

**UNITED STATES DISTRICT COURT  
DISTRICT OF MAINE**

<b>UNITED STATES OF AMERICA</b>	)	
	)	
	)	
<b>v.</b>	)	<b>CRIMINAL No. 10-86-P-H</b>
	)	
<b>JACKIE DARREL TAYLOR, JR.,</b>	)	
	)	
<b>DEFENDANT</b>	)	

**DECISION AND ORDER ON MOTION TO SUPPRESS**

The indictment charges the defendant with failure to pay child support, in violation of 18 U.S.C. § 228(a)(3). After indictment, the government obtained a search warrant for an e-mail account registered to the defendant. The defendant has filed a motion to suppress all the seized e-mails and related information on the following grounds: (1) the government failed to take adequate precautions to exclude privileged communications, (2) attorney-client information has in fact been disclosed to the government, (3) the search warrant was overly broad and insufficiently particularized, and (4) e-mails that qualified as “arguably privileged” were not isolated in the review process. The motion to suppress is **DENIED**.

**FACTS**

It is undisputed that, before indictment, lawyers were appointed for the defendant in both Idaho, where he lives, and Maine, where he has been indicted, and that the government knew of their appointment. After indictment, a magistrate judge of this court issued a warrant that authorized a

search of all information associated with an identified Microsoft hotmail account of the defendant, and the seizure of all information “that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 228” including “[r]ecords relating to business and/or other financial and accounting matters, as well as all records relating to the purchasing and selling of goods and services.”<sup>1</sup>

In response to the warrant, Microsoft provided a “zip drive” containing messages from the e-mail address.<sup>2</sup> When a government agent began searching the e-mails, he first began viewing only the header information, which revealed the sender, receiver, date, and subject.<sup>3</sup> In this initial review of header information, the agent saw that there was e-mail correspondence to or from the defendant’s lawyer(s).<sup>4</sup> At that point he stopped his review and contacted the prosecuting AUSA.<sup>5</sup>

The government then filed a Motion for Approval of Government’s Search Procedure to Protect Privileged Materials, proposing a “filter agent” procedure whereby an AUSA uninvolved with the prosecution would review the e-mail materials to cull out any potentially privileged materials before the investigating agent and the prosecuting AUSA received them.<sup>6</sup> Over the

---

<sup>1</sup> No. 2:10-mj-91-JHR, Search and Seizure Warrant (Docket Item 3) (incorporating Attachments A and B to the Application for Warrant and Supporting Affidavit).

<sup>2</sup> Mot. for Approval of Gov’t’s Search Procedure to Protect Privileged Materials at 1 (No. 2:10-cr-86-DBH, Docket Item 31).

<sup>3</sup> Id.

<sup>4</sup> Id.

<sup>5</sup> Id. The defendant does not contest the government’s statement of the facts.

<sup>6</sup> Id. at 2.

defendant's objection<sup>7</sup> and after making modifications for the defendant's benefit, the magistrate judge entered an order permitting the filter agent procedure.<sup>8</sup> The order identified three categories of materials: privileged, arguably privileged, and unprivileged.

Next, the filter agent reviewed the materials using the procedures prescribed in the court's order and removed eleven privileged e-mails. These privileged materials were provided to counsel for the defendant, not to the prosecuting AUSA or the investigating agent.<sup>9</sup> The filter agent also determined that there was nothing within the category of "arguably privileged" material, and so informed the defendant's lawyer.<sup>10</sup> The remaining, unprivileged, materials were provided to the investigating agent and the prosecuting attorney in the case.<sup>11</sup>

---

<sup>7</sup> The defendant objected to the proposed procedure because he feared that his consent could be construed as a waiver of the privilege and because he argued that the motion should not be ruled upon until any suppression motion pertaining to the seized e-mails was decided. Resp. to Gov't's Mot. to Approve Search Procedure to Protect Privileged Materials at 1-2 (Docket Item 33).

<sup>8</sup> Mem. Decision and Order on Mot. for Approval of Search Procedure (Docket Item 35).

<sup>9</sup> Gov't's Opp'n to Def.'s Mot. to Suppress at 4 (Docket Item 66). In his order authorizing the filter agent, the Magistrate Judge said that he based his decision "upon the expectation and presumption that the Government's privilege team and the trial prosecutors will conduct themselves with integrity." Mem. Decision and Order on Mot. for Approval of Search Warrant Procedure at 2-3 (Docket Item 35) (quoting In re Search of 5444 Westheimer Rd. Suite 1570, Misc. Action No. H-06-238, 2006 WL 1881370, at \*3 (S.D. Tex. July 6, 2006) (citation, internal quotation marks, and footnote omitted)). The defendant does not contend that there has been any sharing of information between the filter agent and the case prosecutor or investigating agent and has not asked for an evidentiary hearing on this issue.

