JUDGE ROBERT J. BRYAN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. DAVID TIPPENS, Defendant.	No. CR16-5110RJB REPLY TO GOVERNMENT RESPONSE TO MOTIONS TO SUPPRESS EVIDENCE ***[Evidentiary Hearing Requested]***
UNITED STATES OF AMERICA, Plaintiff, v. GERALD LESAN, Defendant.	No. CR15-387RJB REPLY TO GOVERNMENT RESPONSE TO MOTIONS TO SUPPRESS EVIDENCE ***[Evidentiary Hearing Requested]***
UNITED STATES OF AMERICA, Plaintiff, v. BRUCE LORENTE, Defendant.	No. CR15-274RJB REPLY TO GOVERNMENT RESPONSE TO MOTIONS TO SUPPRESS EVIDENCE ***[Evidentiary Hearing Requested]***

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

I. REPLY ARGUMENT

A. The Government Ignores the Law Holding That a Warrant Cannot be Expanded With an Unincorporated Affidavit.

The Government gives short shrift to the essential fact that the NIT warrant limited the NIT searches to the Eastern District of Virginia (EDVA). While calling our argument an "obtuse and crabbed reading of the authorizing warrant," the Government conspicuously fails to discuss any of the authority that dictates how the warrant can be read. *See* Govt. Response at 53.

We are mindful that this Court found in *Michaud* that the term "activating computer—wherever located," buried on page 29 of the warrant application, allowed the Court to construe the warrant to cover computers located anywhere in the world. *United States v. Michaud*, 2016 WL 337263 (January 28, 2106) at *9. ("Because this interpretation is objectively reasonable, execution of the NIT warrant consistent with this interpretation should be upheld, even if there are other possible reasonable interpretations."). What was missing in *Michaud*, however, are all of the cases that hold that this Court is bound by the four corners of the warrant itself. *See* Motion to Suppress (dkt. 35) at 24-26.[1] These cases require suppression because the rules of construction are based on the Fourth Amendment's particularity requirements and prohibition on overbroad and general warrants.[2]

In *United States v. Sedaghaty*, 728 F.3d 885, 913 (9th Cir. 2013), the Ninth Circuit explained that "[i]t is the description in the search warrant, not the language of the affidavit, which determines the place to be searched." *Sedaghaty* was evaluating

[1] Docket citations refer to the docket entries in *Tippens*.

[2] In *Michaud*, at *9, this Court cited *Bergquist v. County of Cochise*, 806 F.2d 1364 (9th Cir. 1986), abrogated on other grounds, *City of Canton, Ohio v. Harris*, 489 U.S. 378 (1989), to support this statement. *Bergquist* was a § 1983 civil action in which the Court of Appeals addressed the scope of qualified immunity for police officers and claims of negligent supervision. It does not address the rules for construing a warrant for suppression purposes.

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

whether the items seized were particularly described in the warrant, rather than whether the location was properly described. However, the court explained that the particularity requirements apply equally to a description of the search location. *Id*. at 914.

The Ninth Circuit also stated that its approach to construing warrants is identical to that of the D.C. Circuit, which rejected the argument that "'the scope of the search warrant [can be] determined or broadened by the . . . supporting affidavit.'" *Id*., quoting *United States v. Kaye*, 432 F.2d 647, 649 (D.C. Cir. 1970). In *Kaye*, the police executed a warrant which authorized a search of "the premises known as 3618 14th Street N.W." *Id.* at 649. The D.C. Court of Appeals held that the search of an apartment one floor above the listed address was not authorized by this warrant and was therefore invalid. Most pertinently, the court rejected the Government's argument that the search was proper if the court construed the address in conjunction with a description of the premises found in the supporting affidavit. "It is the description in the search warrant, not the language of the affidavit, which determines the place to be searched." *Id.* at 649.

In this case, Magistrate Judge Buchanan had no particularized address information for the "activating computers," so it makes sense that she authorized searches of those computer wherever they were located *in her district*. The Government's claim that Judge Buchanan made the unprecedented leap from her district in Virginia to a worldwide warrant, based on two ambiguous words ("wherever located") buried in the unincorporated application is wrong. *See* Govt. Response at 53. For its argument is foreclosed by Ninth Circuit's bright line rules for construing warrants. It also violates the Fourth Amendment's requirement that a warrant "particularly describe[] the place to be searched," Rule 41's jurisdictional rules, and the Federal Magistrate Act's limits on Judge Buchanan's authority to issue a warrant.

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

The Government's failure to even discuss *United States v. SDI Future Health, Inc.*, 568 F.3d 684 (9th Cir. 2009), should be dispositive. There, the Ninth Circuit explained the two requirements for using an affidavit to expand a warrant: "We consider an affidavit to be part of a warrant, and therefore potentially curative of any defects, **only if** (1) the warrant expressly incorporated the affidavit by reference **and** (2) the affidavit either is attached physically to the warrant or at least accompanies the warrant while agents execute the search." *Id.* at 699 (emphasis added).

Here, there is no dispute that neither of those requirements are present. The clear import of *Sedaghaty* and *SDI Future Health* is that a specified search location—Eastern Virginia—cannot be expanded to the rest of the world by means of an unincorporated affidavit.

And the Government knows all this perfectly well. The Government falsely claims that judges have previously approved warrants like the Virginia warrant, when in fact every known case involving malware searches was based on warrants that clearly stated that they were executable outside the issuing district. *See* Govt. Response at 33-34 (citing the Colorado "texas.slayer@yahoo.com" and *Cottom* cases in Nebraska; *compare with* exh. A ("texas.slayer" warrant, authorizing searches in "Colorado *and elsewhere*"); exh. B (Nebraska NIT warrants authorizing searches in "Nebraska *and elsewhere.*") (emphasis added). Those warrants still violated the Federal Magistrate Act and Rule 41 (issues that were never raised or decided in those cases). But at least the Government did not mask its intentions, or claim that the Magistrate Judge had issued a worldwide warrant without making his or her intentions perfectly clear.

