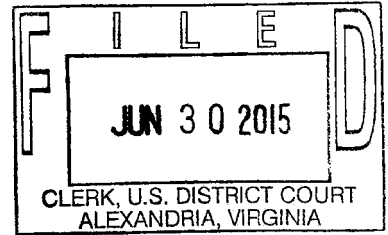


IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN THE MATTER OF THE SEARCH)
OF COMPUTERS THAT ACCESS) **Case No. 1:15-SW-89**
upf45jv3bziuctml.onion) **UNDER SEAL**

SECOND REQUEST FOR EXTENSION OF DELAYED NOTICE

The United States of America, by and through its attorneys Dana J. Boente, United States Attorney for the Eastern District of Virginia, and Whitney Dougherty Russell, Assistant United States Attorney, herein requests a 90-day extension of delayed notice to users of computers that accessed the child pornography website identified as upf45jv3bziuctml.onion (the "TARGET WEBSITE"). In support thereof, the United States represents as follows:

On February 20, 2015, this Court authorized a search warrant to allow the Federal Bureau of Investigation to deploy a Network Investigative Technique ("NIT") on the computer server operating the child pornography website upf45jv3bziuctml.onion in an attempt to identify the actual IP addresses and other information of computers used to access that website. The warrant, application and affidavit are attached hereto. The warrant authorized delayed notice of the search, pursuant to 18 U.S.C. § 3103a, for 30 days after the user of a computer that accessed the website was identified to a sufficient degree as to provide notice. On April 3, 2015, the court granted the government's requested 90-day extension of that delayed notice pursuant to 18 U.S.C. § 3103a(c). The government hereby requests an additional 90-day extension of delayed notice.

Delayed Notice Provisions

Federal Rule of Criminal Procedure 41 allows for the delay of any notice required by Rule 41 “if the delay is authorized by statute.” FED R. CRIM P. 41(f)(3). Title 18 Section 3103a allows for any such notice to be delayed if:

- (1) the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in section 2705, except if the adverse results consist only of unduly delaying a trial);¹
- (2) the warrant prohibits the seizure of any tangible property, any wire or electronic communication (as defined in section 2510), or, except as expressly provided in chapter 121, any stored wire or electronic information, except where the court finds reasonable necessity for the seizure; and
- (3) the warrant provides for the giving of such notice within a reasonable period not to exceed 30 days after the date of its execution, or on a later date certain if the facts of the case justify a longer period of delay

18 U.S.C. § 3103a(b). Title 18 Section 3013a also permits the court to extend delayed notice, as follows:

- (c) Extensions of delay. Any period of delay authorized by this section may be extended by the court for good cause shown, subject to the condition that extensions should only be granted upon an updated showing of the need for further delay and that each additional delay should be limited to periods of 90 days or less, unless the facts of the case justify a longer period of delay.

18 U.S.C. § 3103a(c).

¹ Under 18 U.S.C. § 2705(2), any of the following constitute an adverse result:

- (A) endangering the life or physical safety of an individual;
- (B) flight from prosecution;
- (C) destruction of or tampering with evidence;
- (D) intimidation of potential witnesses; or
- (E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

The Initial Delayed Notice Request

In a section of the warrant affidavit titled “REQUEST FOR DELAYED NOTICE,” the affidavit in support of the NIT search warrant application cited and described the delayed notice provisions of Rule 41 and 18 U.S.C. § 3013a, articulated in detail why delayed notice was necessary, and requested authorization to delay notice to the person whose computer the NIT was used upon. *See* ¶¶ 38-41. In particular, the affidavit requested that the Court “authorize the proposed use of the NIT without the prior announcement of its use” because “[a]nnouncing the use of the NIT could cause the users or administrators of the TARGET WEBSITE to undertake other measures to conceal their identity, or abandon the use of the TARGET WEBSITE completely, thereby defeating the purpose of the search.” *See* ¶ 38. The affidavit articulated that notice of the use of the NIT “would risk destruction of, or tampering with, evidence, such as files stored on the computers of individuals accessing the TARGET WEBSITE” and therefore would “seriously jeopardize the success of the investigation into this conspiracy and impede efforts to learn the identity of the individuals that participate in this conspiracy, and collect evidence of, and property used in committing, the crimes (an adverse result under 18 U.S.C. §3103a(b)(1) and 18 U.S.C. § 2705).” *See* ¶ 39. The affidavit further articulated that “the investigation has not yet identified an appropriate person to whom such notice can be given.” *See* ¶ 40. Accordingly, the affidavit requested “authorization, under 18 U.S.C. §3103a, to delay any notice otherwise required by Federal Rule of Criminal Procedure 41(f), until 30 days after any individual accessing the TARGET WEBSITE has been identified to a sufficient degree as to provide notice, unless the Court finds good cause for further delayed disclosure.” *Id.* Further, in a section of the affidavit titled “SEARCH AUTHORIZATION REQUESTS,” the affidavit reiterated its request that:

pursuant to 18 U.S.C. § 3103a(b)(3), to satisfy the notification requirement of Rule 41(f)(3) of the Federal Rules of Criminal Procedure, the government may delay providing a copy of the search warrant and the receipt for any property taken for thirty (30) days after a user of an “activating” computer that accessed the TARGET WEBSITE has been identified to a sufficient degree as to provide notice, unless notification is further delayed by court order.

See ¶ 46(d).

This Court granted the request for delayed notice, checking the box on the warrant itself to commemorate the finding that “immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial),” and authorizing “the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized for 30 days.”

