Sealed Documents

3:15-cr-05351-RJB USA v. Michaud

BOND

U.S. District Court

United States District Court for the Western District of Washington

Notice of Electronic Filing

The following transaction was entered by Fieman, Colin on 12/2/2015 at 3:53 PM PST and filed on 12/2/2015

Case Name: USA v. Michaud
Case Number: 3:15-cr-05351-RJB
Filer: Dft No. 1 - Jay Michaud
Document Number: 69

Docket Text:
SEALED DOCUMENT ***Reply to Government Response to First Motion to Suppress Evidence*** **by Jay Michaud, re [68] MOTION to Seal Document *Reply to Government Response to First Motion to Suppress Evidence*. (Attachments: # (1) Exhibit A, # (2) Exhibit B, # (3) Exhibit C, # (4) Exhibit D)(Fieman, Colin)**

3:15-cr-05351-RJB-1 Notice has been electronically mailed to:

Colin Fieman colin_fieman@fd.org, Carolynn_Calder@fd.org, Christine_Bowie@fd.org, Jessica_Cvitanovic@fd.org, WAW_ECF_notifications@fd.org

Kate S Vaughan kate.vaughan@usdoj.gov, ecf-crm.usawaw@usdoj.gov, katelyn.mitchell@usdoj.gov, rebecca.eaton@usdoj.gov, Shontrice.Eaton@usdoj.gov

Keith Becker keith.becker@usdoj.gov

Linda R Sullivan linda_sullivan@fd.org, Carolynn_Cohn@fd.org, Christine_Bowie@fd.org, Jessica_Cvitanovic@fd.org, WAW_ECF_notifications@fd.org

Matthew H Thomas matthew.h.thomas@usdoj.gov, Chantelle.Smith2@usdoj.gov, ECF-CRM.USAWAW@usdoj.gov, Ellaine.Wi@usdoj.gov, jennifer.biretz@usdoj.gov, lisa.crabtree@usdoj.gov, Nichole.Barnes@usdoj.gov

Reginald E Jones reginald.jones4@usdoj.gov

3:15-cr-05351-RJB-1 Notice will not be electronically mailed to:

The following document(s) are associated with this transaction:

Document description: Main Document
Original filename:n/a
Electronic document Stamp:
[STAMP dcecfStamp_ID=1035929271 [Date=12/2/2015] [FileNumber=5922610-0] [ab4eb51d64f5bdd0480b1e3621e12d09b905edfab2c3449c636e834bfa4dc25bf45f9368d129c92568fc8d14cfc61ac638dd8018299a87c32320c9639cd1128b]]
Document description: Exhibit A
Original filename:n/a
Electronic document Stamp:
[STAMP dcecfStamp_ID=1035929271 [Date=12/2/2015] [FileNumber=5922610-1] [c455911dea8ec1631f2c279b3500092d02b5c9f126fcbe3e926724648487af08bea60ac72e883494b6ad81994e77a0b35a926fd1603994f84884141f07ac81f5]]
Document description: Exhibit B
Original filename:n/a
E lectronic document Stamp:
[STAMP dcecfStamp_ID=1035929271 [Date=12/2/2015] [FileNumber=5922610-2] [61221af70a98a8609c26290c747e7c040a34f99e29d1726ceec508c98d92c375b4b92b70a86f89cddea9851c4808fca3da7bbeade094b5c746447ac17870ec0e]]
Document description: Exhibit C
Original filename:n/a
Electronic document Stamp:
[STAMP dcecfStamp_ID=1035929271 [Date=12/2/2015] [FileNumber=5922610-3] [38e64503b75c59dee9e57485e4f14854a992a87cddc5875dd8a5a033263fd47c1c9353703239eb75bf19ad404d29447cfa2c1788ce0d743616ee1867be1d8001]]
Document description: Exhibit D
Original filename:n/a
Electronic document Stamp:
[STAMP dcecfStamp_ID=1035929271 [Date=12/2/2015] [FileNumber=5922610-4] [2e74cab28e2676f62c6b9349cb33c20f04f33bdf0e6633962a58b6f3a6a70b34ae4f15c11e3b6b6fe1a67792735f97a41d5b309c68f5a95136633f373aad698c]]

JUDGE ROBERT J. BRYAN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. JAY MICHAUD, Defendant.	No. CR15-5351RJB REPLY TO GOVERNMENT RESPONSE TO FIRST MOTION TO SUPPRESS EVIDENCE **FILED UNDER SEAL** ***[Evidentiary Hearing Requested]***

I. INTRODUCTION

In its Response to Defendant's Motion to Suppress Evidence, the Government offers six arguments to avoid suppression. All of the arguments are meritless, and a few are so unsupported by relevant facts and law that they are frivolous.

First, the Government maintains that "the NIT warrant was consistent with Rule 41." Govt. Response at 9. To the contrary, there is no way to reconcile the plain language of Rule 41 with the Government's claim that the warrant authorized it to search personal computers regardless of where they were located. If there were any doubt about this, a brief review of the Department of Justice's (DOJ's) internal analysis of Rule 41 shows that the Government's arguments here are inconsistent with its own conclusions elsewhere. *See* §§ II.A.1 – II.A.3 (pp. 3-12), *infra*.

Second, the Government claims that even if the NIT warrant was defective, the Tittle III warrant provided independent authority to search Mr. Michaud's computer.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Govt. Response at 9, 14-15; *see also* First Motion to Suppress, exh. B (Dkt. 26) (Title III warrant and application). In fact, apart from the inherent limitations of the Title III (wiretap) authorization, the Government's own representations in the Title III and NIT applications about the relationship between the two and the need for a separate NIT warrant directly undercuts its argument here. *See* § II.D (pp. 16-18), *infra*.

Third, the Government argues that "if neither the NIT warrant nor the Title III order provided authority" for the search of target computers, the NIT searches were nevertheless justified because of "exigent circumstances." Govt. Response at 9, 15-16. This argument ignores the fact that the narrow exigency exception to the Fourth Amendment's warrant requirement only applies when there is an actual emergency (which there wasn't) that makes it difficult or impossible for law enforcement officers to obtain a timely warrant (which the Government did, albeit a fatally flawed one). A brief review of the case law that defines and limits the exigency exception is sufficient to show that it is not relevant. *See* § II.B (pp. 12-14), *infra*.