In short, all of the available facts indicate that Magistrate Judge Buchanan followed the law and the Fourth Amendment's particularity requirements by not specifying any locations outside her district; not incorporating the application; and not violating the jurisdictional limits of the Federal Magistrate Act and Rule 41. Given

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

these facts, the Court should reject the Government's efforts to now reverse engineer the warrant to its liking.

Finally, the violation of the geographical scope of the warrant is a constitutional violation that requires suppression. If the scope of the search exceeds that permitted by the warrant's express terms, the subsequent seizure is unconstitutional and nothing more need be shown to mandate suppression. *Horton v. California*, 496 U.S. 128, 140 (1990); *see also Sedaghaty*, 728 F.3d at 915 ("The government's seizure of items beyond the terms of the warrant violated the Fourth Amendment [and] the exclusionary rule generally bars admission of the evidence seized that was beyond the scope of the warrant").

B. The Virginia Warrant's Territorial Limit Was Not a Magistrate's Error.

The Government addresses the defects in its NIT search in part by shifting blame to Magistrate Judge Buchanan. For example, the Government quotes with approval the conclusion in *Werdene* that "to the extent a mistake was made in this case. . . . it was made by the magistrate when she mistakenly issued a warrant outside her jurisdiction." *See* Govt. Response at 47. Similarly, the Government argues that "[d]efendants' suggestion that the purported jurisdictional flaw should have been apparent at the start cannot be squared [with] the fact that its obviousness escaped…the issuing judge," as well as others. *See* Govt. Response at 48.

This is an odd argument for the Government to make, since it is the FBI's lack of candor about how it planned to execute the warrant anywhere in the world that created the problem. As the Ninth Circuit has stated, the Government has a "duty of candor in presenting a warrant application," and "a lack of candor in [any] aspect of the warrant application must bear heavily against the government in the calculus of any subsequent motion to return or suppress the seized data." *United States v. Comprehensive Drug*

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

Testing, Inc., 621 F.3d 1162, 1178 (9th Cir. 2010) (Kozinski, J., concurring) (hereinafter "*CDT*"). And, as Judge R. Brooke Jackson concluded in *Workman*, "In my view, had Magistrate Judge Buchanan understood that the NIT technology would search computers in other districts—rather than track information as it traveled from her district to others—she probably would not have issued the NIT Warrant given the limitations of the Rule." *United States v. Workman*, No. 15-cv-00397-RBJ-1, 2016 WL 5791209, at *5 (D. Colo. Sept. 6, 2016).

Moreover, the defendants maintain here that the warrant application's defects likely *were* understood by Magistrate Judge Buchanan; that is precisely why she did not issue a worldwide warrant as the Government now claims. *See* Defendants' Motions to Suppress (dkt. 35) at 23-25. In stark contrast to the warrants in earlier NIT cases, where the judges expressly approved searches outside their districts, the only clearly identified location in the instant warrant is the Eastern District of Virginia. While the warrant attachment references "activating computers," without more, the common sense and plain reading of this authorization is that Judge Buchanan approved searches of activating computer within her district, but not "elsewhere." *Compare* exhs. A and B.

In asking the Court to conclude otherwise, the Government is really asking the Court to find that Judge Buchanan acted incompetently, and that she rubber stamped a warrant that exceeded her authority. However, "[t]rial judges are presumed to know the law and to apply it in making their decisions." *Walton v. Arizona*, 497 U.S. 639, 653 (1990), *overruled on other grounds by Ring v. Arizona*, 536 U.S. 584 (2002); *Clark v. Arnold*, 769 F.3d 711, 727 (9th Cir. 2014) ("Nothing in the record here overcomes that presumption"). This is especially true where, as here, the only way to read the warrant the way the Government wants is to ignore the Ninth Circuit's rules of construction (as it did in its Response). The Government is also asking the Court to ignore the Ninth Circuit's admonishment, in response to previous governmental overreaching, that

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

judicial officers must exercise "greater vigilance" when issuing and reviewing data search warrants. *CDT*, 621 F3d at 1177.

In short, the Government is asking this Court to approve the most sweeping search and seizure operation in our nation's history based on one of two assumptions; either (a) Magistrate Judge Buchanan did not know what she was doing when she signed the NIT warrant, or (b) she chose to issue an unprecedented worldwide warrant even though she is presumed to know she could not do so under the Federal Magistrate Act and Rule 41.

There is a third option, however, and it is both the most reasonable one and the only one that is consistent with both the text of the warrant and the law. The Court should simply find that Magistrate Judge Buchanan knew and followed the law; authorized searches of all "activating computers" located in her district; and declined the FBI's invitation to issue the cyber equivalent of a general warrant by choosing not to amend the warrant or incorporate the warrant application. Those findings, if the Court makes them, lead to suppression.

C. The NIT Warrant, if Construed in the Way the Government Wants, Would Violate the Federal Magistrate Act.

The Government avoids a detailed discussion of the Federal Magistrate Act. Instead, it muddles together the issues arising from the Act with arguments about whether a "good faith" violation of Rule 41 requires suppression. *See* Govt. Response at 47-49. The Federal Magistrate Act and Rule 41 are separate hurdles for the Government. A violation of Rule 41 is not necessarily fundamental and does not necessarily require suppression if it involves a mere technicality, such as the timing of when the police serve a copy of their search warrant. *See United States v. Williamson*, 439 F.3d 1125 (9th Cir. 2006). A violation of the Federal Magistrate Act, however, is jurisdictional and it cannot be remedied.

