Per C. Olson, OSB #933863
HOEVET OLSON HOWES, PC
1000 SW Broadway, Suite 1500
Portland, Oregon 97205
Telephone: (503) 228-0497
Facsimile: (503) 228-7112
Email: per@hoevetlaw.com

Of Attorneys for Defendant

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

UNITED STATES OF AMERICA, Plaintiff, v. DAVID LEE FRY, Defendant.	Case No. 3:16-CR-00051-13-BR MEMORANDUM IN SUPPORT OF DEFENDANT'S MOTION TO SUPPRESS EVIDENCE (FACEBOOK ACCOUNTS)

Defendant David Fry hereby submits this Memorandum of Law in Support of Defendant's Motion to Suppress Evidence obtained as a result of a search warrant served on Facebook.

Background

The government executed a search warrant on Facebook for the entire accounts of Ammon Bundy, Jon Ritzheimer, Joseph O'Shaughnessy, Ryan Payne, Ryan Bundy, Shawna Cox, Peter Santilli (2 accounts), Jason Patrick, Sean Anderson, Sandra Anderson, David Fry, Blaine Cooper (two accounts), Wesley Kjar, Corey Lequieu, Jason Blomgren, Travis Cox, Darryl Thorn, Geoff Stanek, and Eric Lee Flores. The search

HOEVET OLSON HOWES, PC
ATTORNEYS AT LAW
1000 S.W. BROADWAY, #1500
PORTLAND, OREGON 97205
(503) 228-0497

warrant also targeted the Bundy Ranch Community."[1] The search warrant application and affidavit, drafted and signed by FBI Special Agent Peter Summers, is attached as Exhibit A (filed under seal). The search warrant and the return is attached as Exhibit B (filed under seal).

The search warrant affidavit attempts to state a probable cause basis for the search of the Facebook accounts for evidence of defendants' involvement in the crimes alleged in the indictment. It provides a summary of events leading up to the January 2, 2016, occupation of the Malheur National Wildlife Refuge (MNWR), the occupation itself, and the arrest of defendants. The affidavit provides examples of Facebook activity from each account. (Ex. A, starting at page 18 of 98). This activity consists of public postings of comments, photos, and videos; the "sharing" of posts or material from other sources; and links to other websites or sources.

Facebook and its various functions and features are described beginning at page 81 of the affidavit. (Ex. A, page 82 of 98). It is not clear from which Facebook feature(s) the government obtained the various postings summarized in the affidavit. It could be assumed that the agent found the postings simply by logging in as a Facebook user and looking at the publically viewable Facebook pages of each targeted user, but even that is not clear.

In contrast to the narrow category of public postings for which arguably there was probable cause, the search warrant affidavit sought production of private Facebook features for which there was no probable cause. (See "Attachment B" to search warrant affidavit in Ex. A, starting at page 94 of 98). Included in this broad sweep were "private messages" that Facebook users send or receive from other users – the functional equivalent of email messages. (Described at Ex. A, page 84 of 98, ¶ 106). Also

[1] The government also served a warrant for Duane Ehmer's account, but Facebook apparently did not provide any responsive materials for him.

HOEVET OLSON HOWES, PC
ATTORNEYS AT LAW
1000 S.W. BROADWAY, #1500
PORTLAND, OREGON 97205
(503) 228-0497

included were other functions viewable only by the user and/or designated "friends," such as photographs; lists of "friends" and the friends' Facebook user identification numbers; groups or websites that the user followed or liked; profile information; etc.[2] Attachments A and B to the affidavit were also attached to the search warrant. (Ex. B).

Defendants contend that the warrant was overbroad by authorizing the search and seizure of private email messages and other applications for which there was no probable cause.

