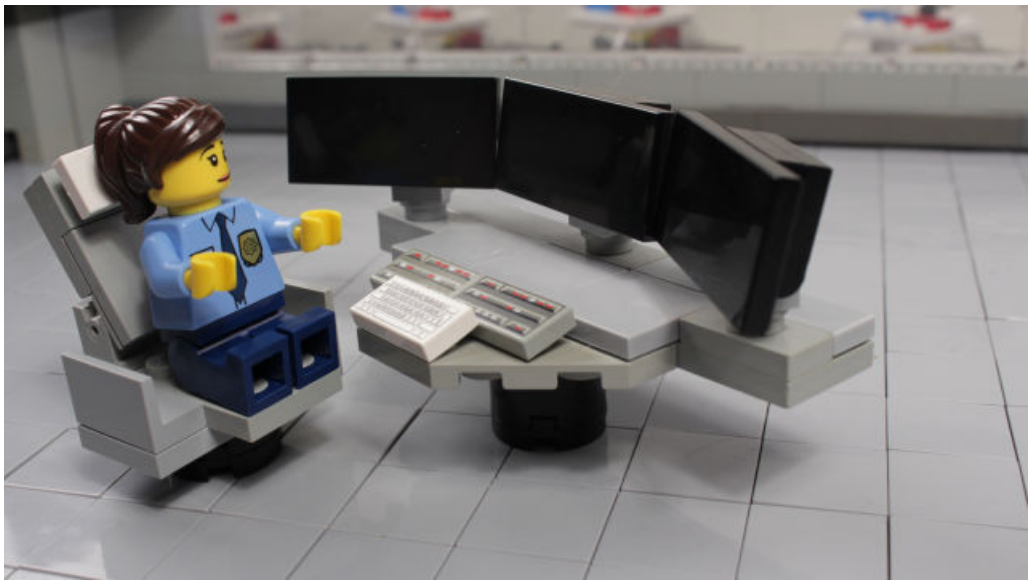
LAW & DISORDER / CIVILIZATION & DISCONTENTS

Judge rules in favor of child porn suspect: Search warrant was improper

FBI used a Tor vulnerability to find child porn on suspect's computer.

by **Cyrus Farivar** - Apr 27, 2016 6:05am PDT



Brick Police

A second federal judge has now invalidated a search warrant that authorized a search of a suspect's computer via a Tor exploit, meaning the child pornography authorities say they found on that man's computer cannot be used as evidence. For now, the case remains live, but absent a successful government appeal, it will be quite difficult for the case against Scott Frederick Arterbury to go forward.

FURTHER READING

JUDGE INVALIDATES WARRANT THAT LET FEDS HACK TOR-USING CHILD PORN SUSPECT

Massachusetts judge finds warrant issued by magistrate in Virginia was improper.

A week ago, a federal judge in Massachusetts made a similar ruling and similarly tossed the relevant evidence. The Massachusetts magistrate judge and now the Oklahoma magistrate judge came largely to the same conclusion: that only more senior judges, known as district judges, have the authority to issue out-of-district warrants. Because the warrant was invalid *ab initio*, or from the beginning, any evidence that resulted from that search must be suppressed.

Experts say that with two similar results by two different judges across judicial districts, some if not most of the other 135 "Operation Pacifier" child pornography cases that are being prosecuted may be in jeopardy. (Here, in *United States v. Arterbury,* an Oklahoma district judge could overrule the magistrate's ruling, and even that ruling could be appealed further.)

"The FBI conducted a global sting operation by serving malware to thousands of computers without first obtaining proper judicial authority," Ahmed Ghappour, a law professor at the University of California, Hastings, told Ars by text message. "Whether this was due to gross incompetence, or an

LATEST FEATURE STORY

FEATURE STORY (2 PAGES)

Power tools: S through the c specialized da toolbox

With so many choices database to need isn't

WATCH ARS VIDEO

expectation that the courts would grant a free pass, the FBI played fast and loose with this one, and we may see more cases getting thrown out as a result."

That initial warrant, which was issued in early 2015 by a federal magistrate in Virginia, allowed investigators to use a "network investigative technique" (NIT). That's fed-speak for the deployment of malware used to penetrate the digital security of Tor users accused of accessing this Tor-hidden child pornography site, "Playpen." In yet another related case prosecuted out of New York, an FBI search warrant affidavit described both the types of child pornography available to Playpen's 150,000 members and the malware's capabilities.