Fourth, almost as an aside, the Government suggests that Mr. Michaud has no legitimate privacy interest in the data stored on his computer, if that data consists of an IP address or other identifying information. Govt. Response at 16, 21. This contention is also meritless because, in making it, the Government mistakenly relies on cases where the defendant not only had disclosed his or her information to a third party, but the Government obtained the information from the third party. In this case, Mr. Michaud's identifying information was not disclosed when he used the Tor network (that was the very reason for using an NIT to search his computer), and the data seized by the Government was taken from Mr. Michaud's personal computer, located inside his home. *See* § II.C (pp. 15-16), *infra*.[1]

[1] This is as good a place as any to correct a persistent misstatement by the Government about Mr. Michaud. *See, e.g.*, Govt. Response at 1. He is not a teacher. Instead, Mr. Michaud was, until his recent forced retirement, an administrator for the Vancouver School District. In that

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Fifth, the Government argues that even if the NIT warrant was invalid, "suppression is not an appropriate remedy." Govt. Response at 9, 17-21. This is really an argument better directed to the Ninth Circuit, since in making it the Government conspicuously fails to discuss, let alone distinguish, the controlling Court of Appeals authority. *See* § II.E (pp. 18-12), *infra*. That authority requires suppression when a violation of Rule 41 was deliberate or was of "constitutional magnitude," or when the search could not have been accomplished without the violation. Although the Court need only find one of these factors to order suppression, the facts in this case establish all three.

Sixth, and finally, the Government claims that even if the NIT warrant was invalid, the "good faith" exception should apply. Govt. Response at 22. Given the facts in this case and controlling case law, the Government's invocation of good faith is misplaced. As discussed more fully in section II.F (pp. 23-26), *infra*, the good faith exception does not apply to deliberate violations of Rule 41, nor does it apply when the Government has obtained a warrant with reckless or intentional disregard for the truth or relied on a facially overbroad warrant. Moreover, the Government's actions throughout the investigation and litigation of this case have been characterized by such deliberate disregard for the law, investigatory overreaching and lack of candor with the courts that suppression is not only appropriate but necessary to deter future violations of Rule 41 and the Fourth Amendment.[2]

II. ARGUMENT

A. The Government Deliberately Violated Rule 41.

---

capacity he had little or no direct contact with students, apart from various administrative meetings that were attended by other school district personnel.

[2] The Government's arguments related to probable cause (Govt. Response at 22-28) were addressed in Mr. Michaud's November 25, 2015, Second Motion to Suppress and Motion for *Franks* Hearing (Dkt. 65).

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

The Government's arguments about Rule 41 are hampered by a fundamental contradiction that it does not even attempt to resolve. On one hand, the Government maintains that the NIT warrant is "consistent" with Rule 41, and that the Rule allows a judge in one district to issue a search warrant for property in unknown locations around the world. At the same time, the warrant that the Government obtained is expressly limited to persons or property located in the Eastern District of Virginia. *See* First Motion to Suppress, exh. C. at C-002 (Bates 135); *see also* Defendant's Second Motion to Suppress (Dkt. 65) at 15-17. The obvious question is why the Government felt the need to present Magistrate Judge Buchanan with a warrant that, on its face, conformed to the plain language of Rule 41 and was limited to property located within her district, but at the same time ostensibly authorized searches anywhere. If the Government had been candid about its intentions when it applied for the warrant, and if Rule 41 did in fact allow for NIT searches regardless of the search location, the warrant itself would have expressly authorized searches of target computers regardless of their location.

In this regard, it is important to recognize that Rule 41 and its provisions have the force of law and are not, as the Government's response seems to suggest, merely advisory, procedural or susceptible to whatever interpretation suits its purposes. *See* 28 U.S.C. § 2072(b). Consistent with this understanding of the Rule's legal import, DOJ has sought amendments to the Rule that would allow courts to issue warrants for data searches outside an issuing court's district.[3] These proposed amendments have not been approved. Its proposal, as detailed in § II.E, *infra*, made clear the Government's view that the current version of the Rule contained "an unnecessary obstruction" to the kind of search that occurred here, one that needed to be "remove[d]." As a result, the

[3] In September, 2013, DOJ proposed amendments to Rule 14 that would remove the territorial limits for electronic data searches. Numerous objections to the proposed changes on constitutional and privacy grounds have been filed, including objections by the ACLU, EPIF (Electronic Privacy Information Center), the EFF (Electronic Frontier Foundation) and the Federal Bar Council.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Government is now in the uncomfortable position of having advised Congress that Rule 41 must be changed to allow for things like NIT data searches, while at the same time telling this Court that the NIT warrant was just fine and fully complied with the Rule as it is now written.

The Government's awareness that the NIT warrant violated Rule 41 is also revealed by DOJ's own analysis of the limits the Rule places on law enforcement. According to DOJ's manual on *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (DOJ Electronic Evidence Manual), when "data is stored remotely in two or more different places within the United States and its territories, agents should obtain additional warrants for each location where the data resides *to ensure compliance with a strict reading of Rule 41(a).* For example, if the data is stored in two different districts, agents should obtain separate warrants from the two districts" (emphasis added). *Id.* at 84-85.[4]

The DOJ manual then addresses situations where, as here, "agents do not and even cannot know that data searched from one district is actually located outside the district[.]" *Id.* at 85. In these types of situations, the manual cautions that the violation should not lead to suppression in two circumstances. One is where a court concludes "that agents sitting in one district who search a computer in that district … *unintentionally* cause[d] intangible information to be sent from a second district into the first…." *Id.* (emphasis added). The manual goes on to explain that failure to comply with Rule 41 may lead to suppression if agents "intentionally and deliberately disregarded the Rule, or the violation leads to 'prejudice' in the sense that the search might not have occurred or would not have been so 'abrasive' if the Rule had been followed." *Id.*

[4] Available at http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Here, by contrast, the sending of information from Mr. Michaud's Washington computer to the FBI in Virginia was not an unintended byproduct of a search of a Virginia computer; the Government knew that most or all of the target computers were located outside the district where the NIT warrant was issued; and the FBI intentionally deployed its NIT for the very purpose of causing data to be sent from many districts back to Virginia. *See also*, *id*. at 85 (noting that evidence seized as part of a multi-district data search in violation of Rule 41 may lead to suppression unless agents "cannot know" at the time of the search that it would violate the Rule "either legally or factually").

Given these facts and DOJ's own assessment of the limits imposed by Rule 41, the Government's position can be summarized as follows. First, its efforts to amend Rule 41 and vastly expand its search and surveillance powers have not been successful. Second, the Government nevertheless elected to deliberately circumvent the Rule. Third, the Court should now endorse the Government's direct challenge to the rule of law and approve a vast expansion of its search and seizure powers by adopting an interpretation of Rule 41 that has no basis in the Rule itself and is inconsistent with DOJ's own understanding of the limits imposed by the Rule. *See generally United States v. Coreas*, 419 F.3d 151, 151 (2d Cir. 2005) ("Child pornography is so repulsive a crime that those entrusted to root it out may, in their zeal, be tempted to bend or even break the rules. If they do so, however, they endanger the freedom of all of us.").