<sup>10</sup> Gov't's Opp'n to Def.'s Mot. to Suppress at 4.

<sup>11</sup> Id.

## ANALYSIS

### A. ***Failure to Take Adequate Precautions to Exclude Privileged Communications***

The defendant argues that he is entitled to suppression of all the seized evidence because “the government seized privileged and confidential communications as a result of the failure to take adequate protective measures in the drafting of the warrant and in its execution.”<sup>12</sup> His argument is that the filter agent approach “is *per se* inadequate as a matter of law,” that knowing he already had a lawyer the government should have realized in advance that its search warrant would produce privileged communications and have taken preventive steps accordingly, and that these failures call for suppression of all the material seized.<sup>13</sup>

The parties have not referred me to any First Circuit decision dealing with the use of a filter agent. Case law from the rest of the country does not yield clear answers,<sup>14</sup> but some themes emerge. A number of cases have

---

<sup>12</sup> Mot. to Suppress Evidence at 1 (Docket Item 39).

<sup>13</sup> *Id.* at 2-3.

<sup>14</sup> For example, here is the Department of Justice’s summary of the case law:

Preferred practices for determining who will comb through the files vary widely among different courts. In general, however, there are three options. First, the court itself may review the files *in camera*. Second, the presiding judge may appoint a neutral third party known as a “special master” to the task of reviewing the files. Third, a team of prosecutors or agents who are not working on the case may form a “filter team” or “taint team” to help execute the search and review the files afterwards. The filter team sets up a so-called “ethical wall” between the evidence and the prosecution team, permitting only unprivileged files to pass over the wall.

Because a single computer can store millions of files, judges will undertake *in camera* review of computer files only rarely. Instead, the typical choice is between using a filter team and a special master. Most prosecutors will prefer to use a filter team if the

(continued next page)

permitted its use.<sup>15</sup> At the same time, there is a healthy skepticism about the reliability of a filter agent or Chinese or ethical wall within a prosecutor's office,<sup>16</sup> a skepticism perhaps prompted by the famous failures of such a procedure in United States v. Noriega, 764 F. Supp. 1480 (S.D. Fla. 1991).<sup>17</sup> Courts exhibit particular concern over use of filter agents or taint teams in searches of lawyers' offices, where privileged materials of many clients could be compromised.<sup>18</sup> There, judges have sometimes required alternatives such as

---

court consents. A filter team can usually review the seized computer files fairly quickly, whereas special masters often take several years to complete their review. On the other hand, some courts have expressed discomfort with filter teams.

Although no single standard has emerged, courts have generally indicated that evidence screened by a filter team will be admissible only if the government shows that its procedures adequately protected the defendants' rights and no prejudice occurred. One approach to limit the amount of potentially privileged material in dispute is to have defense counsel review the output of the filter team to identify those documents for which counsel intends to raise a claim of privilege. Files thus identified that do not seem relevant to the investigation need not be litigated. Although this approach may not be appropriate in every case, magistrates may appreciate the fact that defense counsel has been given the chance to identify potential claims before the material is provided to the prosecution team.

In unusual circumstances, the court may conclude that a filter team would be inadequate and may appoint a special master to review the files.

United States Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, ch. 2(F)(2)(b) (3d ed. 2009) (citations omitted), available at <http://www.cybercrime.gov/ssmanual/02ssma.html> (last visited February 9, 2011).

<sup>15</sup> See, e.g., United States v. Evanson, 2007 WL 4299191, \*16-17 (D. Utah Dec. 5, 2007); United States v. Winters, 2006 WL 2789864 (S.D.N.Y. Sept. 27, 2006); Hicks v. Bush, 452 F. Supp. 2d 88, 102-03 (D.D.C. 2006).

<sup>16</sup> See, e.g., United States v. Neill, 952 F. Supp. 834, 841 (D.D.C. 1997) (placing burden on government to rebut presumption that tainted material reached the prosecution team); In re Search Warrant for Law Offices, 153 F.R.D. 55, 59 (S.D.N.Y. 1994).

<sup>17</sup> See In re Grand Jury Subpoenas, 454 F.3d 511, 523 (6th Cir. 2006).