Legal Standards

The Fourth Amendment protection "against unreasonable searches and seizures" requires that a search warrant "particularly describe[ ] the place to be searched and the persons or things to be seized." 4th Amend, U.S. Const. The purpose of this particularity requirement was to prevent "general searches." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). "The Fourth Amendment's specificity requirement prevents officers from engaging in general, exploratory searches by limiting their discretion and providing specific guidance as to what can and cannot be searched and seized." *United States v. Adjani*, 452 F.3d 1140, 1147 (9th Cir. 2006); s*ee also United States v. Vasquez*, 654 F.3d 880, 885 (9th Cir. 2011).

The Ninth Circuit refers to "this requirement as one of 'specificity'" which has two aspects: particularity and breadth. Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based." *United States v. Hill*, 459 F.3d 966, 973 (9th Cir. 2006), *citing United States v. Towne*, 997 F.2d 537, 544 (9th Cir. 1993) (internal quotation marks and citations omitted).

---

[2] The Facebook user can select the privacy setting with regard to each Facebook feature except for the private message feature. The choices are "Only Me" (visible only to the user); "Your friends" (visible to the user and friends); and "Public" (visible to anyone with a Facebook account). Private messages are seen only by the sender and recipient with a Facebook account.

HOEVET OLSON HOWES, PC
ATTORNEYS AT LAW
1000 S.W. BROADWAY, #1500
PORTLAND, OREGON 97205
(503) 228-0497

"[T]the concept of breadth may be defined as the requirement that there be probable cause to seize the particular thing named in the warrant." *Does I Through IV v. United States (In re Grand Jury Subpoenas Dated December 10, 1987)*, 926 F.2d 847, 857 (9th Cir. 1991). "[T]he scope of the warrant, and the search, is limited by the extent of the probable cause." *Id*. Hence, "... the scope of the warrant to search is dependent upon the extent of the showing of probable cause. The command to search can never include more than is covered by the showing of probable cause to search." *United States v. Whitney*, 633 F.2d 902, 907 (9th Cir.1980) (quoting *United States v. Hinton*, 219 F.2d 324, 325 (7th Cir.1955)), *cert. den.*, 450 U.S. 1004 (1981).

Judicial scrutiny of general warrants is at its highest when the warrants seek written correspondence, literary material, and other things protected by the First Amendment. After surveying the history leading up to the Fourth Amendment, the Supreme Court in *Stanford v. State of Texas*, 379 U.S. 476 (1965), stated:

> "[W]hat this history indispensably teaches is that the constitutional requirement that warrants must particularly describe the 'things to be seized' is to be accorded the most scrupulous exactitude when the 'things' are books, and the basis for their seizure is the ideas which they contain. * * * No less a standard could be faithful to First Amendment freedoms." *Id*. at 485. (internal citations, footnote omitted).

A finding of overbreadth may result in the suppression of all evidence obtained by the warrant and all fruits thereof. *See United States v. Spilotro*, 800 F.2d 959 (9th Cir. 1986) (good faith exception to exclusionary rule did not apply to overbroad warrant, resulting in suppression); *United States v. Center Art Galleries – Hawaii, Inc.*, 875 F.2d 747, 750 (9th Cir. 1995) (warrant overbroad because it was not limited to scope of investigation, resulting in suppression); *United States v. SDI Future Health, Inc.*, 568 F.3d 684 (9th Cir. 2009) (warrant for "documents relating to non-privileged internal memoranda and E-mail" was too broad because it did not focus on the subject of the

HOEVET OLSON HOWES, PC
ATTORNEYS AT LAW
1000 S.W. BROADWAY, #1500
PORTLAND, OREGON 97205
(503) 228-0497

investigation, resulting in partial suppression); *United States v. Cardwell*, 680 F.2d 75 (9th Cir. 1982) (overbroad warrant resulted in total suppression); *United States v. Kow*, 58 F.3d 423, 427 (9th Cir. 1995) (same).