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

In choosing to largely ignore the Act, the Government also ignores the precedents cited in the defendants' motion, including *United States v. Colacurcio*: "Federal magistrates are creatures of statute, and so is their jurisdiction. We cannot augment it; we cannot ask them to do something Congress has not authorized them to do." 84 F.3d 326, 328 (9th Cir. 1996) (citation omitted).

Consistent with this holding, the Supreme Court has always construed the Magistrate Act narrowly. Magistrate Judges are not Article III judges and the legislative history establishing that their powers had been carefully circumscribed "in the interests of policy as well as constitutional constraints." *Gomez v. United States*, 490 U.S. 858, 872 (1989) (reversing the convictions of two defendants when a Magistrate Judge exceeded his authority by selecting a jury); *see also, Mathews v. Weber*, 423 U.S. 261, 270 (1976) (Congress limited the Magistrates' role in Medicare cases referred to them); *United States v. Raddatz*, 447 U.S. 667, 676 (1980) (only where Congressional intent is "unmistakable" can Magistrate Judges make pretrial determinations.)

For reasons that are unclear, most of the courts that have reviewed the NIT searches have focused entirely on the Rule 41 issues, not the Federal Magistrate Act or (as discussed above) the limited geographic scope of the warrant. In the majority of cases where defendants have raised the Federal Magistrate Act issue, the courts have held not only that the Act was violated, but that the violation required suppression. *See United States v. Levin*, 2016 WL 2596010 (D. Mass. May 5, 2016); *United States v. Arterbury*, 2016 U.S. Dist. LEXIS 67091 (N.D. OK. May17, 2016); *United States v. Workman*, 2016 U.S. Dist. LEXIS 133782 (D. CO. Sept. 6, 2016); and *United States v Croghan*, 2016 WL 4992105 (S.D. Iowa Sept. 19, 2016); *but see, United States v. Broy*, 2016 U.S. Dist. LEXIS 128616 (C.D. Ill. Sept. 21, 2016) (doing a combined analysis of the Act and Rule 41and finding that they were violated, but not ordering suppression).

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

Moreover, in a sixth recent case involving similar overreaching by the Government, a district court suppressed the fruit of a Maryland search warrant that a Magistrate Judge had issued for Google email records in California. *United States v. Barber*, ___F. Supp.3d ____, 2016 WL 1660534 (D. Kansas, April 27, 2016). The court held that the issuing judge had no authority to issue the warrant; that the warrant was therefore "void" at its inception; and that suppression was required because the seizure of the Google records was an unconstitutional warrantless search:

> Courts have found that warrants issued without jurisdiction are void from their inception. See, e.g., *United States v. Baker*, 894 F.2d 1144, 1147–48 (10th Cir. 1990). A warrant that is void from its inception is no warrant at all. See *United States v. Krueger*, 809 F.3d 1109, 1124–25 (10th Cir. 2015) (Gorsuch, J., concurring); *see also Groh v. Ramirez*, 540 U.S. 551, 559, 124 S. Ct. 1284, 157 L.Ed.2d 1068 (2004) ("[T]he warrant was so obviously deficient that we must regard the search as 'warrantless' within the meaning of our case law."). Using this logic, the search of defendant's email account was the equivalent of a warrantless search.

Id. at *4.

It should be noted that the Government has moved to dismiss its appeal in *Barber*. The Government is also delaying or avoiding appellate review of adverse Operation Pacifier decisions. It has obtained three continuances of the briefing deadlines for *Levin* and *Arterbury*, and in both cases the Courts of Appeal have issued orders denying any further extensions. The Government has also obtained a continuance of the briefing deadline in *Michaud*, with its opening brief now due on October 24. This avoidance of timely review suggests that the Government lacks confidence in the ultimate merits of its arguments.[3]

This Court has not previously ruled on whether a warrant issued in violation of the Federal Magistrate Act is "void" and, as a result, the good faith exception is

[3] The *Workman* and *Croghan* decisions are so recent that it remains to be seen if the Government will seek delays in those cases as well.

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

inapplicable to a search conducted pursuant to that warrant. The defendants therefore urge the Court to adopt the reasoning and conclusions of the sister courts that have ruled on the Magistrate Act violation, both because that reasoning is sound and because the Government has made no meaningful attempt to argue otherwise. If, as the Government insists, Magistrate Judge Buchanan approved a warrant that could be executed anywhere, then there is no escaping the fact that she had no statutory or constitutional authority for such an unprecedented warrant, making it *void ab initio*.

D. This Court Correctly Ruled That the Warrant Violated Rule 41, and Accordingly it Should Grant Suppression.

1. The Prejudice to the Defendants.

The Court previously found in *Michaud* that construing the warrant in any of the ways that the Government proposes would violate Rule 41, and there is no need to revisit the related arguments in detail. With some exceptions employing dubious reasoning, most of the district courts that have reviewed the NIT warrant are in agreement that the warrant, as construed by the Government, violates Rule 41.

These cases are still "all over the map," as this Court has observed, primarily because there is a split among the circuits about when suppression is required for a Rule 41 violation and because many courts have misapplied the good faith exception. In the Ninth Circuit the rule is that suppression is the appropriate remedy for a rule violation when it is prejudicial, deliberate or of constitutional magnitude. While the Court concluded in *Michaud* that suppression was not required for the violation, the defendants respectfully submit that this ruling is contrary to the controlling authority in this circuit.

In *Michaud*, this Court said that, under the defendant's interpretation of what the Ninth Circuit deems prejudice, "defendants suffer prejudice whenever a search occurs that violates Rule 41(b)." 2016 WL 337263 at *20. With respect, that is not correct.