In support of its argument, the Government maintains that "three separate provisions of Rule 41(b) support issuance of the NIT warrant." Govt. Response at 11. Each of these arguments is readily disposed of.

1. Mr. Michaud's Computer was Not Located in Virginia When the NIT Warrant was Issued (Rule 41(b)(2)).

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

The Government first makes a run at Rule 41(b)(2), which allows magistrates "to issue a warrant for a person or property outside the district if the property is located within the district when the warrant is issued but might move or be moved outside the district before it is executed." *See* Govt. Response at 11. According to the Government, this provision applies because "Website A" was located on a server in Virginia; the NIT malware was stored on the server prior to its deployment against target computers; and Mr. Michaud "reached into EDVA to access the site." *Id*.

All of which is irrelevant. According to the plain language of Rule 41(b)(2), the property subject to a search must be located "*within the district* when the warrant is issued." There is no dispute that Mr. Michaud and his computer were nowhere near Virginia when either the Title III or NIT warrants were issued. *See also In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 757 (S.D. Tex. 2013) (rejecting the Government's "interpretation" of (b)(2) because "a moment's reflection reveals" that if it were valid, "there would be effectively no territorial limits for warrants involving personal property, because such property is moveable and can always be transported to the issuing district, regardless of where it might initially be found").[5]

Further, none of the data seized by the FBI was delivered to Virginia until *after* the FBI sent its malware to Mr. Michaud's computer in Washington State; the malware

[5] In regard to the *In re Warrant* decision, the Government states that courts have approved NIT-type warrants in three other cases. Govt. Response at 13. Of course, warrant applications are made *ex parte*, so the real test is whether any courts have upheld an NIT warrant after it was challenged. In *Cottom*, the Nebraska NIT cases discussed in earlier pleadings, the only challenge the defendants made to the searches of their computers was a claim that the Government had not given timely notice of the searches. *See* exh. A (Findings and Recommendation in *Cottom, et al*). The "Timberlinebombinfo" case (*see* Govt. Response at 13, ll. 17-20) involved a juvenile defendant and most of the court records are unavailable, so it is unclear if any search and seizure issues were even litigated. Defense counsel was also unable to identify the defendant in the "texas.slayer" case (*see* Govt. Response at 13, ll. 14-16) or determine what, if any, challenges he or she made to the search warrant.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

executed a data search on the Washington computer; and then sent that data *back to* Virginia. To suggest that this sequence of events amounts to a search in Virginia not only fails the straight face test, but is inconsistent with the Government's concession in other cases that its NIT's are in fact conducting searches on target computers in the various places where those computers are located. *See* exh. A, attached hereto, at 4 (Findings and Recommendations in *United States v. Cottom,* a 2013 Nebraska NIT case, noting that "the parties agree and stipulate the Court may assume that the court/warrant authorized deployment of the pertinent investigative technique *effected a Fourth Amendment search of an activating* [i.e. target user's] *computer*") (emphasis added).

2. The NIT is Not a Tracking Device (Rule 41(b)(4)).

The Government's attempt to characterize the NIT as a "tracking device" for purposes of Rule 41(b)(4) is equally misguided; in fact, this part of the Government's argument practically refutes itself. Govt. Response at 12. As the Government itself recognizes, a tracking device is defined as a mechanism that "permits the tracking of the movement of a person or object." *See* Fed. R. Crim. P. 41(a)(2)(e) (referencing 18 U.S.C. § 3117(b)). The NIT had nothing to do with tracking or movement; it is designed to search and seize data on target computers. The fact that "investigators subsequently used this network information to identify and locate Michaud," Govt. Response at 12, does not transform the NIT into a tracking device any more than the use of a seized address book to locate a suspect transforms the book into a tracking device.

In addition, Rule 41(b)(4) specifies that it applies only if the tracking device is installed within the district where the warrant is issued. According to the Government, it met this requirement because it "installed" the NIT on the Virginia server. Govt. Response at 12. But the installation at issue for purposes of the Rule is not where the

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Government happens to store its search tools, but the location of the person or property on to which a tracking device is attached. If the Rule could be read in the way the Government proposes, its limitations would be meaningless. For example, in an actual tracking case, the Government could store all its GPS locators at FBI headquarters; get Virginia warrants to install them all over the country; and simply mail the trackers to local FBI offices for attachment to cars anywhere in the country. It should go without saying that the Rule does not allow for these types of circumventions.

Finally, the Government never suggested in its warrant applications that it was seeking authorization for a tracking device, and it concedes now that the data it seized from Mr. Michaud's computer "was not itself location information." Govt. Reply at 12, l. 16. In short, the NIT is a data search tool, not a tracking device; the data it seized has nothing to do with "the movement of a person or property"; and it was installed on a Washington computer, not in Virginia. Despite all that, according to the Government, the Court should find that Rule 41(b)(4) serves nicely.

3. Rule 41(b)(1) Also Does not Apply Because Mr. Michaud's Computer Was Never in Virginia.

In its final attempt to rewrite Rule 41, the Government half-heartedly suggests that Rule 41(b)(1) might apply, regardless of the fact that this provision only authorizes warrants for "a person or property located within the district." Govt. Response at 12-13. Although the Government's argument is hard to grasp, it appears to be contending that since legal and readily available privacy software makes it difficult or impossible to determine where a computer is located, it is "reasonable" to just ignore Rule 41(b)(1) entirely. That is not much of an argument, and the Government hardly helps it by suggesting that ignoring the Rule "does not risk significant abuse" because searches done in violation of it are subject to later judicial review for reasonableness. Govt. Response at 12-13. Of course, that is exactly where we are in the process, and the fact

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

that the Government cannot offer a persuasive argument for concluding that the NIT warrant was properly issued goes a long way toward showing that the search of Mr. Michaud's computer was unreasonable.

The Government also cites three cases for the vague proposition that the NIT warrant was "consistent" with Rule 41. Govt. Response at 10-11. None of these cases are relevant.

The Government first cites *United States v. New York Telephone Co.*, 434 U.S. 159 (1977), a case decided long before the dawn of personal computers and the Internet, in support of the odd notion that Rule 41 is "sufficiently flexible" to allow for searches that the Rule's actual language does not allow. Govt. Response at 10. There, the issue before the Court was whether call information collected pursuant to an otherwise valid pen register order fell within the definition of "property" in Rule 41(h) (now Rule 41(a)(2)(A)). In a straightforward exercise of statutory interpretation, the Court noted the Rule's language that "[t]he term 'property' is used in this rule to *include*" various specified items (emphasis by the Court), which the Court concluded "indicates that it was not intended to be exhaustive." *Id.* at 169 n. 18; s*ee also id.* at 169 ("it does not restrict or purport to exhaustively enumerate all the items which may be seized").