As a way to ensnare users of this website, the FBI took control of Playpen and ran it for 13 days before shutting it down. During that period, with many users' Tor-enabled digital shields down, the government was able to identify, arrest, and prosecute 135 other individuals besides the two men in Oklahoma and Massachusetts. (However, nearly 10 times that number of IP addresses were revealed as a result of the NIT's deployment, which could suggest that still more charges could be filed.)

"We're happy to see when courts are looking at these issues seriously and even more happy when they rule in the defense's favor," Colin Fieman, a federal public defender who represents a client in a related case in Tacoma, Washington, told Ars on Tuesday.

Follow the rules

In Oklahoma, US Magistrate Judge Paul Cleary excoriated the government's reasoning in his 29-page filing. As the judge articulated, prosecutors argued that they indeed followed the relevant law, known as Federal Rule of Criminal Procedure 41 (b)(2) and (b)(4). Those rules essentially provide conditions under which a magistrate judge is allowed to issue a search warrant for a person or property within his or her district, even if that target moves elsewhere.

As prosecutors in *US v. Arterbury* argued in court papers, because the defendant accessed the government-controlled Playpen, which was being operated temporarily out of Virginia, and then his computer transmitted data back to Oklahoma, the Virginia warrant was valid.

FURTHER READING

AFTER FBI BRIEFLY RAN TOR-HIDDEN CHILD-PORN SITE, INVESTIGATIONS WENT GLOBAL

"It's amazing the shit law enforcement leave online, accessible by some Google-fu."

Judge Cleary wrote:

> The Court is not persuaded by this argument. The property seized in this instance was Arterbury's computer, which at all relevant times remained in Oklahoma. The NIT warrant allowed the Government to send computer code or data extraction instructions to Arterbury's computer, wherever it was located. The Government "seized" that computer and directed it to send certain information to the Government—all without Arterbury's knowledge or permission. Arterbury's computer was never in the Eastern District of Virginia and subsection (b)(2), therefore, does not apply. Furthermore, even if the property seized was electronic information, that property was not located in the Eastern District of Virginia at the time the warrant was signed. This information only appeared in Virginia after the Warrant was signed and executed and the Government seized control of Defendant's computer in Oklahoma.

Judge Cleary also slammed the government's secondary arguments that even if the Virginia magistrate judge had not signed off on the warrant, the search was allowed under the exigent circumstances exception.

As he continued:

The Court is not persuaded by this argument either. Exigent circumstances were the on-going downloading and distribution of child pornography. In this instance, the specific activity at issue was on-going only because the Government opted to keep the Playpen site operating while it employed the NIT. The Government cannot assert exigent circumstances when it had a hand in creating the emergency.

Don't hate the player...

Fieman also told Ars that when the FBI uses a vulnerability, a zero-day, or some other technique to gain unauthorized access someone's computer, then it "affects all of us."

"That's what the Fourth Amendment is all about it—it's not there to protect criminals, it's to protect against the government," he added. "That's the ultimate bulwark for our privacy and restraint on law enforcement powers."

In fact, the government wants an expansion of its ability to use this technique in future cases. For over two years now, the Department of Justice has lobbied to change Rule 41, which would allow magistrates in one district to authorize searches across multiple districts. The change is now pending before the Supreme Court, and presuming it approves by May 1, the revised Rule 41 would move to Congress. The legislative branch then has until December 1 to "enact legislation to reject, modify, or defer the amendment." (Google has even publicly lobbied against this proposed change.)

In the Oklahoma case, DOJ spokesman Pete Carr e-mailed Ars to say that the agency was "disappointed with the court's decision," adding that it is reviewing it options. But, he added that this case underscored why Rule 41 revisions are sorely needed.

"The decision highlights why the government supports the clarification of the rules of procedure currently pending before the Supreme Court to ensure that criminals using sophisticated anonymizing technologies to conceal their identities while they engage in crime over the Internet are able to be identified and apprehended."

FURTHER READING

FEDS BUST THROUGH HUGE TOR-HIDDEN CHILD PORN SITE USING QUESTIONABLE MALWARE

FBI seized server, let site run for two weeks before shutting it down.

READER COMMENTS 99

Cyrus Farivar / Cyrus is the Senior Business Editor at Ars Technica, and is also a radio producer and author. His first book, *The Internet of Elsewhere*, was published in April 2011.
@cfarivar on Twitter

← OLDER STORY NEWER STORY →