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

Prejudice occurs, and suppression should follow, if a search violates the Rule and the search could not have occurred without that violation having happened. If the Rule is violated only because of some technicality (such as not serving a copy of the warrant in a timely manner), then the officers could have complied with the rule and still obtained the warrant. Here, if the rule had been heeded, there would have been no search of the defendants' computers at all, particularly in view of the narrow two week window of the warrant.

Applying the same Rule 41 standards that the Ninth Circuit prescribes, the court in *United States v. Croghan* analyzed the prejudice issues as follows:

> It is clear in this case that neither the search pursuant to the NIT Warrant nor the searches pursuant to the Iowa Warrants would have occurred without the violation of Rule 41(b). Had Rule 41 been complied with, law enforcement would not have obtained Defendants' IP addresses, would not have been able to link those IP addresses to Defendants through subsequent investigation and the use of administrative subpoenas, and would not have had sufficient probable cause to obtain the Iowa Warrants. Thus, Defendants have satisfied their burden to prove that they were prejudiced by the Rule 41(b) violation.

2016 WL 4992105 at *8.

Likewise, in the Tenth Circuit, the court held in *United States v. Aterbury* that the searches of the defendant's computers would not have occurred had Rule 41(b) been followed: "The Tenth Circuit's definition of 'prejudice" – i.e., 'prejudice in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed' – is similar to the Ninth Circuit definition." Dkt. 61-1, exh. A-1 at *22. Also consistent with Ninth Circuit standards, the judge granted suppression.

These opinions make sense because if the NIT searches had been properly confined to the Eastern District of Virginia, the defendants' computers would never have been searched. The defendants therefore respectfully submit that, given the facts of this case, the prejudice analysis is irrefutable. *See also Workman*, 2016 U.S. Dist.

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

LEXIS 133782 at *10 ("The Court finds that Mr. Workman has established prejudice because the search of his computer would not have occurred had Rule 41(b)(1) been followed.").

By contrast, all of the cases that the Government relies on involved mere technicalities. These are violations which, even if they had not occurred, would not have prevented the occurrence of the searches themselves. For example, in *United States v. Vasser*, 948 F.2d 507 (9th Cir. 1980), the police used a tape recorded warrant application, rather than a written or telephonic one as specified in Rule 41. *See* Govt. Response at 42. Regardless of whether the police had followed the rule, the search could have proceeded anyway, because the error did not relate to the propriety of the search itself—they would simply have used the right application method. Here, by contrast, if the FBI had respected Rule 41, the defendants' computers would not have been searched at all.

The Government also baldly misstates the holding in *United States v. Goff*, 681 F.2d 1238 (9th Cir. 1982), to argue that a "violation of Rule 41's geographical restrictions" does not require suppression. Govt. Response at 49. In *Goff*, a DEA agent obtained a search warrant from a judge in Seattle while he was following drug trafficking suspects on a flight from Miami. Upon arrival in Seattle, the police executed a search at the airport and recovered cocaine. The defendants argued that the warrant had violated Rule 41 because it had been issued before the drugs had arrived in the district where the warrant had been issued. But this argument was patently meritless, because the Rule only required that the search take place in the district where the warrant was issued, and there was no dispute that had happened. 681 F.2d at 1240.

In our cases, by contrast, this Court has already held that the different jurisdictional limits prescribed by the Rule were violated. Neither in *Goff* nor elsewhere

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

has the Ninth Circuit ever held, or even suggested, that a search which violates Rule 41's jurisdictional requirements can be considered "technical."

The Government further errs when it relies on *United States v. New York Telephone Co.*, 434 U.S. 159 (1977), a 40 year old case. In *New York Telephone*, the Court used the plain text of Rule 41 and the rules of statutory construction to hold that district judges have the power to order pen registers. The Court focused on Rule 41's definition of the term "property"; found that it was an illustrative rather than exhaustive list of what qualified as property; and unsurprisingly concluded that it could include information collected by a pen register. *Id.* at 169. Hence, contrary to the Government's claim that *New York Telephone* allows for whatever "flexible" construction of Rule 41 suits its purposes, the case applies rules of statutory construction to find that *particular portion of the rule* to be "flexible" because it included an illustrative list. The same rules of construction foreclose the Government's arguments here, where the relevant provisions are limited and exclusive.

2. The NIT is Plainly Not a Tracking Device.

The Government's related argument, based on four district courts that have held that the NIT is sort of like a "tracking device," is also misguided. *See* Govt. Response at 30-31; *see also Michaud*, 2016 WL 337263 at *5 (rejecting tracking device argument). Rule 41(b)(2) only permits "a warrant for a person or property outside the district if ***the person or property is located within the district when the warrant is issued*** but might move or be moved outside the district before the warrant is executed") (emphasis added).

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

Three of the four cases cited by the Government were decided in Virginia, where the NIT warrant was issued, so the tracking device provision might apply there. It has no application to computers in Washington.[4]

In the fourth case, *United States v. Jean*, 2016 WL 4771096 (W.D. Ark. Sept. 13, 2016), the court found that the NIT Warrant "did not violate Rule 41(b)(4)'s jurisdictional boundaries, because law enforcement did not leave the Eastern District of Virginia to attach the tracking device." 2016 WL 4771096, at *16. This conclusion is plainly erroneous because even the Government has conceded that the NITs were planted in target computers in the myriad places where those computers were located, not in the district where the warrant was issued (apart from Eastern Virginia computers). Hence, this Court (and every other court) has ruled that the searches occurred where target computers were located.