Here, the situation could hardly be more different. Rule 41(b) enumerates in detail five categories of searches a magistrate judge may authorize. The categories are limited and exhaustive, not illustrative. To expand the list in the way the Government proposes, to allow searches anywhere and everywhere regardless of jurisdiction, would render the language of the Rule meaningless. It thus plainly does not allow courts to authorize searches of unknown targets located in unknown locations outside the issuing district, and there is no remotely credible interpretation of the Rule that does.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Likewise, *United States v. Koyomejian*, 970 F.2d 536 (9th Cir. 1992), has nothing to do with the issues in this case. *See* Govt. Response at 10. In *Koyomejian,* a judge in the Central District of California issued a warrant authorizing silent video surveillance of a target located in the district. The defendant challenged the surveillance on the ground that it was prohibited by 18 U.S.C. § 2511 (relating to the interception of wire communications) and the Foreign Intelligence Surveillance Act. *Id*. at 538. The defendant did not claim that the Government had violated Rule 41, and the court merely noted in passing (as a straightforward application of the *New York Telephone Co*. holding that electronic information was among the property encompassed by the Rule) that the Rule authorizes courts to issue video surveillance warrants. *Id*. at 542. No doubt it does, when the authorization is for surveillance of a person or property located within the issuing court's district; the surveillance is particularized and does not extend to thousands of unknown targets across the country and around the world; and the Government has been candid about the nature and scope of the authorization it is seeking. Unfortunately for the Government, none of those things happened here and the decision in *Koyomejian* is not helpful to it.

Reaching even further afield, the Government also cites an old Seventh Circuit case, *United States v. Torres*, 751 F.2d 875 (7th Cir. 1985). Govt. Response at 11. *Torres* also involved video surveillance, this time of a terrorist group engaged in bomb making. *Id.* at 876. The court, relying on *New York Telephone,* concluded that Rule 41 allows courts to issue warrants for video surveillance, just as the *Koyomejian* court did. *Id*. at 877-78. The rest of the opinion addresses whether the surveillance warrant also complied with Title III, *id.* at 883-85, and other issues not relevant to this case.

In sum, DOJ's deliberate violation of Rule 41 amounts to a direct challenge to the rule of law when it comes to Congress's and the Supreme Court's authority to oversee federal investigation of criminal cases and ensure that the Government's law

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

enforcement methods are consistent with constitutional guarantees. What the Government is saying in effect here is that it wants Rule 41 changed in a way that vastly increases its powers, but since Congress and the Supreme Court have not approved that expansion of powers, it is free to ignore the rules. It goes virtually without saying that the Government's efforts to coopt this Court in its efforts to circumvent the law should be firmly rejected.

B. The Exigency Exception to the Fourth Amendment's Warrant Requirement Does not Apply.

The Government fares no better when it invokes exigency as a basis for avoiding suppression. Govt. Response at 15-16. The exigency exception is narrow and only applies to warrantless searches prompted by a risk of harm so imminent that there is no time to obtain a warrant. A variety of circumstances may give rise to an exigency sufficient to justify a warrantless search, including law enforcement's need to provide emergency assistance to an occupant of a home, *Michigan v. Fisher*, 558 U.S. 45, 47–48 (2009) (*per curiam*), or to engage in "hot pursuit" of a fleeing suspect. *United States v. Santana*, 427 U.S. 38, 42–43 (1976). In some circumstances, law enforcement officers may also conduct a warrantless search to prevent the imminent destruction of "highly evanescent" evidence. *Cupp v. Murphy*, 412 U.S. 291, 296 (1973) (limited intrusion of collecting fingernail scrapings from murder suspect without a warrant was reasonable, particularly in light of facts indicating that he was trying to destroy the evidence during interrogation). "While these contexts do not necessarily involve equivalent dangers, in each a warrantless search is potentially reasonable because 'there is compelling need for official action and *no time to secure a warrant*.'" *Missouri v. McNeely*, __ U.S. __, 133 S. Ct. 1552, 1559 (2013) (citation omitted) (emphasis added).

Here, the harm was so far from imminent that the Government elected to maintain the status quo and continue distributing child pornography for an additional

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

two weeks. Nor was the Government in any way concerned with the imminent destruction of evanescent evidence; it instead deployed the NIT to seek out and collect stored data.

Given these facts and the applicable law, the exigency exception to warrantless searches is a non-starter, and what the Government is really asking the Court to do is create a new Fourth Amendment rule. The Government's argument seems to go as follows: If the Court finds that Rule 41 does not allow for warrants like the NIT warrant, then the FBI can never get a warrant to capture identifying data about many criminals who use the Tor network, and therefore there were "exigent" circumstances. With this argument, the Government seeks to create an entirely new exception to the Fourth Amendment's warrant requirement – where a warrant would not be authorized because the law does not allow it, the police can simply ignore the law and search without one. *See generally Mincey v. Arizona*, 437 U.S. 385, 393, (1978) ("the mere fact that law enforcement may be made more efficient can never by itself justify disregard of the Fourth Amendment"). Not surprisingly, the Government cannot cite to any case supporting this novel concept of "exigent" circumstances, which might better be characterized as "the ends justify the means" rule. Even accepting the dubious proposition that the Government had no alternative ways of trying to identify people who accessed "Website A," the Government does not get to unilaterally strike its preferred balance between the limits on its search and seizure powers and allowing some Internet criminals possibly to go unapprehended.

Finally, the Government's repeated claim that it will be unable to identify targets on the Tor network without circumventing Rule 41 is indeed doubtful. Traditionally, law enforcement has engaged in such legitimate tactics as engaging in chats with Internet targets; posing as pornography distributors or as minors to elicit identifying information; offering to exchange new pictures or videos on peer-to-peer networks,

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

which exposes a target's identifying data; or luring targets to messaging forums and sites where their IP addresses can be more readily captured. *See, e.g.*, Donna Leinwald Leger, *How FBI Brought Down Cyber-Underworld Site Silk Road,* USA Today, May 15, 2015.[6] In addition, it appears that the FBI is now identifying targets on the Tor network by means of controlling or gaining access to network "relays," which alter or strip identifying information as it travels on the network. *See* Cory Bennett, *Researchers Deny FBI Paid Them $1M to Unmask Dark Web Users,* The Hill, Nov. 18, 2015;[7] *see also* Bruce Schneir, *Attacking Tor; How the NSA Targets Users' Online Anonymity*, The Guardian, Oct. 4, 2013 (reporting on NSA and law enforcement methods for monitoring and identifying Tor users by redirecting illicit network traffic).[8] While some of these methods may also be subject to legal challenge, the point here is that the Government's investigatory options are not nearly as limited as it suggests.

