

small potatoes in comparison to Pacifier. The FBI was only able to collect 25 IP addresses. With Pacifier, the FBI went bigger. To catch a criminal, it seems, you have to become one. And that's exactly what the FBI did, at least according to the legal professionals involved in the case.Was the operation legal?First, it's important to understand that what the FBI did resides very much in the grey area of our legal system. As much as I tried, securing a conclusive and concrete answer to the legality of the FBI running this type of site proved elusive. New York attorney Joseph Potashnik[3] informed me that in federal cases this kind of conduct by law enforcment is legal. He wasn't alone. An attorney who preferred not to be named remarked that it was not only legal, but it was 'abused by the government on a regular basis' in other cases he's tried, citing an officer that committed a sex act with a prostitute and then charged her with prostitution. Oddly enough, he wasn't the only attorney to use that reference. Others, like attorneys Mark McBride[4] and Norm Pattis[5] disagreed. According to McBride, who has defended these types of cases before, 'It's definitely not legal.' Attorney Christopher Eskew[6] noted that it wasn't legal, but it wouldn't be a case the US government would prosecute. In short, there isn't a clear answer as to the legality of what the FBI did. The agency did secure a warrant, but the warrant was strictly for the usage of the NIT, not running a lewd site disseminating explicit images and video of children. It's not even clear if the federal judge that signed the warrant understood the scope of what he was authorizing. A Motherboard piece[7] detailed this exchange between Judge Robert J. Bryan and defense attorney Colin Fieman, who is representing one of the accused, Jay Michaud:'Do the FBI experts have any way to look at the NIT information other than going to the server?' Judge Bryan asked. 'Your Honor, they don't go to the server,' Colin Fieman, replied. 'Where do they go? How do they get the information?' 'They get it from Mr. Michaud's computer.' 'They don't have his computer.' 'That's what the NIT is for,' Fieman explained.While Judge Bryan didn't sign the warrant used to charge Michaud, it speaks to the complicated nature of understanding the scope of the malware under broad and vauge guidelines within its request. There are several additional pages of transcripts that show Judge Bryan attempting to figure out just what this NIT is, and how it was going to be used. All told, the court spent more than two hours on definitions and descriptions of NIT. Lack of understanding aside, there are also issues with the warrant itself, most notably, jurisdiction. Fieman, and Michaud's other attorney, Linda Sullivan, argue that the warrant 'is limited to persons and property in the Eastern District of Virginia.' Keith Becker, an attorney for the Department of Justice (DOJ) said in a hearing, that the warrant, 'clearly requested the authorities to deploy to computers wherever located.' Michaud's attorneys then proceeded to call into question the legality of the sting operation itself, stating: There is no law enforcement exemption, or statutory exemption for the distribution of child pornography. In this case, it's easy to see that the need to catch a criminal overshadowed the FBI's desire to stop the flow of information, which arguably, is more important. Sullivan and Fieman argued that the harm caused by the dissemination of child sexual abuse images is summed up on the DOJs own website: Once an image is on the Internet, it is irretrievable and can continue to circulate forever At this point, the only thing we can be clear about in terms of legality was that we're really not sure, but it doesn't seem as if it matters whether the FBI broke any laws. As Eskew put it, it's highly unlikely the government would prosecute FBI agents.Do the ends justify the means?Leaving the attorneys and judges to decide legality, it's much easier to debate whether the methods the FBI used to catch pedophiles justified the means. No one would argue the benefit of apprehending those that are creating and distributing child sexual abuse images and video, but is it ever appropriate to display these images to pedophiles in an attempt to catch them? Pattis eloquently states: They claim they do so to draw out defendants, and defeat the market for prohibited images, yet the demand for the images remains the same. Lawmen can't stamp out desire; they can only join the fray, becoming as twisted as

the folks they prosecute. I spoke with both the FBI and DOJ regarding this matter. According to DOJ spokesperson, Peter Carr: While [shutting Playpen down] would end the trafficking of child pornography taking place on that one website, it would do nothing to prevent those same users from disseminating child pornography through other means … At no time in an operation like this does the FBI post any images, videos, or links to images of child pornography. Any posting of child pornography images and links are done by users of the website, not by the FBI. While it wasn't actively contributing to the cache of images, videos or links, the FBI was facilitating the practice for others who were doing just that. No matter where you stand on legality, this has to bring questions of morality to the table. Is 'not actively contributing' enough to negate government responsibility in Operation Pacifier? McBride doesn't think so, 'taking down 10 perverts does not outweigh the damages of even one image being disseminated.' It's hard to argue his logic. If capturing and releasing a sexually explicit image of a child is a crime against the victim, every time it's viewed and passed on is akin to recommitting the crime, only this time with a new offender. McBride was unwavering in this belief. In other sting operations, investigations have revolved around enticing users into registration through use of suggestive, but not explicit, images of minors. Let's attempt to quanitfy the success of this operation. Playpen had a total of 215,000 members. Operation Pacifier collected 1,300 unique IP addresses and led to 137 users charged, meaning, nearly 90 percent of those tracked were never charged with a crime nearly a year after the investigation concluded. What's not quantifiable is the reach of these images and just how much the government's operation, or the facilitation of pedophilia, did to benefit — or damage — child sexual abuse rings. At the end of the day, you have to weigh the ends, 137 men charged, against the means, being complicit in the dissemination of sexually explicit imagery, and attempt to make a judgement call as to whether becoming a criminal is worth catching one. [ 1]: *http://thenextweb.com/insider/2013/10/08/what-is-tor-and-why-does-it-matter/#gref* [ 2]: *http://thenextweb.com/insider/2016/01/24/fbi-hosted-images-of-child-sexual-abuse-on-dark-web-to-hack-pedophiles-around-the-world/#gref* [ 3]: *http://www.jpolawfirm.com* [ 4]: *http://www.gototrial-now.com* [ 5]: *http://www.normpattis.com* [ 6]: *http://www.eskewlaw.com* [ 7]: *http://motherboard-.vice.com/read/judge-in-fbi-hacking-case-is-unclear-on-how-fbi-hacking-works*

## Classification

**Language:** English

**Publication-Type:** Web Blog

**Journal Code:** TNXW-125814

**Subject:** LAW ENFORCEMENT (90%); SEXUAL ASSAULT (90%); CHILD SEXUAL ABUSE (90%); CHILD ABUSE (89%); INVESTIGATIONS (89%); SPECIAL INVESTIGATIVE FORCES (89%); PORNOGRAPHY (77%); CRIMINAL OFFENSES (77%); LAWYERS (73%); CIVIL RIGHTS (72%); Insider

**Organization:** FEDERAL BUREAU OF INVESTIGATION (94%)

**Industry:** INTERNET & WWW (90%); HIDDEN WEB (90%); MALICIOUS SOFTWARE (77%); COMPUTER VIRUSES (77%); WEBSITES (75%); LAWYERS (73%); NETWORK PROTOCOLS (68%); NETWORK SERVERS (66%)

**Geographic:** NORTH CAROLINA, USA (79%); UNITED STATES (73%)

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