Likewise, *United States v. Koyomejian*, 970 F.2d 536 (9th Cir. 1992), has nothing to do with the issues in these cases. *See* Govt. Response at 28. In *Koyomejian*, a judge in the Central District of California issued a warrant authorizing video surveillance of a target inside the district. The defendant challenged the surveillance on the ground that it was prohibited by the Foreign Intelligence Surveillance Act and other statutes, and did not even claim that the Government had violated Rule 41. *Id*. at 538. The court merely noted in passing that Rule 41 authorizes courts to issue video surveillance warrants. *Id*. at 542. No doubt it does, when the authorization is for surveillance of property in the issuing court's district; the warrant particularly and accurately describes the location of the surveillance; and that surveillance does not extend to tens of thousands of targets around the world. The opposite happened here.

[4] *See United States v. Darby*, 2016 WL 3189703, at *12; *United States v. Eure*, 2016 WL 4059663, at *8; *United States v. Matish*, 2016 WL 3545776, at *17-18.

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

3. There Were No Exigent Circumstances.

The Government fares no better when it claims exigency to avoid suppression. Govt. Response at 51-53. The exigency exception is quite 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).

Here, the harm was so far from imminent that the FBI chose to maintain the status quo and continue distributing pornography. The FBI was also not concerned with the imminent destruction of evanescent evidence; it instead deployed the NIT to seek out and collect stored data. The court in *Arterbury*, 2016 U.S. Dist. LEXIS 67091 at *35, shot down the exigent circumstances argument with this succinct observation: "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."

4. The Rule Violation was of Constitutional Magnitude.

Suppression is also required if a violation of Rule 41 is of "constitutional magnitude." *United States v. Weiland*, 420 F.3d 1062, 1071 (9th Cir. 2005). While "constitutional magnitude" is nowhere defined, it is safe to say that if this case does not involve a violation of "constitutional magnitude," it is hard imagine one that does.

As a result of the rule violation, the FBI obtained an unprecedented worldwide warrant, targeting the homes and computers of as many as 100,000 people, thereby turning a single warrant into the modern cyber equivalent of the general warrants that were anathema to the Founders. And, as *The Seattle Times* recently reported,

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

"Operation Pacifier" and the issues surrounding the NIT warrant have put Internet privacy in the "crossfire."[5] The Government therefore displays remarkable chutzpah when it blithely assures the Court that any "error, defect or irregularity" in the NIT warrant did not affect substantial rights. Govt. Response at 43.

5. The Violation was Deliberate.

As the district court observed in *Croghan*, suppression is appropriate (and the good faith exception is inapplicable) to the NIT searches because "law enforcement was sufficiently experienced, and that there existed adequate case law casting doubt on magisterial authority to issue precisely this type of NIT Warrant, that the good faith exception is inapplicable." 2016 WL 4992105 at *8.

More than that, DOJ's own guidelines instruct agents that they cannot properly obtain multi-jurisdictional warrants, let alone a worldwide warrant targeting tens of thousands of computers. *See* Defendants' Motions to Suppress at 22. While the Government tries to minimize the import of these guidelines by pointing to decisions upholding the NIT searches (*see* Govt. Response at 36), this deflection misses the point: Whatever disputes about the jurisdictional limits of the Federal Magistrate Act and Rule 41 that have emerged from Operation Pacifier (which will ultimately be resolved on appeal), the Government's *own view of the law* at the time it obtained the NIT warrant is the same as that of the defendants and the majority of courts that have found that the warrant was not properly issued. *See* Defendants' Motions to Suppress at 21-22. 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 officers are themselves ultimately responsible for the defects

[5] *See* Mike Carter, *FBI's Massive Porn Sting Puts Internet Privacy in Crossfire*, The Seattle Times (August 27, 2016) ("The investigation has sparked a growing social and legal controversy over the FBI's tactics and the impact on internet privacy."). Available at: http://www.seattletimes.com/seattle-news/crime/fbis-massive-porn-sting-puts-internet-privacy-in-crossfire/

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

in the warrant." *United States v. Reilly*, 76 F.3d 1271, 1281 (2d Cir. 1996). And more than just the officers involved in this case were responsible for the defects. On October 14, during cross-examination at a hearing in Boston, Agent Alfin finally confirmed that the NIT warrant was debated and approved at the highest levels of DOJ and the FBI.

The Government is hard pressed to explain how on one hand DOJ can be advising its agents that multi-district warrant are not valid and be lobbying for changes to Rule 41 to eliminate its explicit restrictions and, at the same time, approve submission of the NIT warrant application. Contrary to the Government's suggestion that its own search and seizure guidelines are out of date (*see* Govt. Response at 41), they remain in effect and they have not been changed because Rule 41 has not changed. Plainly, there would be no need for DOJ to seek changes to Rule 41 now if it believed that the rule already allowed for worldwide warrants. And even if Congress does allow changes to Rule 41, there are no pending changes to the Federal Magistrate Act.

The bottom line is that Government is not free to ignore existing law, no matter how much it disagrees with it. This is especially true given that the Government's repeated claim that it will be unable to identify targets on the Tor network without circumventing Rule 41 is not credible. Traditionally, law enforcement has engaged in such legitimate tactics as taking part 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, 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] The FBI is also now identifying targets on the Tor network by means of controlling or

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

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

gaining access to network nodes or "relays." *See* Bruce Schneir, *Attacking Tor: How the NSA Targets Users' Online Anonymity*, *The Guardian*, Oct. 4, 2013 (reporting on NSA and law enforcement methods for identifying Tor users by intercepting and redirecting illicit network traffic).[7]

Upholding the Fourth Amendment, and the laws and rules that implement its guarantees, inevitably comes with some crime-fighting costs. But requiring the Government to follow the law in these case will by no means leave it helpless to fight crime on the Tor network.