<sup>18</sup> See, e.g., United States v. Stewart, 2002 WL 1300059 (S.D.N.Y. June 11, 2002); Note, The Search and Seizure of Privileged Attorney-Client Communications, 72 U. Chi. L. Rev. 729, 742-44 (2005); Note, The Department of Justice Guidelines to Law Office Searches: The Need to (continued next page)

appointment of a special master, a wholly independent third party.<sup>19</sup> Courts seem to recognize a distinction between circumstances where the government has not yet obtained the records on the one hand (allowing defense counsel's preliminary review),<sup>20</sup> and, on the other hand, what the government should do when it has already seized the records, then realizes that it may have privileged materials (allowing use of filter agent there).<sup>21</sup> Finally, some of the cases and some of the commentators suggest a role for judicial review.

In the circumstances of this search and this e-mail account, I have no reason to find that it was inherently negligent for the government to fail to foresee that its seizure of the defendant's e-mails would produce privileged documents simply because he had a lawyer, and I do not conclude that every warrant for an e-mail search must have at the outset a built-in privilege protection procedure, any more than there is such a requirement for every paper document search.<sup>22</sup> Instead, I conclude that the government behaved reasonably here by immediately seeking judicial instructions once its agent

---

Replace the "Trojan Horse" Privilege Team with Neutral Judicial Review, 43 Wayne L. Rev. 1855 (1997).

<sup>19</sup> Stewart, 2002 WL 1300059.

<sup>20</sup> In re Grand Jury Subpoenas, 454 F.3d at 522-23.

<sup>21</sup> Id.; United States v. Mower, 2010 WL 3938265, at \*3 (D. Utah Oct. 6, 2010).

<sup>22</sup> In such cases, there is actually a seizure, then a search, then another seizure. First the zip drive was seized from Microsoft. Then it had to be reviewed to determine which documents fit within the parameters of the warrant such that they could be finally seized. The paper analogy would be the segregation of boxes or file cabinets containing documents, then a search of the contents to determine which could be finally seized. See, e.g., United States v. Hargus, 128 F.3d 1358, 1363 (10th Cir. 1997); Note, The Search and Seizure of Privileged Attorney-Client Communications, 72 U.Chi. L. Rev. at 745 n.73 (advancing reasons why initial seizures should be allowed even though they may contain privileged materials). The Model Code of Pre-Arraignment Procedure § 220.5 (1975) suggests a procedure for such cases involving intermingled paper documents. It has been endorsed by a number of courts, see, e.g., United States v. \$92,422.57, 307 F.3d 137, 154 (3d Cir. 2002) (Alito, J.); United States v. Tamura, 694 F.2d 591, 595-97 (9th Cir. 1982). Similar issues of intermingling arise and are dealt with by statute in electronic wire surveillance cases. See Nixon v. Administrator of General Services, 408 F. Supp. 321, 363-64 & n.57 (D.D.C. 1976) (3-judge district court, McGowan, J.).

noticed that e-mail headers reflected communications between lawyer and client. It is true that some cases could be read to suggest that at that point the defendant and his lawyer should have been allowed a first look at the e-mails, so as to create a privilege log and then let the government challenge it in court, rather than vice versa as here. But the defendant did not propose that procedure to the magistrate judge, and instead simply opposed the government's proposal in toto. The government sought judicial instructions, the magistrate judge modified its proposal, and then issued an order on how to proceed. I reject the argument that somehow that was per se an inappropriate way of proceeding.

Moreover, if something was seized improperly, the remedy is suppression of that item and perhaps its fruit,<sup>23</sup> not suppression of everything: "The remedy in the case of a seizure that casts its net too broadly is . . . not blanket suppression but partial suppression."<sup>24</sup> Here, there is nothing to suppress. After becoming aware of the existence of potentially privileged e-mails, the government took the appropriate steps to remove those e-mails from the materials the prosecuting attorney and case agent could obtain, and thus they cannot be used at trial.

Finally, there is no suggestion that the government has failed to comply with the procedures prescribed by the magistrate judge. During the initial review, the agent examined only the header information and not the content of

---

<sup>23</sup> But see United States v. Warshak, 2010 WL 5071766 (6th Cir. December 14, 2010) ("no court ha[s] applied the fruit-of-the-poisonous-tree doctrine to derivative evidence obtained as a result of improper access to materials covered by a non-constitutional privilege").