The Deployment of the NIT and Subsequent Investigation

Between February 20, 2015 and March 4, 2015, a NIT was deployed pursuant to this Court’s authorization on the TARGET WEBSITE. The NIT collected information, including IP address information, for some, but not all, users of the TARGET WEBSITE. The FBI has subsequently issued subpoenas to Internet Service Providers seeking subscriber information for more than [REDACTED] IP addresses derived from the use of the NIT and is actively engaged in the process of conducting other investigation in an effort to determine the actual identity of the users of the website for whom the NIT provided IP address information.

Although the NIT identified IP addresses of computers that accessed the TARGET WEBSITE, at that point there was no person identified to whom notice could be given. The NIT did not identify a person or the user of a computer that was searched – it only identified the IP address and other information about a computer used to access the TARGET WEBSITE. That information is helpful, but not sufficient, to identify the actual user of the computer or the computer that was searched. Subscriber information from an Internet Service Provider is also helpful, but not sufficient, to identify the actual user of the computer or the computer that was

searched. Accordingly, further investigation, to include a search of a residence to which an IP address was assigned, review of computers seized from such a residence, and interviews of potential suspects, is necessary before a determination can be made as to the actual identity of the user behind the computer that accessed the TARGET WEBSITE while the NIT was deployed.²

Second Request for Extension of Delayed Notice

Since the first request for extension of delayed notice was granted on April 3, 2015, law enforcement agents have continued to be actively engaged in the process of conducting further investigation in an effort to determine the actual identity of the more than [REDACTED] users of the website for whom the NIT provided IP address information. For example, in some cases, law enforcement agents have amassed sufficient information to execute search warrants which were based in part upon IP address information derived from the use of the NIT. In some of the searches, sufficient information was obtained via the seizure of evidence, preliminary computer forensic examinations, interviews of suspects, or other information to identify the actual user of a computer that accessed the TARGET WEBSITE to a sufficient degree as to provide notice of the NIT warrant. Accordingly, in some of those cases, notice to identified users would be due within 30 days of the date of those respective searches under the terms of the initial warrant authorization. However, because the first request for extension of delayed notice was granted, identified users were not then provided notice of the execution of the NIT.

The investigation into the thousands of users and administrators of the TARGET WEBSITE, including but not limited to those more than [REDACTED] users for whom the NIT returned

² In the case of a residential search of a suspect address based on IP information, law enforcement must consider numerous contingencies in identifying the actual perpetrator of an offense under investigation, including but not limited to the possibility of multiple residents or computer users at the address or open/unsecured wireless connections which may allow an individual in the vicinity of an address to use an Internet connection assigned to that address.

IP address information, remains ongoing. The FBI has, to this point, disseminated suspect information to FBI field offices in many of the jurisdictions to which the IP addresses resolve. Because of the number of users involved, that is a time-consuming and labor-intensive process, which remains ongoing.

As search warrants continue to be executed, an individual whose residence is searched may become aware that his or her activity on the website is under investigation. However, such an individual would not necessarily know the full scope of the government's investigation merely because that individual's residence had been searched. Providing that individual with notice of the execution of the NIT, however, would alert such an individual to the scope of the investigation, because the full Uniform Resource Locator ("URL") for the TARGET WEBSITE is contained on the NIT warrant and associated attachments. Giving such an individual with notice of the execution of the NIT warrant could accordingly alert thousands of suspects under investigation to the ongoing investigation and the fact that law enforcement has interdicted the TARGET WEBSITE. For instance, one of the suspects to whom notice is due could publish the warrant on the Internet and, accordingly, notify individuals under investigation of the existence and scope of the current investigation.

Users of illegal child pornography websites on the Tor network are extremely sensitive to law enforcement infiltration. In a similar and ongoing investigation into Tor network child pornography websites, a search warrant affidavit describing (but not naming) a Tor network child pornography website under investigation was mistakenly left unsealed. Upon the publishing of a news story describing the website in that warrant, users immediately started discussion threads on two Tor-network child pornography websites which were then operating, in which users posted the news article and correctly identified the website under investigation,

even though that website's name was not published either in the search warrant or the news article. Some users posted comments to that thread disclosing that they had been a member of the website under investigation and seeking advice regarding whether they should destroy evidence of their activity.

More recently, users of a currently-operating Tor-network child pornography website posted detailed information about law enforcement's infiltration and interdiction of another Tor-network child pornography website, following the publication of a news article detailing the arrest of a member of that website, which article did not actually name the website. The discussion included a detailed analysis of a network investigative technique used by a law enforcement agency on the site in order to identify users, and a point-by-point analysis of tactics used by law enforcement agencies when Tor-network child pornography sites are interdicted.

Providing notice of the NIT warrant at this time is therefore likely to result in disclosure of the details of the investigation and alert other offenders under investigation. That may result in flight from prosecution, the destruction of or tampering with evidence and otherwise seriously jeopardize the investigation – all of which are “adverse results” under 18 U.S.C. § 2705(2). It is accordingly requested that this Court extend the notice required pursuant to Rule 41(f) and 18 U.S.C. § 3103a for an additional 90 days from the date of this order.

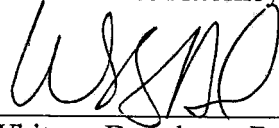
The foregoing is based on information provided to me in my official capacity by agents of the FBI.

WHEREFORE, it is respectfully requested that this Court grant the second requested 90-day extension of delayed notice pursuant to 18 U.S.C. § 3101a(c).

Respectfully submitted,

Dana J. Boente
United States Attorney

By:



Whitney Dougherty Russell
Assistant U.S. Attorney
United States Attorney's Office
2100 Jamieson Avenue
Alexandria, VA 22314
Tel: (703) 299-3700
Fax: (703) 299-3980
whitney.russell@usdoj.gov