Finally, in arguing against finding a deliberate violation, the Government miscites *United States v. Luk*, 859 F.2d 667 (9th Cir. 1987), to argue that suppression is required only if agents acted in "bad faith." Govt. Response at 39. The Rule 41 violation in *Luk* involved a warrant that had been innocently requested by an investigator for the Department of Commerce, who did not technically qualify as a "federal law enforcement officer." The defendant claimed that this violation was deliberate, and did not claim that it was prejudicial or of constitutional magnitude. The Court simply found no evidence that the violation was deliberate, hence no suppression. *Id*. at 673.

Nevertheless, the Government misleadingly quotes *Luk* for the proposition that suppression is an appropriate remedy only when a violation "rises to the level of bad faith." Govt. Response at 39. In actuality, the court stated that it had not found "any indication of 'bad faith' ***or*** 'deliberate disregard' of Rule 41" by either the agent who submitted the application or the prosecutor who had approved it. *Id.* at 674 (emphasis added). *Luk* therefore does not stand for the proposition that a court must find "bad faith" in addition to a deliberate disregard for the Rule. The court simply found that

[7] Available at: https://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

there had been "absolutely no attempt to avoid compliance with any of Rule 41's requirements[.]" *Id.*, at 674.

The same cannot be said in these cases. Further, the Government's contention that the agents and prosecutors who prepared and submitted the NIT warrant were not aware of Rule 41's requirements underscores the need for discovery of the records related to the FBI's and DOJ's review and approval of the warrant. *See* Defendants' Motion to Compel Discovery (dkt. 100) at 2.

E. The Defendants' Had a Core Expectation of Privacy in Their Computers and Their Homes.

In *Michaud* this Court ruled that the defendant did not have a reasonable expectation of privacy in his IP address. The Government harps on this by arguing that the "individual privacy interests here were also extremely limited. . . ." Govt. Response at 38. This is a red herring, because the Government ignores the Supreme Court authority establishing a person's privacy interest in both their computer data and, more fundamentally, his or her home. *See* Defendants' Motions to Suppress at 18-20. It also ignores the private, non-IP data that was seized, including "MAC" addresses.

The Government does not dispute that the NIT searches "trespassed" upon all three of the defendants' homes and personal computers, nor could it. This intrusion is dispositive of the Government's efforts to minimize the privacy interests at stake in this case. *See United States v. Jones*, 132 S. Ct. 945, 950 (2012).

In regard to computers in particular, the Ninth Circuit has explained that "electronic storage devices such as laptops 'contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails," and [we have] held that '[t]hese records are expected to be kept private and this expectation is one that society is prepared to recognize as reasonable.'" *Grand Jury Subpoena v. Kitzhaber*, 828 F.3d 1083, 1090 (9th Cir. 2016) (citations omitted). "The

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

Supreme Court, too, has emphasized recently the ability of digital troves to contain '[t]he sum of an individual's private life,' and the corresponding need for our jurisprudence to reflect the changing technological landscape." *Id*., citing *Riley v. California*, 134 S. Ct. 2473, 2489 (2014).

A common sense approach to the privacy issue was perhaps best expressed by the Honorable Robert Pratt in Iowa:

> If a defendant writes his IP address on a piece of paper and places it in a drawer in his home, there would be no question that law enforcement would need a warrant to access that piece of paper—even accepting that the defendant had no reasonable expectation of privacy in the IP address itself.

Croghan, 2016 WL 4992105 at *7.

In light of the relevant Supreme Court authority, and the Government's failure to address or distinguish that authority, this Court should conclude that the FBI's actions encroached on the defendants' core privacy interests in their homes and computers.

F. The Warrant Application Did Not Establish Probable Cause.

The NIT warrant application sought authorization to search the computers of anyone who landed on Playpen's home page. Consequently, under *United States v. Gourde*, 440 F.3d 1065 (9th Cir. 2006), it is the perception of the average person, and what he or she would likely have concluded when looking at the home page, that is the crux of establishing probable cause.

As a threshold matter, the Government appears to concede that content of the home page, apart from the pictures posted on it, is irrelevant. Although the warrant application recited at length various notices and technical terms that were on the home page, the Government acknowledges that none of these would have been significant "to the untrained eye." Govt. Response at 19.

The Government goes on to fairly summarize the holding in *Gourde*, but then fails to apply it to the facts here. In *Gourde*, the first key fact was that the site at issue

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

"unabashedly announced" that it contained child pornography, in various blatant ways. This is starkly different from how the FBI ran the Playpen site, with a home page devoid of child pornography or any references to "lolitas," minors, or similar red flags.

In addition, probable cause in *Gourde* did not just rest on the appearance of the website. Going even further, the Ninth Circuit concluded that "someone who paid for access for two months to a website that actually purveyed child pornography probably had viewed or downloaded such images onto his computer." *Id.* at 1071. It was this continuing membership, establishing that Gourde's contact with the site was not accidental or fleeting, that was equally important to finding probable cause.

In sharp contrast here, the FBI did not require payment or membership to access Playpen, and the FBI deployed its NITs **before** the targets had browsed the site or could see what it contained. *See generally* Kevin Poulsen, *Visit the Wrong Website, and The FBI Could End Up in Your Computer*, Wired.com, August 5, 2014 (although targeted use of "malware" by the FBI is not new, "[w]hat's changed is the way the FBI uses its malware capability, deploying it as a driftnet instead of a fishing line").[8]

The Government not only fails to distinguish *Gourde*, but it offers a string of citations from other circuits that track the Ninth Circuit's standard for determining probable cause based on visits to a website. *See* Govt. Response at 20-21, citing, *inter alia*, *United States v. Shields*, 458 F.2d 269 (3rd Cir. 2006); *United States v. Martin*, 426 F.3d 68, 75 (2d Cir. 2005). All of these cases stem from the investigation of a site called "Candyman," which unabashedly announced its illegal purpose to anyone who stumbled upon it, and all of the defendants had prolonged memberships on the site.