<sup>24</sup> United States v. Falon, 959 F.2d 1143, 1149 (1st Cir. 1992); Evanson, 2007 WL 4299191 at \*18 (only documents covered by the privilege can be suppressed).

the e-mail.<sup>25</sup> Thereafter, the government used the filter agent procedure approved by the magistrate judge. That agent removed the privileged e-mails and they were not disclosed to the prosecuting attorney or the case agent. Those assertions have not been contested, nor has the defendant requested an evidentiary hearing concerning them.<sup>26</sup>

**B. *Whether Attorney-Client Information was Disclosed to the Government***

The defendant asserts that because eleven e-mails were determined to be privileged, the record confirms the disclosure of attorney-client communications to the government's filter agent. Disclosure of privileged communications to any government agent, even if that individual is not involved with prosecuting the case, the defendant contends, violates the privilege and requires suppression of everything seized.

The record does not support the defendant's assertion that attorney-client information was disclosed to the filter agent or any other government representative. The magistrate judge's order states that the filter agent "will use the 'header' information on the e-mails to filter out any e-mails purporting

---

<sup>25</sup> There is no assertion that the header of the privileged e-mail contained confidential information.

<sup>26</sup> The defendant also asserts that United States v. Leon, 468 U.S. 897 (1984) does not apply. I disagree. In Leon the Supreme Court held that a violation of the Fourth Amendment does not justify exclusion of the resulting evidence "when an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope." Id. at 920. The good-faith inquiry "is confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization." Id. at 922 n.23. The exception will not apply if the warrant is "so facially deficient-i.e., in failing to particularize the place to be searched or the things to be seized-that the executing officers cannot reasonably presume it to be valid." Id. at 923. In this case, there was no basis for the government to know that its failure to take additional precautions in either obtaining the warrant, or in the warrant's execution, would result in a violation of the Fourth Amendment. Thus, the application of Leon would prevent suppression of any illegally-obtained evidence.

to be either to or from the defendant's current attorney, J. Hilary Billings, Esq., or his previous attorney, Dennis Charney, Esq., without reviewing the content of those e-mails. S/he will review the content of the remaining e-mails to ensure that no privileged information may be contained within them. S/he shall maintain a log detailing the disposition of each document in question."<sup>27</sup> There is no suggestion that the filter agent failed to follow these procedures (the government asserts the contrary<sup>28</sup> and the defendant has not requested an evidentiary hearing). Thus, as the record stands, not even the filter agent read any privileged communications.

**C. Overbreadth and Insufficient Particularity**

The defendant contends that the government made no effort to limit the scope of the warrant so as to seek only "those communications likely to produce the evidence of 'financial means.'"<sup>29</sup> The search for evidence of financial means, the defendant asserts, should have been limited to "the e-commerce sites that were [listed in the affidavit as being] linked to the e-mail address of the defendant." *Id.*

In cases involving a violation of 18 U.S.C. § 228(a)(3), however, the inquiry is broad: the defendant's income and financial means are relevant, as well as the defendant's voluntary failure to maintain employment.<sup>30</sup> Here, the

---

<sup>27</sup> Mem. Decision and Order on Mot. for Approval of Search Procedure at 3.

<sup>28</sup> Gov't's Opp'n to Def.'s Mot. to Suppress at 4.

<sup>29</sup> Reply to the Gov't's Resp. in Opp'n to Def.'s Mot. to Suppress at 2 (Docket Item 73).

<sup>30</sup> See e.g., United States v. Edelkind, 525 F.3d at 388, 398-99 (5th Cir. 2008) (approving a jury instruction that defined willfulness in section 228 in terms of whether the defendant "had money which he used to pay other expenses beyond living expenses instead of paying his child support"); United States v. Smith, 278 F.3d 33, 38-39 (1st Cir. 2002) (finding no plain error in section 228 jury instruction requiring government to prove willful failure to pay by either  
(continued next page)

search warrant permitted the government to search the e-mail account and seize “records relating to business and/or other financial and accounting matters, as well as all records relating to the purchasing and selling of goods and services.”<sup>31</sup> This scope reasonably limits the evidence to be seized. But the defendant contends that the warrant was insufficiently particularized because it permitted personal communications to be *searched* in order to seize this evidence. The defendant would prefer that the scope of the search had been limited to e-mails linked to specific internet e-commerce websites that he used or, in some fashion, have other limiting terms to limits its scope to communications that would produce evidence of financial means (he does not identify what those limiting terms should have been).

While there may be a degree of uncertainty as to the precise “applicability of the Fourth Amendment’s particularity requirement with respect to searches of computer data,”<sup>32</sup> the warrant in this case was not overly broad in allowing search of this e-mail account. The agent’s affidavit extensively documented the repeated use of this e-mail account in connection with various business enterprises, evidentiary support for a violation of the statute for failure to pay child support.