Of course, these methods may require law enforcement to invest considerable time and resources to develop their leads, rather than merely keep an illicit web site up and running while NIT's are automatically deployed to thousands of computers. And it is certainly possible that some criminals would not get apprehended without using NIT's. But upholding the Fourth Amendment, and the laws and rules that implement its guarantees, inevitably comes with some crime-fighting costs, and requiring the Government to adhere to Rule 41 will not leave it as helpless to fight crime on the Tor network as it claims.

C. Mr. Michaud had a Reasonable Expectation of Privacy in his Personal Data.

---

[6] Available at: http://www.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/

[7] Available at: http://thehill.com/policy/cybersecurity/260598-researchers-deny-fbi-paid-them-1m-to-unmask-dark-web-users

[8] Available at: http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

The Government asserts, almost in passing, that Mr. Michaud had no reasonable expectation of privacy in the IP address and other computer data (such as the type of operating system he was using) that was captured by the NIT. Govt. Response at 16, 21. Its minimal emphasis on this point is understandable, because it is completely misplaced.

The Government states that *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2007), held that "a defendant lacks a reasonable expectation of privacy in IP addresses." Govt. Response at 16. This characterization of the case is misleading. What *Forrester* dealt with (as is made clear in the opinion and as the Government concedes later in its Response at 21) was computer users' expectation of privacy in "IP addresses of the *websites they visit*." 512 F.3d at 510 (emphasis added). Moreover, the Government had collected the defendant's IP address by installing a monitoring program with a third party, his Internet service provider, not by searching Forrester's personal computer. *Id*. at 505. The *Forrester* court therefore concluded that the situation was analogous to telephone pen registers, which involve "a device that records numbers dialed from a phone line," information that the caller had necessarily shared with his or her phone company. *Id.* at 509.

Here, by contrast, a computer user who accesses a web site through the Tor network does not need to convey his or her IP address, and in fact has taken steps to protect the privacy of that information. *See also id.* at 511 (where the *Forrester* court emphasized that its analysis applied only to the specific facts and techniques at issue).

The Government also cites to *United States v. Suing*, 712 F.3d 1209, 1213 (8th Cir. 2013). Govt. Response at 19. What *Suing* held, along with the cases on which it relies, is that a person who chooses to share files on a peer-to-peer network has no reasonable expectation of privacy in his or her IP address, since that address is inevitably disclosed along with the shared files. *Id.* The very essence of a peer-to-peer

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

network is that one publicly announces, via a network, that one is sharing files and then gives others access to the computer on which those files are stored. "One who gives his house keys to all of his friends who request them should not be surprised should some of them open the door without knocking." *United States v. Stults*, 575 F.3d 834, 843 (8th Cir. 2009).

In this case, Mr. Michaud did not engage in peer-to-peer file sharing or offer to share his identifying data. In sharp contrast to *Suing*, he used the Tor network to ensure that, when he contacted sites on the network, he was not announcing his IP address or otherwise inviting anyone to open his door without knocking.

Simply put, the facts in this case are almost diametrically opposed to the facts in *Forrester* and *Stults*. Mr. Michaud had a reasonable expectation of privacy in his IP address and other information.

D. The NIT Search is Not Authorized by the Title III Order.

The Government argues that the Title III warrant also authorized it to deploy the NIT and remotely search Mr. Michaud's computers. Govt. Response at 14-15. As the Title III warrant itself makes plain, it did not.

First, the Title III application sought authorization for real time interception of private chat and messages on "Website A's" chat forums and instant messaging services. *See, e.g.*, First Motion to Suppress, exh. B at B-035-38 (Bates 293-96); B-057 at ¶ (b) (Bates 315). As explained in Mr. Michaud's First Motion to Suppress, the Government sought a Title III warrant because 18 U.S.C. § 2511 generally prohibits electronic communication service providers from monitoring the content of customer communications, and the FBI had become the service provider for the child pornography site. *See* First Motion to Suppress at 4. Mr. Michaud did not chat or send any messages on the site, and his alleged activity was limited to viewing various

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

pictures, links and postings. Accordingly, the Title III warrant does not apply to him and it has no bearing on the search of his computer.

Second, the Government's Title III argument rests on *United States v. Kail*, 612 F.2d 443 (9th Cir. 1979), which held that the Government need not got separate authorization for a pen register if it already has Title III authorization to monitor related communications. *See* Govt. Reply at 14. Setting aside the fact that Mr. Michaud's limited activities on the site were not covered by the Title III warrant, an NIT is not a pen register. A "pen register" is a device or process for capturing "signaling information" (such as a telephone number) that is transmitted with an electronic communication. *See* 18 U.S.C. § 3127(3). Even assuming an IP address would qualify as "signaling information," the NIT captured more than that (including the type of operating system on target computers). First Motion to Suppress, exh. C (NIT application) at C-028-030 (Bates 161-63).

More importantly, none of the information seized by the NIT was transmitted as part of Mr. Michaud's communications with "Website A;" in fact, finding and seizing that data was the reason an NIT was deployed, because it was not sent with any communications between users of the site and the site itself. It was only *aft*er data was separately seized by the NIT that it was transmitted to the FBI, without Mr. Michaud's knowledge or consent. *See* First Motion to Suppress, exh C (NIT Warrant Application) at C-028, ¶ 33 (Bates 161) (after a "user's computer successfully downloads those instructions [*i.e.* the NIT] from the TARGET WEBSITE," the NIT would then cause "the user's 'activating' computer to transmit certain information to a computer controlled by or known to the government."). Given these facts, the NIT was used to effect an independent search on Mr. Michaud's computer for undisclosed data, and it is not comparable to a pen register that merely records information that has already been shared as part of a voluntary communication.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Finally, the Government should know that the Title III warrant does not cover the NIT searches or the type of information those searches were seizing, because it said as much in its Title III application. Specifically, the Government included a section in that application titled "Deployment of Network Investigative Technique." Motion to Suppress, exh. B at B-041-042 (Bates 299-300). There, the Government summarized how the NIT would execute searches on target computers and informed the court that it would seek "separate authorization" for deployment of the NIT and the execution of NIT searches. *Id*. at B-042, ¶ 53. That "separate authorization" was the NIT warrant, and the Government cannot credibly maintain now that the NIT did not actively seize data that was not part of the communications between target computers and "Website A" or that the entire NIT warrant was unnecessary.