Significantly, in another case cited by the Government, *United States v. Falso*, 544 F.3d 110 (2d Cir. 2008), the Second Circuit found no probable cause when the

[8] Available at: http://www.wired.com/2014/08/operation_torpedo/

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

warrant application failed to alleged that the defendant had actually entered the site. *See* Govt. Response at 21. Moreover, "[e]ven if one assumes (or infers) that Falso accessed the cpfreedom.com site, there is no specific allegation that Falso accessed, viewed or downloaded child pornography." 544 F.3d at 121. Here, the warrant authorized the FBI to execute NIT searches when visitors were just on the home page, a patently insufficient tripwire for allowing the FBI to search thousands of computers.

G. The Undisputed Facts and Government Concessions Establish the Need for a *Franks* Hearing.

The probable cause issues in this case are intertwined with the *Franks* issues that the defendants have raised, particularly the FBI's false description of Playpen's home page. To obtain a *Franks* hearing, a defendant need only make a substantial showing of a reckless failure to verify material information. *United States v. Chesher*, 678 F.2d 1353, 1362 (9th Cir. 1982). The undisputed facts establish much more than that.

First, the Government does not dispute that the description of the home page in the NIT application was inaccurate in at least one critical respect: the Government claimed that the page displayed child pornography, when in fact it did not.

Second, the Government does not dispute that, by including a detailed description of the home page in the first place, the FBI knew that the appearance and content of the home page was important. Indeed, Agent Alfin conceded during his testimony in *United States v. Jean* that, "importantly," the logo described in the warrant application was different from the way it actually appeared. Defendants' Motions to Suppress, exh. K at 34. Without that description, all that remains is the fact that thousands of unknown targets were using the Tor network to visit Playpen and some notices on the home page that the Government concedes were not significant. Govt. Response at 19.

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

Third, the Government does not dispute that Playpen's home page, as it actually appeared at the time of the NIT searches, was tamer than many mainstream websites. *See* dkt. 37-9 and 37-10 (Motions to Suppress exhs. I and J).

Fourth, the Government does not dispute that Agent Alfin had actual knowledge of the changes to the site.

Fifth, the Government does not dispute that, regardless of what Agent Alfin reported to other agents, the "fellow officer" rule renders everyone involved with "Operation Pacifier" accountable for the omissions and misrepresentations. *See* Motions to Suppress at 34. Moreover, while repeatedly touting the experience of Agent Alfin and others who were involved in the operation, the Government makes no effort to explain how such experienced agents would not have known that they needed to verify the appearance of Playpen in a timely manner and describe it accurately.

In regard to this last point in particular, the Ninth Circuit has stated that "[a]n affidavit in support of a search warrant "must speak as of the time of the issue of that warrant." *Chesher*, 678 F.2d at 1362 (failure of agent to discover report showing that defendant was no longer with Hell's Angels, contrary to affidavit, was sufficient showing of intentional or reckless falsity to warrant *Franks* hearing). And, when it comes to uncorrected information of even arguable materiality to a finding of probable cause, "silence is as troubling as it is unjustifiable." *United States v. Meling*, 47 F.3d 1546, 1554 (9th Cir. 1995) (ultimately holding that the information at issue was not material); *see also United States v. Garcia-Zambrano*, 530 F.3d 1249, 1257-58 (10th Cir.2008) (district court's finding that statements were recklessly included was based, *inter alia*, on fact that officers failed to verify information before submitting affidavit).

A *Franks* hearing is also appropriate because the Government has invoked the good faith exception to the exclusionary rule. *See, e.g.*, Govt. Response at 45 (maintaining that it was reasonable for the FBI to rely on the NIT warrant because the

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

judge signed it "after having been made aware of how the NIT would be implemented and its reach," claims which the defense vigorously disputes). A claim of "good faith" is foreclosed if the Court finds that the NIT warrant application included intentionally or recklessly false material statements or omissions. *Mills v. Graves*, 930 F.2d 729, 733 (9th Cir. 1991) (citing *Leon*, 468 U.S. at 914).

H. The Good Faith Exception Does Not Apply Here.

As discussed above, the good faith exception cannot salvage a jurisdictional violation of the Federal Magistrate Act; prejudicial, deliberate or constitutionally significant Rule 41 violations; or searches predicated on a *Franks* violation. More broadly, the Government suggests that because the FBI was investigating the distribution of child pornography, it meant well, and therefore it acted in good faith. If generic crime fighting intentions were enough to establish good faith, the Government could claim them in every case to avoid suppression. Not surprisingly, both the Supreme Court and Ninth Circuit have a much narrower view of when the Government can legitimately invoke the good faith exception.

To begin, the subjective intentions of the agents or prosecutors who are involved in a search are irrelevant when determining whether the exception applies. *United States v. Song Ja Cha*, 597 F.3d 995, 1005 (9th Cir. 2010) ("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 the law and to conform their conduct to these rules. *Hudson v. Michigan*, 547 U.S. 586, 599 (2006). Here, we know that the FBI not only did not conform its conduct to the rules, but acted in defiance of DOJ's own search and seizure guidelines.

Granting suppression in these cases would have exactly the type of deterrent effect that the exclusionary rule is intended to impart. The Supreme Court has made

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

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). Here, as the court in *Croghan* explained, "Suppression is an appropriate means to deter law enforcement from seeking warrants from judges lacking jurisdiction to issue them, and this deterrence function outweighs the societal costs associated with suppression." 2016 WL 4992105 at *8.

