reflect

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

2Àµ’€4$Ó€

[] information." Id. Accord, United States v. Gomez, 807 F. Supp. 2d 1134, 1138 (S.D. Fla. 2011) (describing an iPhone as "maintaining sophisticated computer-like data storage capabilities").

As a result, regardless of whether the cell phone contains data within the scope of the search warrant, it may well contain a huge quantity of data outside the scope of the search warrant, revealing the most intimate aspects of Mr. Navarro's private and lawful life. The Government is entitled to everything within the scope of a valid search warrant; however, it is not entitled to any of the latter category. Thus, the search of the cell phone in this case presents the issue of intermingled data, a problem occurring with increasing frequency in this era of searches of computers and computer-like devices.

The Ninth Circuit spoke to problem of intermingled data in United States v. Tamura, 694 F.2d 591 (9th Cir.1982); it again focused on that problem, this time in the context of electronic data, in United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162 (9th Cir. 2010) (en banc). The CDT began by discussing the problem faced by law enforcement:

There is no way to be sur[illegible]

E. The search warrant Does Not Contain Adequate Protections Consistent with CDT's Admonitions.

The Government may contend that the search warrant in fact adequately protects Mr. Navarro's privacy interests, i.e. that it ensures that the Government will examine only material within the scope of the warrant. Although the search warrant application contains language that appears to provide such assurances, those assurances are illusory.

For example, the affidavit "anticipates the use of a hash value library to exclude normal operating system files that do not need to be searched[.]" Affidavit at 8. Even putting aside the non-committal nature of the word "anticipates," the issue is far less the Government's review of operating system files than of documents, email, diaries, and similar personal items, if they are outside the scope of the warrant.

Similarly, the affidavit "anticipates the use of hash values and known file filters to assist the digital forensics examiners/agents in identifying known and/or suspected child pornography image files. Use of these tools will allow for the quick identification of evidentiary files but also assist in the filtering of normal system files that would

to view their precise contents and determine whether the data fall within the list of items to be seized pursuant to the warrant." Id. In other words, the affidavit provides for exactly what the CDT opinion (and not just the concurrence) condemns: "Let's take everything back to the lab, have a good look around and see what we might stumble upon." Id. at 1171. The affidavit expressly envisions that all of the intermingled data may be examined by law enforcement, regardless of whether it comes within the scope of the warrant. This Court should not issue an order that assists the Government in viewing evidence outside the scope of the warrant.

F. It is Appropriate for this Court to Ensure that the Government's Search Properly Balances Mr. Navarro's Interests and the Government's, Notwithstanding the Existing Search Warrant.

The Government may argue that because the magistrate has issued the search warrant for the cell phone, this Court is restricted to simply approving the order to Apple to implement the dictates of the search warrant. In other words, the Government may argue, this Court should not address any of the CDT court's concerns – either the magistrate addressed them adequately, or it did not, but that is none of this Court's business. Should the Government make such an argument, it would be wrong.

"The All Writs Act invests a court with a power [that is] essentially equitable . . ." Clinton v. Goldsmith, 526 U.S. 529, 530 (1999). The Government is asking this Court to use its equitable power to require a third party to assist the Government in an endeavor. Even if that endeavor has already been approved by a magistrate, this Court should insist that, if its equitable powers are being called upon, those powers be used to properly balance the Government's legitimate law enforcement interests and Mr. Navarro's legitimate privacy interests.

As discussed in Mr. Navarro's Memorandum in Opposition to ex Parte Proceeding (Dkt. 34), his remedies to challenge the search warrant after the fact are limited. They would never actually remedy any violation of his privacy interests but would at most

FEDERAL PUBLIC DEFENDER
1331 Broadway, Ste 400
Tacoma, Washington 98402
(253) 593-6710

"may consider such protocols or a variation on those protocols as appropriate in electronic searches." Id. at *8. It then observed:

> Ultimately, the proper balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures of electronic data must be determined on a case-by-case basis. The more scrupulous law enforcement agents and judicial officers are in applying for and issuing warrants, the less likely it is that those warrants will end up being scrutinized by the court of appeals.

Id.

The Schesso court noted that the specific protocols discussed in the CDT concurrence were not constitutional requirements. That is irrelevant for the issue posed here - how can this son

1
2
3
4
5
6
7
8
9
10
11

iPhone 5 at issue in this case.[1] Apple, not Defendant, is the party with standing to challenge the order. It is also undisputed that Apple has reviewed the proposed order presented to this Court, and has indicated that, upon receipt of a signed copy of the order, it will comply with the order by unlocking the iPhone 5. There is simply no evidence whatsoever that Apple is requesting any further notice or opportunity to be heard prior to the entry of an order. In fact, there is no evidence at all that Apple is unwilling to comply with the Court's order; to the contrary, Apple has indicated its willingness to assist upon receipt of such an order. Defendant cannot insert himself into these proceedings to make any arguments on behalf of Apple, as he absolutely lacks standing to do so.[2]

Defendant's reliance on United States v. Mountain States Tel. & Tel. Co., 616 F.2d 1122 (9th Cir. 1980) is misplaced. In that case, the Ninth Circuit considered an appeal from the telephone company—not from the customer whose records were sought—which challenged an order issued under the All Writs Act to compel the telephone company's assistance in identifying the individual using a particular telephone number. Id. After the order had been issued, the telephone company contacted the Government with concerns about the order and suggested revisions to it. Id. at 1124. Revisions were made to that original order—at the request of the party whose compliance the order directed, i.e., the telephone company. Id. Upon receiving the information requested through that original order, the Government obtained a second order directing the telephone company to assist with an "in-progress" trace of the telephone number. Id. at 1125-26. The telephone company then challenged that order as burdensome and as outside the court's authority,

---

[1] [2]

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

valid warrant based on probable cause to believe those items may contain evidence of a crime or crimes.