E. The Government's Violation of Rule 41 and NIT Search Requires Suppression.

The Government maintains that, even if it violated Rule 41, "suppression is neither required by law nor reasonable under the circumstances." Govt. Response at 17. Conspicuously missing from the Government's response, however, is any substantive discussion of the standard for suppression set forth in *United States v. Weiland*, 420 F.3d 1062 (9th Cir. 2005). *See* First Motion to Suppress at 14. There, the Ninth Circuit held that suppression is the appropriate remedy for a violation of Rule 41 if the violation was the result of an "intentional and deliberate disregard" for a provision in the Rule; the violation was of "constitutional magnitude"; or the defendant was prejudiced by the violation, in the sense that the search would not have occurred but for the violation. 240 F.3d at 1071. Any one of these circumstances requires suppression, and in fact all three apply in this case.

The Government starts by suggesting that it did not deliberately violate the Rule because it can offer several tortured interpretations of provisions in it (like those related

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

to tracking devices) that the Court should adopt as after-the-fact justifications for the NIT warrant. Beyond the fact that these interpretations ignore what the Rule actually says and are patently meritless, it is abundantly clear that the Government knew at the time the NIT warrant was issued that it violated Rule 41. In this regard, the Court need only consider DOJ's efforts to get Rule 41 changed, starting in 2013 and well before applying for the NIT warrant.

Obviously, there would be no need to change the Rule if it already allowed the Government to do what it did. Moreover, DOJ's efforts were prompted, at least in part, by the decision in *In re Warrant*, 958 F. Supp. 2d 753 (S.D. Tex. 2013). As the Court is aware, that decision considered many of the same arguments the Government is making here about the scope of Rule 41 and unequivocally rejected all of them. *See* First Motion to Suppress at 10. In a 2013 letter to the Advisory Committee on Criminal Rules, DOJ cited the decision as a reason to change the Rule's jurisdictional limits. *See* September 18, 2013 letter from Acting Asst. Attorney General Mythili Raman to the Hon. Reena Raggi, Chair, Advisory Committee on the Criminal Rules (available at: www.uscourts.gov/file/15534/download, at p. 172) (minutes and records of the Advisory Committee's April 7-9, 2014 meeting). This letter also makes plain that DOJ fully understood, at least since 2013, that the Rule did not permit multi-district data searches, and directly contradicts the Government's representations now that Rule 41 allows for such searches. *See id*. at 173 ("Authorizing a court in a district where activities related to a crime have occurred to issue a warrant for electronic storage media within or outside the district would better align Rule 41 with the extent of constitutionally permissible warrants and *remove an unnecessary obstruction currently impairing the ability of law enforcement to investigate*. . . multi-district Internet crimes") (emphasis added); *see also id.* at 171 ("The amendment *would establish* a court-supervised framework through which law enforcement can successfully

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

investigate and prosecute sophisticated Internet crimes, *by authorizing* a court in a district where activities related to a crime have occurred to issue a warrant - to be executed via remote access - for electronic storage media and electronically stored information located within or outside that district") (emphasis added). And, of course, if there were any lingering doubt that the Government's violation of the Rule was deliberate, the Court need only consider DOJ's own analysis of the Rule (which is consistent with Mr. Michaud's) and the Government's calculated efforts to mask the true targets of the NIT warrant to put those doubts to rest. *See* pp. 5-6, *supra*.

If the Court finds that the violation was deliberate, no further analysis is required for suppression under *Weiland*. Nevertheless, the Government argues that, even if it deliberately violated the Rule, suppression is not required unless the violation was also the product of "bad faith." Govt. Response at 21. In positing this argument, the Government not only ignores the standard for suppression set forth in *Weiland*, *supra*, which does not include any such "bad faith" test, but also misconstrues the decisions in two other cases.

The Government first cites *United States v. Luk*, 859 F.2d 667 (9th Cir. 1987), a case that pre-dates *Weiland* by almost two decades, for the proposition that suppression is not an appropriate remedy unless any "putative violation" of Rule 41 "rises to the level of bad faith." Govt. Response at 21. In *Luk*, the defendant claimed that a search warrant was invalid because it had been requested by an investigator for the Department of Commerce and she did not qualify as a "federal law enforcement officer or an attorney for the government" under Fed. R. Crim. P. 41(d)(2)(A). *Id*. at 670. The court found that the error, unlike the violations in this case, was merely "technical" and "not a constitutional violation." *Id*. at 673. Moreover, contrary to the Government's misleading quotation from the decision (Govt. Response at 21, ll. 9-10), the court actually went on to state, "[n]or was there any indication of 'bad faith' *or* 'deliberate

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

disregard' of Rule 41," by either the agent who submitted the application or the prosecutor who had approved it. *Id.* at 674 (emphasis added). Hence, contrary to the Government's suggestion that the decision required a showing of "bad faith" separate and apart from deliberate disregard for the Rule, the court recognized that evidence of deliberate disregard supports suppression; it simply found that there had been "absolutely no attempt to avoid compliance with any of Rule 41's requirements[.]" *Id.*

The Government's reliance on *United States v. Williamson*, 439 F.3d 1125 (9th Cir. 2006), is equally misplaced. *See* Govt. Response at 21. There, the defendant sought suppression because the officers who had executed a search at his home had shown him the search warrant but failed to give him a copy of it until they were leaving the house, rather than at the outset of the search. *Id*. at 1130. Although Rule 41 does not expressly require officers to serve a copy of the warrant at the outset, Williamson relied on Ninth Circuit case law that imposed such a requirement. *Id*. at 1130. The officer who had given Williamson a copy of the warrant testified that he was not aware of any requirement that service should have been completed earlier, and the court found that he had been genuinely unaware of the requirement, rather than deliberately ignoring it. *Id*. at 1134. The court also noted that Williamson (unlike Mr. Michaud) had not claimed that the alleged violation was more than a technical error, or that the search would not have occurred if the applicable rules had been followed, as required to show prejudice. *Id*. at 1132-33 (further noting that "suppression is rarely the proper remedy for a Rule 41 violation," but then listing the three circumstances also set forth in *Weiland* where suppression is required); *compare also United States v. Gantt*, 194 F.3d 987, 994-95 (9th Cir. 1999) (granting motion to suppress based on showing that officers had deliberately violated Rule 41(d) by failing to provide the defendant with a copy of the warrant) (overruled on other grounds, *United States v. W.R. Grace*, 526 F.3d 499, 506 (9th Cir. 2008)).

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Here, by contrast, there can be no credible dispute that the Government knew full well that it was circumventing Rule 41 when it applied for the NIT warrant. After all, DOJ had tried get the Rule changed before applying for the warrant, and it can hardly claim now that it was unaware of the limits imposed by the Rule. And, as previously noted, DOJ's own analysis of Rule 41 explains the limits it imposes on data searches and the risk of suppression if those limits are not respected. Even beyond the test articulated in *Weiland*, what the Government's "good faith" argument misses is that if agents deliberately violate a legal requirement, they cannot be said to have acted in good faith.