These cases also do not come before the Court in isolation. Instead, they are part of an emerging pattern of overreaching when it comes to computer and "cyber" searches. This pattern includes the Government's "deliberate overreaching" in *CDT*, 621 F.3d at 1172; the FBI's efforts to conceal its use of "Stingray" cell phone trackers and their capabilities;[9] and illegal DEA wiretapping.[10] If the courts do not exercise diligent oversight over the Government's constantly expanding and evolving use of search and surveillance "techniques," and suppress evidence when appropriate, then it is hard to see who else will stand between the average citizen and the Government's exercise of law enforcement powers in increasingly Orwellian ways.

---

[9] *See* Adam Lynn, *Tacoma Police Change How They Seek Permission to Use Cellphone Tracker*, The News Tribune, November 15, 2014 ("Pierce County judges didn't know until recently that they'd been authorizing Tacoma police to use a device capable of tracking someone's cellphone" because, following an agreement with the FBI not to disclose the surveillance technology, police concealed its use of the technology in numerous cases). Available at: http://www.thenewstribune.com/news/local/crime/article25894096.html

[10] Brad Heath, *Justice Officials Fear Nation's Biggest Wiretap Operation May Not be Legal*, *USA Today*, November 11, 2015 (reporting on "a massive wiretapping operation" by DEA agents that DOJ lawyers have determined may not be legal, but the DEA nevertheless continues to operate) (Available at: http://www.usatoday.com/story/news/2015/11/11/dea-wiretap-operation-riverside-california/75484076/); Greg Miller, *Misinformation on Classified NSA Programs Includes Statements by Senior U.S. Officials*, The Washington Post, June 30, 2013 (reporting on false testimony before Congress by government officials about surveillance measures) (Available at: https://www.washingtonpost.com/world/national-security/misinformation-on-classified-nsa-programs-includes-statements-by-senior-us-officials/2013/06/30/7b5103a2-e028-11e2-b2d4-ea6d8f477a01_story.html).

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

II. CONCLUSION

For the reasons stated above, the Court should grant the defendants' Motions for a *Franks* hearing and/or Suppression.

DATED this 17th day of October, 2016.

Respectfully submitted,

s/ *Colin Fieman*
Colin Fieman
Attorney for David Tippens

s/ Robert Goldsmith
Robert Goldsmith
Attorney for Gerald Lesan

s/ Mohammad Hamoudi
Mohammad Hamoudi
Attorney for Bruce Lorente

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

CERTIFICATE OF SERVICE

I hereby certify that on October 17, 2016, I electronically filed the foregoing 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.

s/ *Amy Strickling, Paralegal*
Federal Public Defender Office

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

AO 93 (Rev. 12/09) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

District of Colorado

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Network Investigative Technique ("NIT") for email address texas.slayer@yahoo.com	)	Case No. 12-sw-5685-KMT

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the State and District of Colorado and elsewhere *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

See Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before October 24, 2012
(not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10 p.m. ☑ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge Kathleen M. Tafoya.
(name)

☑ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 and 3103(a) (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☒ for 30 days *(not to exceed 30)*.
☑ until, the facts justifying, the later specific date of _____.

Date and time issued: Oct 09, 2012 4:14 pm

Judge's signature

City and state: Denver, Colorado

Kathleen M. Tafoya
United States Magistrate Judge
Printed name and title

Exhibit A-1

AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

Return		
Case No.:	*Date and time warrant executed:*	*Copy of warrant and inventory left with:*
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

Exhibit A-2

Attachment A

Place to Be Searched

The portion of the computer activating the network investigative technique ("NIT") that may assist in identifying the computer, its location, other information about the computer, and the user of the computer.

Exhibit A-3

Attachment B

Things To Be Seized

Information that may assist in identifying the computer, its location, other information about the computer, and the user of the computer, all of which is evidence of violations of Section 1038 of Title 18, United States Code (False information and hoaxes). This information may include environmental variables and/or certain registry-type information, such as:

A. The computer's IP address. An IP Address is a unique numeric address used to direct information over the Internet and is written as a series of four numbers, each in the range 0 – 255, separated by periods (e.g., 121.56.97.178). Conceptually, IP addresses are similar to telephone numbers in that they are used to identify computers that send and receive information over the Internet.

B. The computer's MAC address. Each time a computer communicates over a local area network (or "LAN"), it uses a hardware device called a network interface card. Manufacturers of network interface cards assign each one a unique numeric identifier called a media access control or "MAC address."

C. The computer's open communication ports. A communication port number is information that helps computers to associate a communication with a particular program or software process running on a computer efficiently. For example, if a communication is sent to port 80, the receiving computer will generally associate it with world wide web traffic and send it to the web server, which can then send back a web page to the requesting computer.

D. A list of programs running on the computer.

Exhibit A-4

AO 93 (Rev. 12/09) Search and Seizure Warrant

SEALED

UNITED STATES DISTRICT COURT

COPY

for the

District of Nebraska

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
computers that access the website "Hidden Service B" located at s7cgvirt5wvojli5.onion

Case No. 8:12MJ359

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of Nebraska and elsewhere
(identify the person or describe the property to be searched and give its location):

See Attachment A, incorporated herein.

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before December 1, 2012
(not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10 p.m. ☑ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge F.A. Gossett
(name)

☑ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☑ for 30 days *(not to exceed 30)*.

☐ until, the facts justifying, the later specific date of _____

Date and time issued: 11/12/12 4:23 PM

Judge's signature

City and state: Omaha NE

F.A. Gossett U.S. Mag Jud
Printed name and title

233

Exhibit B-1