

## *FBI's porn sting puts privacy in crossfire*

The Seattle Times

August 28, 2016 Sunday

Copyright 2016 The Seattle Times Company All Rights Reserved

**Section:** ROP ZONE; Pg. A1

**Length:** 1357 words

**Byline:** Mike Carter, Seattle Times staff reporter

### **Body**

---

For two weeks in the spring of 2015, the FBI was one of the largest purveyors of child pornography on the internet.

After arresting the North Carolina administrator of The Playpen, a "dark web" child-pornography internet bulletin board, agents seized the site's server and moved it to an FBI warehouse in Virginia.

They then initiated "Operation Pacifier," a sting and computer-hacking operation of unparalleled scope that has thus far led to criminal charges against 186 people, including at least five in Washington state.

The investigation has sparked a growing social and legal controversy over the FBI's tactics and the impact on internet privacy. Some critics have compared the sting to the notorious Operation Fast and Furious, in which the Bureau of Alcohol, Tobacco, Firearms and Explosives allowed the illegal sales of thousands of guns to drug smugglers, who later used them in crimes.

Defense attorneys and some legal scholars suggest the FBI committed more serious crimes than those they've arrested - distributing pornography, compared with viewing or receiving it.

Moreover, the FBI's refusal to discuss Operation Pacifier and reveal exactly how it was conducted - even in court - has threatened some of the resulting criminal prosecutions. Last month, a federal judge in Tacoma suppressed the evidence obtained against a Vancouver, Wash., school district employee indicted in July 2015 on a charge of receiving child pornography because the FBI refused to reveal how it was gathered.

Similar motions are pending in other prosecutions in Washington and elsewhere around the country.

During the two weeks the FBI operated The Playpen, the bureau says visitors to the site accessed, posted or traded at least 48,000 images, 200 videos and 13,000 links to child pornography. At the same time, agents deployed a secret "Network Investigative Technique," or NIT, to invade their computers, gather their personal information and send it back to the FBI.

According to court documents, between Feb. 20 and March 4, 2015, as many as 100,000 people logged onto the site, which was accessible only by using the anonymous "Tor" browser, which encrypts and routes internet traffic through thousands of other computers to hide the identity of a user.

Tor, which is used for private communications by government officials, lawyers, journalists, judges and others, was thought to be virtually uncrackable until news of the FBI's operation became public.

Amy Strickling

## FBI's porn sting puts privacy in crossfire

Mozilla, the company that offers the Tor browser, asked the FBI to reveal its methods so it can be patched, warning in a court motion that, "absent great care, the security of millions of individuals using Mozilla's Firefox internet browser could be put at risk" by its disclosure. The Tacoma judge denied the request.

The FBI declined to be interviewed for this story. The Department of Justice (DOJ) referred The Seattle Times to court filings by prosecutors in the case.

In those pleadings, the government has defended the operation as the only way to pierce the anonymity of the so-called "dark web" and get at the criminals who dwell there. Such websites cannot be found by Google or by typing in a web address and are typically operated on the Tor network.

"The United States, the FBI, did not create this website," said Assistant U.S. Attorney Keith Becker, a trial attorney with the DOJ's Child Exploitation and Obscenity Section, at a Tacoma court hearing in January.

"It was created by its users, and administrators, and existed and substantially distributed child pornography long before the government took it over in an effort to actually identify its criminal users."

Defense attorneys, however, alleged in filings last week that FBI agents actually improved The Playpen site during the two weeks they had control, making it faster and more accessible. Visitation of The Playpen while under FBI control jumped from 11,000 to 50,000 people a week.

"This is easily the largest domestic use of hacking by law enforcement in U.S. history," said Mark Rumold, a senior staff attorney at the Electronic Frontier Foundation, a digital freedom and legal services nonprofit in San Francisco. "The problem is that there just aren't a lot of rules on how they go about it."

"I will not be surprised at all if we wind up before the U.S. Supreme Court," he said. Critics also accuse the FBI of committing crimes more serious than it was investigating - distribution of pornography versus receiving it - and say the operation flies in the face of the Justice Department's pronouncement that a child is re-victimized every time a pornographic photo is viewed or distributed.

Chris Soghoian, the principal technologist and a senior policy analyst with the American Civil Liberty Union's Speech, Privacy, and Technology Project, said The Playpen investigation bears striking similarities to Operation Fast and Furious.

"Except here, it's child porn," Soghoian said.

Soghoian said the bureau's refusal to turn over the NIT to allow the Tor vulnerability to be patched is inviting criminals to figure it out and use it themselves.