The All Writs Act "cannot be used to circumvent the safeguards set in place by existing law." In re Application of the United States for an Order Authorizing Disclosure of Location Information of a Specified Wireless Telephone, 849 F.Supp.2d 526, 580 (D. Md. 2011); Goldsmith, 526 U.S. at 537 (the All Writs Act generally does not provide alternatives to "other, adequate remedies at law"). Here, the safeguards are outlined in the Fourth Amendment and Rule 41. The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause," and Rule 41 likewise requires the Government to establish probable cause to search for and seize property. U.S. Const. Amend. IV, Fed. R. Crim. Pro. 41(d)(1). Rule 41 also sets forth the remedies available to Defendant, should he determine that he has suffered unwarranted intrusions by the Government. Fed. R. Crim. Pro. 41(g)-(h). When a rule of criminal procedure addresses a particular issue, it "provides the applicable law," and the All Writs Act cannot be used to the contrary. Carlisle v. United States, 517 U.S. 416, 429 (1996). Because the Government seeks an order from this Court "in aid of" the execution of the two previously issued search warrants, and because Rule 41(g)-(h) provides the applicable law, if Defendant wishes to challenge those search warrants, he must do so through a motion to suppress evidence after the warrants are executed, not before.

The Ninth Circuit's decision in United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162 (9th Cir. 2010) (en banc) provides no support for Defendant's belief that he can rewrite the parameters of the search warrants in this case through his proposed changes to the order the Government seeks.[4] In fact, the protocols Defendant seeks to implement—a waiver of reliance on the plain view doctrine, the use of a taint team, or a

[4] Again, Defendant is not a party to the Government's proposed order. Apple is the party to whom the Government's proposed order is directed.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

"detailed search protocol"—are not required by the Fourth Amendment and are not required by Ninth Circuit case law. Id. at 1178 (protocols are not constitutional requirements and serve as "guidance" only); United States v. Schesso, 730 F.3d 1040, 1047-48 (9th Cir. 2013).[5] Magistrate Judge Strombom, who issued the underlying search warrants in this matter, is extremely familiar with Defendant's proposed search protocols inasmuch as she was the Chief Magistrate Judge during the period of time when such search protocols were mandatory in the Ninth Circuit. See Chief Magistrate Judge Karen L. Strombom's October 1, 2009 Letter to the United States Attorney's Office (attached hereto as Government's Exhibit (Exh.); A). See also Schesso, 730 F.3d at 1048-49 (noting that magistrate judges in the Western District of Washington implemented the then-mandatory search protocols for approximately a year until the search protocols were no longer binding circuit precedent). Magistrate Judge Strombom nonetheless concluded that search protocols like those now proposed by Defendant were unnecessary, and issued the underlying warrants without them. As the Ninth Circuit recently recognized in Schesso, this is precisely what magistrate judges should do with each warrant presented. Id. at 1050. If Defendant disagrees with Magistrate Judge Strombom's decision with the terms of the underlying search warrants, his recourse is to seek suppression of specific evidence once the search has been conducted.

Finally, the search protocols Defendant seeks to implement in his proposed order have nothing to do with Apple, the party to whom the Government's Application and proposed order is directed. They are simply a preview of arguments Defendant may use in a future motion to suppress evidence and, as no evidence has yet been retrieved from the iPhone5, are wholly premature.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

3. Conclusion.

The Government's Application, filed pursuant to the All Writs Act, seeks to compel a third-party, Apple, to aid the Government in its execution of previously issued search warrants. Defendant is not a party to the Government's Application, and is not the party to whom the Government's proposed order is directed. Defendant cannot reshape the parameters of the previously issued search warrants and circumvent Rule 41(g)-(h) by using the Government's Application under the All Writs Act to challenge the terms of those search warrants. Thus, for all the foregoing reasons, Defendant's proposed order should be denied. For the reasons set forth herein, and those set forth in the Government's Application, the Government requests that its proposed order be issued forthwith.

DATED this 6th day of November, 2013.

Respectfully submitted,

JENNY A. DURKAN
United States Attorney

s/Marci L. Ellsworth
MARCI L. ELLSWORTH
Assistant United States Attorney
United States Attorney's Office
1201 Pacific Ave., Suite 700
Tacoma, Washington 98402
Phone: (253) 428-3800

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on Nove7 T16 >>BDC (5)Tj ( )Tj EMC /P <</MCID /P <</MC

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. DAVID MICHAEL NAVARRO, Defendant.	CASE NO.CR13-5525 BHS ORDERGRANTING THE GOVERNMENT'S APPLICATION

This matter comes before the Court on the Government's application for an order to direct Apple to unlock Defendant David Michael Navarro's ("Navarro") iPhone. (Dkt. 22).

On September 20, 2013, the Government filed the application ex parte. Id. On October 25, 2013, the Court denied the ex parte status and set a briefing schedule. Dkt. 35. On November 1, 2013, Navarro responded. Dkt. 36. On November 6, 2013, the Government replied. Dkt. 37.

Navarro objects to the application on three basis: (1) Apple must have an opportunity to be heard, (2) the factual basis is lacking, and (3) the Court should impose

BENJAMIN H. SETTLE