The prohibition of general warrants and the concern for overbreadth apply not only to traditional searches and seizures of documents in tangible form, but to searches of digital evidence, including computers and social media. In *United States v. Cotterman*, 709 F.3d 952, 957 (9th Cir. 2013), the Court stated:

> "Laptop computers, iPads and the like are simultaneously offices and personal diaries. They contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails. This type of material implicates the Fourth Amendment's specific guarantee of the people's right to be secure in their 'papers.' US Const. amend. IV. The express listing of papers 'reflects the Founders' deep concern with safeguarding the privacy of thoughts and ideas – what we might call freedom of conscience – from invasion by the government.' * * * These records are expected to be kept private and this expectation is 'one that society is prepared to recognize as "reasonable."'" *Cotterman*, 709 F.3d at 964 (citations omitted).

The Supreme Court ruled consistently with the foregoing with regard to cell phones in *Riley v. California*, 134 S. Ct. 2473 (2014), when it held that officers may not conduct a warrantless search of a cell phone incident to an arrest. The Court emphasized the privacy concerns with cell phones that are present to a greater degree than with other physical objects that an arrested person might possess. The incredible quantity and variety of private information storable on a smart phone sets it apart in its ability to store communications, contacts, photographs, health records, web searching habits, and so on. The Court also found a privacy interest in the phone's "apps" that can reveal the user's political views, health issues, finances, hobbies, and romantic interests. These apps "can form a revealing montage of the user's life." *Riley*, 134 S. Ct. at 2490. The phone's ability to access the Internet through Cloud computing and storage did not diminish the user's expectation of privacy. In fact, that feature of a cell

HOEVET OLSON HOWES, PC
ATTORNEYS AT LAW
1000 S.W. BROADWAY, #1500
PORTLAND, OREGON 97205
(503) 228-0497

phone helped to distinguish it from traditional "closed containers" that an officer might otherwise be permitted to search incident to an arrest, because what the phone reveals about the person is not contained within the phone itself. *Riley*, 134 S. Ct. at 2491.

The necessity of a warrant for digital information on a smart phone triggers the associated requirement that the warrant satisfy the specificity requirement discussed above. *See Riley*, 134 S. Ct. at 2494 (stating that the prohibition on search of cell phone in absence of warrant or exigent circumstance goes to heart of prohibition on reviled "general warrants" of colonial era).

Congress has recognized and expressed society's expectation of privacy in social media and electronic communications by requiring law enforcement to obtain a search warrant for such evidence held by a "provider of electronic communication service." 18 USC § 2703(a). Courts also have recognized a reasonable expectation of privacy in stored digital communications. *See generally Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892 (9th Cir. 2008) (employees had reasonable expectation of privacy in content of text messages), *rev'd and remanded on other grounds, City of Ontario v. Quon*, 560 U.S. 746 (2010) (court assumes employees had reasonable expectation of privacy in texts, but concluding that employer review of texts was reasonable); *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (a subscriber enjoys reasonable expectation of privacy in emails maintained by internet service provider); *United States v. DiTomasso*, 56 F. Supp. 3d 584 (S.D. N.Y. 2014) (defendant had reasonable expectation of privacy in texts and on-line chats); *In re Applications for Search Warrants*, 2012 WL 4383917, at *5 (D. Kan. Sept. 21, 2012) (same); *United States v. Ali*, 870 F. Supp. 2d 10, 39 n39 (D.D.C. 2012) (same).

Several courts also have specifically recognized that Facebook users have a reasonable expectation of privacy in messages and private postings. *See Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965 (C.D. Cal. 2010) (private Facebook

HOEVET OLSON HOWES, PC
ATTORNEYS AT LAW
1000 S.W. BROADWAY, #1500
PORTLAND, OREGON 97205
(503) 228-0497

messages are "inherently private" because they "are not readily accessible to the general public."); *R.S. ex rel. S.S. Minnewaska Area School Dist. No.* 2149, 894 F. Supp. 2d 1128, 1142 (D. Minn. 2012) (based on established Fourth Amendment precedent, R.S. had a reasonable expectation of privacy to her private Facebook information and messages.); *United States v. Meregildo*, 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012) ("Whether the Fourth Amendment precludes the Government from viewing a Facebook user's profile absent a showing of probable cause depends, *inter alia,* on the user's privacy settings.")