Last month, U.S. District Judge Robert Bryan in Tacoma threw out the evidence in one of the first "Operation Pacifier" prosecutions, involving a Vancouver school employee named Jay Michaud. The reason: The FBI has refused a court order to reveal to Michaud's defense attorneys the nature of the Tor vulnerability or how the NIT works.

Michaud is accused of visiting the Playpen site multiple times during the two weeks it was under FBI control and viewing explicit photos of children being sexually abused. He faced up to 20 years in prison.

With the evidence tossed out, Michaud's case likely will be dismissed. The government has appealed the judge's decision.

A federal judge in Oklahoma reached the same conclusion in an Operation Pacifier case there, and similar motions are pending in dozens of other cases.

Bryan has also allowed two other Operation Pacifier defendants in Washington state to withdraw guilty pleas so they can challenge the government over the issue.

Michaud's attorney, Colin Fieman, a Tacoma-based federal public defender, is leading a "national defense working group" that is tracking and coordinating challenges to Operation Pacifier cases.

He says the overarching legal issue in all of the cases is the FBI's decision to search and hack thousands - maybe tens of thousands - of computers around the world based on a single warrant obtained by agents in Virginia.

With few exceptions, Fieman says, the federal rules of criminal procedure require a warrant to be issued in the same district as the search to prevent unconstitutional government fishing expeditions. That, contends Fieman and others, is what has happened with Operation Pacifier.

The case has shown that the "FBI cannot be trusted with broad hacking powers," Fieman said.

"There is no question that the internet poses serious challenges to law enforcement," Fieman said.

But he believes that in its desire to overcome those challenges - and fight the scourge of child pornography - the agency "has lost its moral compass and is willing to ignore the rules and even break the law to extend its reach."

Michaud and other defendants have also sought to have their charges dismissed due to "outrageous government conduct" over the FBI decision to take it over and leave the site running.

"It is impossible to reconcile the Playpen operation with the government's own view of the harm caused by the distribution of child pornography," Fieman wrote in motion to dismiss another Washington case filed last week. "The DOJ routinely emphasizes ... that possessing and circulating pornographic images re-victimizes the children depicted in them."

Federal prosecutors routinely seek more stringent sentences for the operators of child-porn websites, Fieman wrote.

Judge Bryan rejected that argument in the Michaud case, stating during a January hearing that agents were "trying to catch the bad guys, so to speak."

"Whether they did it right is a different thing," he said. "But they didn't do it wrong as to be grossly shocking or outrageous to violate the universal sense of justice" and warrant dismissing the charges.

## **Classification**

---

**Language:** ENGLISH

**Publication-Type:** Newspaper

## FBI's porn sting puts privacy in crossfire

**Subject:** CRIMINAL OFFENSES (94%); CHILD PORNOGRAPHY (90%); LAW ENFORCEMENT (90%); SMUGGLING (90%); ARRESTS (90%); PORNOGRAPHY (90%); FIREARMS (90%); INVESTIGATIONS (90%); SPECIAL INVESTIGATIVE FORCES (90%); SEX OFFENSES (90%); JUDGES (89%); JUSTICE DEPARTMENTS (89%); CRIMINAL INVESTIGATIONS (78%); INTERNET CRIME (78%); INDICTMENTS (78%); BLOGS & MESSAGE BOARDS (78%); COMPUTER CRIME (76%); LAWYERS (75%); EVIDENCE (73%); CONTROLLED SUBSTANCES CRIME (73%); SCHOOL DISTRICTS (72%); EDUCATIONAL INSTITUTION EMPLOYEES (72%); LAW COURTS & TRIBUNALS (71%); PRIVACY RIGHTS (69%); WRITERS (60%); DRUG TRAFFICKING (53%)

**Organization:** FEDERAL BUREAU OF INVESTIGATION (95%)

**Industry:** COMPUTER EQUIPMENT (89%); INTERNET & WWW (89%); HIDDEN WEB (89%); INTERNET BROWSERS (84%); COMPUTER NETWORKS (78%); INTERNET CRIME (78%); INTERNET PRIVACY (78%); BLOGS & MESSAGE BOARDS (78%); COMPUTER CRIME (76%); COMPUTER NETWORK SECURITY (76%); LAWYERS (75%); WRITERS (60%)

**Geographic:** TACOMA, WA, USA (92%); SEATTLE, WA, USA (79%); WASHINGTON, USA (90%); NORTH CAROLINA, USA (79%); UNITED STATES (92%)

**Load-Date:** August 30, 2016

---

End of Document