---

evidence that the defendant “had access to resources beyond the basic necessities of life, disposable income” or that he “took himself out of the workforce or reduced his ability” to pay); United States v. Ballek, 170 F.3d 871, 873 (9th Cir. 1999) (explaining that willful can mean “having the money and refusing to use it for child support; or, not having the money because one has failed to avail oneself of the available means of obtaining it”).

<sup>31</sup> No. 2:10-mj-91-JHR, Attach. B to Appl. for Search Warrant at 2 (Docket Item 3-3).

<sup>32</sup> United States v. McDarrah, 2006 WL 1997638, at \*10 (S.D.N.Y. July 17, 2006) (quoting Hensel v. Lussier, 205 F.3d 1323, at \*1 (2d Cir. 2000) (summary order)).

The Fourth Amendment does not require the government to delegate a prescreening function to the internet service provider or to ascertain which e-mails are relevant before copies are obtained from the internet service provider for subsequent searching.<sup>33</sup> The Supreme Court has noted that, even “[i]n searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized.”<sup>34</sup> The First Circuit has said that “the police may look through . . . file cabinets, files and similar items and briefly peruse their contents to determine whether they are among the documentary items to be seized.”<sup>35</sup> The same is true for the search of an e-mail account, and the search does not fail to satisfy the particularity requirement simply because the warrant does not specify a more precise e-mail search method.

#### ***D. “Arguably Privileged” E-mail***

Finally, the defendant claims that the filter process did not work. As evidence, the defendant claims that “there appear to be several e-mails that contain privileged materials” that the filter agent failed to isolate as “arguably privileged.”<sup>36</sup> Specifically, the defendant identifies six “arguably privileged” e-mails sent to law school professors at The McGeorge School of Law at the University of the Pacific. The e-mails appear on a copy of the e-mail account

---

<sup>33</sup> See United States v. Bowen, 689 F. Supp. 2d 675, 682 (S.D.N.Y. 2010); In re Search of: 3817 W. West End, 321 F. Supp. 2d 953, 958 (N.D.Ill. 2004) (“[i]t is frequently the case with computers that the normal sequence of ‘search’ and then selective ‘seizure’ is turned on its head”).

<sup>34</sup> Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976).

<sup>35</sup> United States v. Giannetta, 909 F.2d 571, 577 (1st Cir. 1990).

<sup>36</sup> Reply to the Gov’t’s Resp. in Opp’n to Def.’s Mot. to Suppress at 5.

log and identify the recipients by the initial of their first names and their last names all sent to the domain “pacific.edu”, and indicate in the header notes that the defendant is seeking help with child support issues.<sup>37</sup>

But the defendant does not assert that he ever established an attorney-client relationship with any of these law school professors that would support excluding these communications as actually privileged. I conclude, therefore, that if the filter agent made any error here, it was harmless. Identifying such e-mails as “arguably privileged” would be simply an intermediate step in determining whether they are actually privileged. Otherwise, they are not subject to protection.

#### **CONCLUSION**

Accordingly, I conclude that the defendant has no basis for excluding the seized evidence beyond the privileged e-mails, and they have not been provided to the investigating agent or the prosecuting AUSA. The defendant’s motion to suppress is therefore **DENIED**.

**SO ORDERED.**

**DATED THIS 9TH DAY OF FEBRUARY, 2011**

/s/D. Brock Hornby  
**D. BROCK HORNBY**  
**UNITED STATES DISTRICT JUDGE**

---

<sup>37</sup> Ex. A to Reply to the Gov’t’s Resp. in Opp’n to Def.’s Mot. to Suppress at 5 (Docket Item 73-1).

**U.S. DISTRICT COURT  
DISTRICT OF MAINE (PORTLAND)  
CRIMINAL DOCKET FOR CASE: 2:10cr86 (DBH)**

**United States of America**

Represented by **Craig M. Wolff**  
**Stacey D. Neumann**  
Assistant United States Attorneys  
Office of the United States Attorney  
District Of Maine  
100 Middle Street Plaza  
Portland, ME 04101  
(207) 780-3257  
email: [Craig.Wolff@usdoj.gov](mailto:Craig.Wolff@usdoj.gov)  
[stacey.neumann@usdoj.gov](mailto:stacey.neumann@usdoj.gov)

v.

**Jackie Darrell Taylor, Jr.,  
Defendant**

Represented By **J. Hilary Billings**  
Federal Defender's Office  
P.O. Box 595  
Portland, ME 04112-0595  
email: [j.hilary.billings@fd.org](mailto:j.hilary.billings@fd.org)