Moreover, regardless of whether the Government deliberately violated the Rule, suppression is required in this case on the independent ground that the violation is of constitutional magnitude. *Weiland*, 420 F.3d at 1071. "Constitutional magnitude" is not defined in *Weiland* but, given the constitutional underpinnings of the Rule itself as a tool for preventing overbroad and general warrants, it appears to apply to any violation that is more than merely technical or ministerial. *See* First Motion to Suppress at 14-16. In any event, the Court should find that the violations here are of constitutional magnitude because the Government obtained anticipatory authorization to search an unlimited number of computers and databases, regardless of their location, based on a showing of probable cause that is, at best, marginal. *See* Second Motion to Suppress (Dkt. 65). The scope of the search and seizure power the Government is asking the Court to approve is unprecedented, implicates core privacy interests, and is unreasonable under the Fourth Amendment, all of which makes the rule violation one of constitutional magnitude.

Finally, in contrast to *Luk* and *Williamson*, suppression is also required because Mr. Michaud was prejudiced by the violation. As explained in those cases and *Weiland*, and as DOJ itself has recognized, "prejudice" in this context is "'prejudice' in

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

the sense that the search might not have occurred" if the Rule had been followed. *See* DOJ Electronic Evidence Manual, *supra*, at 85; § II.A, s*upra*; *Williamson*, 439 F.3d at 1133; *Luk*, 859 F.2d at 670; *Weiland*, 420 F.2d at 1071. It is beyond cavil that the search of Mr. Michaud's computer would not have occurred without the NIT warrant, and the warrant itself violated Rule 41. The Government's arguments against a finding of prejudice completely ignore the causality test that these cases use. *See* Govt. Response at 20, ll. 7–21.

Having failed meaningfully to address any of the three independent grounds for suppression set forth in *Weiland*, the Government's argument that suppression is "neither required nor reasonable" is unavailing. *See also United States v. Tucker*, 8 F.3d 673, 679 (9th Cir. 1993) (Norris, J., concurring) ("The exclusionary rule. . . often benefits the guilty as well as the innocent, but we have long since decided we are willing to pay that social cost in order to promote compliance with the Fourth Amendment.")**.**

F. The Government Government Cannot Hide Behind "Good Faith" to Salvage the NIT Warrant.

The Government also tries to save the NIT warrant by invoking the "good faith" exception to the exclusionary rule. *See* Govt. Response at 22 (although some of the relevant facts overlap, this argument is separate from the Government's argument that the Court should not suppress based on a violation of Rule 41 unless it finds "bad faith," *see* § II.E, *supra*). In fact, the good faith exception is not even remotely applicable in this case.

As a threshold matter, if the Court finds that the Government violated Rule 41 and that the violation was deliberate, prejudicial, or of constitutional magnitude, then the good faith exception is inapplicable. *See* § II.E, *supra*. *Weiland* clearly holds that

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

suppression is "required" if any of those types of violations occurred, without reference to good faith (except to the extent that a deliberate violation by definition establishes a lack of good faith). 420 F.3d at 1071 (quoting *United States v. Martinez-Garcia*, 397 F.3d 1205, 1213 (9th Cir. 2005)).

Further, even if the good faith exception could apply in this case, it does not. As a general matter, the Supreme Court has made clear that the exclusionary rule is meant to deter "deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." *Herring v. United States*, 555 U.S. 135, 144 (2009). The *Leon* Court reasoned that where law enforcement conduct is "pursued in *complete* good faith," the exclusionary rule's deterrent function "loses much of its force." *United States v. Leon*, 468 U.S. 897, 919 (1984) (emphasis added). However, an officer's subjective intentions are irrelevant for purposes of determining whether the exception applies. *See United States v. Song Ja Cha*, 597 F.3d 995, 1005 (9th Cir. 2010) ("*Herring* emphasizes that the standard is 'objective,' not an inquiry into the subjective awareness of arresting officers") (citations and internal quotation marks omitted). Instead, responsible law-enforcement officers are expected to learn "what is required of them" under Fourth Amendment precedent and to conform their conduct to these rules. *Hudson v. Michigan*, 547 U.S. 586, 599 (2006). The objective standard also "requires officers to have a reasonable knowledge of what the law prohibits." *Leon*, 468 U.S. at 919, n. 20, *citing United States v Peltier*, 422 U.S. 531, 542 (1975); *see also, e.g., United States v. Brown*, 832 F.2d 991, 995 (7th Cir. 1987) ("Police officers in effecting searches are charged with knowledge of well-established legal principles as well as an ability to apply the facts of a situation to those principles"). The reasonableness of an officer or agent's conduct is therefore determined under an objective standard by asking whether "a reasonably well trained officer would have known that the search was illegal

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

in light of all the circumstances." *United States v. Camou*, 773 F.3d 932 (9th Cir. 2014) (quoting *Herring*, 555 U.S. at 145).

Thus, the question before this Court is what a reasonably well trained officer should have known about the limits imposed by Rule 41 when applying for the NIT warrant. Without belaboring the facts further, it should be obvious at this point that a reasonably well-trained FBI agent would know, from the plain language of Rule 41, that a warrant could not legally authorize searches of potentially thousands of computers in unknown locations. If this were not already self-evident, the Court need only consider DOJ's efforts to amend the Rule and its own analysis of the limits the Rule imposes on data searches to conclude not only that everyone involved with the "Website A" operation and the NIT warrant application was aware that they were not acting in accordance with the law, but also that they were making a concerted effort to circumvent it.

In addition, the good faith exception is not available to the Government if the Court finds that the NIT warrant application was based on intentionally or recklessly false statements or omissions that were material to a finding of probable cause. *Mills v. Graves*, 930 F.2d 729, 733 (9th Cir. 1991) (citing *Leon*, 468 U.S. at 914). In this regard, the Government maintains that it was "objectively reasonable" for the FBI to rely on the NIT warrant because a Magistrate Judge had signed the warrant "after having been made aware of how the NIT would be implemented and its reach." Govt. Response at 22, ll. 15-16. However, as detailed in Mr. Michaud's Motion for *Franks* Hearing (Dkt. 65), the Government in fact went to great lengths to obscure what it was asking for in the NIT warrant application, going so far as to make false statements about the location to be searched. *See id*. at 13-15. As one court has observed, "it is one thing to admit evidence innocently obtained by officers who rely on warrants later found invalid due to a magistrate's error. It is an entirely different matter when the

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

officers are themselves ultimately responsible for the defects in the warrant." *United States v. Reilly*, 76 F.3d 1271, 1281 (2d Cir. 1996). If the Court finds, as it should, that the Government's NIT warrant application was intentionally or recklessly misleading, then the good faith exception simply does not apply.

Finally, the good faith exception does not apply when law enforcement agents rely on a facially overbroad warrant that effectively authorizes a general search. *United States v. Spilotro*, 800 F.2d 959, 968 (9th Cir. 1986). As set forth in Mr. Michaud's Second Motion to Suppress (*see* dkt. 65 at pp. 17-20), the warrant in this case authorized the searching of literally hundreds of thousands of computers. Consequently, regardless of whatever subjective belief the executing officers may have had about the validity of the warrant, the Government cannot rely on the good faith exception in trying to defend it. *See also, generally, United States v. Kow*, 58 F.3d 423 (9th Cir. 1995) (where a warrant encompassed essentially all documents on the premises, the court has been "'vigilant in scrutinizing officers' good faith reliance on such illegally overbroad warrants") (quoting *Ortiz v. Van Auken*, 887 F.2d 1366, 1370 (9th Cir. 1989)).

G. The Delayed Notice Issues.

Finally, in his First Motion to Suppress Evidence, Mr. Michaud alleged that the Government had violated the notice requirements of Rule 41(f). First Motion to Suppress at 16-18. On November 10, 2015, almost a month after the motion was filed, the Government disclosed that it had obtained three sealed orders in the Eastern District of Virginia, each authorizing an additional 90 days of delayed notice, with the latest order issued on September 24, 2015. While this late discovery resolves Mr. Michaud's original claim that the Government had violated the Virginia court's February 20, 2015 delayed notice order, it reveals some new problems. It now appears that the Government's applications for the two most recent orders willfully or recklessly

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

omitted material information that would likely have led the Virginia court to deny the extension requests.

Specifically, the February 20 NIT warrant authorized the Government to delay providing notice of its NIT searches to the target of those searches for up to 30 days "after any individual accessing the TARGET WEBSITE has been identified to a sufficient degree as to provide notice." First Motion to Suppress, exh. C at C-002 (Bates 135).

On April 3, 2015, the Government requested a 90 day extension of the delayed notice order because investigators were still collecting internet service provider subscriber records and other information needed to identify users. *See* exh. B, attached hereto, at Bates 414. However, the Government also told the Virginia court that providing copies of the NIT warrant to any of the targets (even after they were identified) might "alert thousands of suspects under investigation" that law enforcement had interdicted the target website. *Id*. at Bates 415. The Government acknowledged that the only identifying information about the site that appears in the warrant is a reference to its URL address, *see id*., and all of the related records refer to the site simply as the "Target Website." Nevertheless, the Government alleged that users of child pornography sites on the Tor network "are extremely sensitive to law enforcement infiltration" and "providing a single person with notice if the execution of the NIT warrant could. . . alert thousands of suspects under investigation to the ongoing investigation." *Id.* The Government illustrated this point by citing an example where publication of a news article about a different website investigation had generated online postings and comments which may have led some target users to destroy evidence or flee. *Id*.

The Government submitted two more applications for extension of the delayed notice order, on June 30 and September 24, 2015. *See* exhs. C and D, attached hereto.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

In both these applications, the Government renewed its request to withhold notice from anyone who had been subjected to a NIT search, based on a supposed continuing need to avoid potential news reports and publicity about the investigation. S*ee* exh. C (June 30 application) at Bates 422-23; exh. D (Sept. 24 application) at Bates 430-31.

Given that the Government's concerns about timely disclosure of the NIT warrant rested on its single reference to a URL address, it is puzzling that it did not simply request permission to redact the URL address from service copies of the warrant, rather than seek to avoid the requirement of timely notice entirely. Setting aside any concerns about whether the orders should have been more narrowly tailored, it is apparent that the Virginia court issued its extension orders (which authorized delayed notice even to defendants, like Mr. Michaud, who had not only been identified but charged) based on the Government's representations about the need to avoid news reports and publicity about the "Website A" investigation.

Unfortunately, while representing to the Virginia court that avoiding disclosure of the site's URL address was critical to ongoing investigations, the Government failed to inform the court that it already had disclosed the actual name of the website and a host of other identifying details that went considerably beyond its URL address.

As this Court is aware, the Government started disclosing details of the "Website A" investigation prior to the two most recent delayed-notice applications. First, in early June, 2015, the Government publicized its arrest of a Texas doctor and disclosed details about its use of the NIT to shut down "Website A." *See* Defendant's Response to Govt. Reply to Motion to Vacate (Dkt. 42) at 10. Then, on July 6, 2015, the Government filed a motion to unseal the warrant application in *United States v. Ferrell* which, while not naming the site, included such information as a detailed description of its home page, the specific instructions given to new members, the names of its various sections and forums, and descriptions of the site's content. *Id.* at 9. All of that information was

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

at least as likely to alert users to the investigation as disclosure of the site's URL address, which was the only identifying piece of information in the NIT warrant itself.

Finally, on September 23, 2015 (one day before the most recent application for delayed notice), the Government disclosed the actual name of the site in a publicly filed complaint, which was promptly repeated in local and online news reports. *See id.* at 6.

The Government has explained these disclosures as mistakes, which it made despite its repeated assertions that the investigation was highly confidential and its targets are "extremely sensitive" to information leaks. But regardless of the reasons for its disclosures, the Government will be hard pressed to explain why the Virginia court has never been notified about them, so that it could fully assess whether there is a legitimate and continuing need to limit the notice rights of defendants.

In short, the Government's recent production of the delayed notice extensions establishes that it complied with the letter of those orders. Nevertheless, the Court should consider the Government's omissions and apparent lack of candor in seeking those orders when determining whether, under the totality of the circumstances, the search of Mr. Michaud's computer was reasonable; whether the Government's violations of Rule 41 were deliberate, therefore meriting suppression as a remedy; and whether the Government has acted in "good faith."

III. CONCLUSION

For the reasons stated above, as well as in Mr. Michaud's First and Second Motions to Suppress and Motion for *Franks* Hearing, the Court should suppress all evidence seized pursuant to, or as a fruit of, the NIT warrant.

Dated this 2nd day of December, 2015.

Respectfully submitted,

s/ Colin Fieman
s/ Alan Zarky
Attorneys for Jay Michaud

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

CERTIFICATE OF SERVICE

I hereby certify that on December 2, 2015, I electronically filed the foregoing Reply to Government Response to First Motion to Suppress Evidence [Filed Under Seal] with the Clerk of the Court using the CM/ECF system which will send notification of such filing to all parties registered with the CM/ECF system.

I further certify that emailed a copy of the sealed documents to the registered parties.

s/ *Amy Strickling*
Amy Strickling, Paralegal
Federal Public Defender Office
1331 Broadway, Suite 400
Tacoma, WA 98402
253-593-6710 voice
253-593-6714 facsimile