The bedrock Fourth Amendment principle of protecting an individual's privacy by prohibiting general warrants applies with particular force in the digital age, where massive amounts of private information can be captured in an instant. Computers and social media accounts "are postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more." Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 569 (2005). Because a computer or on-line account can store a huge array of one's personal papers in a single place, the seizure of a computer, a hard drive, or the contents of a Facebook account can easily amount to a general search of one's home and belongings. For this reason, courts have correctly warned that "'[c]omputer search warrants are the closest things to general warrants we have confronted in this history of the Republic.'" *In re Appeal of Application for Search Warrant*, 71 A.3d 1158, 1175 (Vt. 2012) (quoting P. Ohm, Response, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 Va. L. Rev. in Brief 1, 11 (2011)).

A magistrate judge in this circuit rejected an overbroad warrant for social media accounts in *In the Matter of the Search of Google Email Accounts*, 2015 WL 926619 (D. Alaska, March 3, 2015). As with Facebook accounts, Google has many separate applications storing different types of data and personal information. The magistrate

HOEVET OLSON HOWES, PC
ATTORNEYS AT LAW
1000 S.W. BROADWAY, #1500
PORTLAND, OREGON 97205
(503) 228-0497

refused to issue warrants requiring the disclosure of entire Google accounts because the warrants were not narrowly tailored to require the production of only the part for which the government had probable cause. *Ibid*.

The court emphasized that the Ninth Circuit has admonished judicial officers to be vigilant in striking the right balance between law enforcement and Fourth Amendment rights. "'The process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has not probable cause to collect.'" *Ibid., quoting United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1177 (9th Cir. 2010). Whereas computer technology may "'in theory justify blanket seizures * * *, the government must still demonstrate to the magistrate *factually* why such a broad search and seizure authority is reasonable in the case at hand. * * * Thus, there must be some threshold showing before the government may "seize the haystack to look for the needle."'" *In re Search of Google Email Accounts*, 2015 WL 926619 at *5, *quoting United States v. Hill,* 459 F.3d 966, 975 (9th Cir. 2006) (emphasis in *Hill*).

In several Ninth Circuit cases, including *Hill*, the Court has addressed the scope of warrants authorizing the wholesale search and seizure of computer equipment and electronic storage devices. Generally speaking, the Court has held that if law enforcement has probable cause to believe that evidence of a crime will be found somewhere on the devices, the search is lawful *as long as* the government agent explained the need to seize and search all devices in the search warrant affidavit. *See, e.g., United States v. Hay*, 231 F.3d 630, 637 (9th Cir. 2000) ("[T]he affidavit explained why it was necessary to seize the entire computer system in order to examine the electronic data for contraband. It also justified taking the entire system off site because of the time, expertise, and controlled environment required for a proper analysis"); *United States v. Lacy*, 119 F.3d 742, 746 (9th Cir. 1997) (same). In *Hill*, the Court found

HOEVET OLSON HOWES, PC
ATTORNEYS AT LAW
1000 S.W. BROADWAY, #1500
PORTLAND, OREGON 97205
(503) 228-0497

the affidavit lacking in that regard and held that the search warrant was overbroad, although it ultimately did not suppress. *Hill*, 459 F.3d at 976-77.

Discussion

1. The Warrant is Overbroad

To determine whether a warrant is sufficiently particular and not overbroad, the Court considers three factors: (1) whether probable cause exists to seize all items of a particular type described in the warrant; (2) whether the warrant sets out objective standards by which executing officers can differentiate items subject to seizure from those that are not; and (3) whether the government was able to describe the items more particularly in light of the information available to it at the time the warrant was issued. *See Adjani*, 452 F.3d at 1148 (applying that methodology).

The full scope of the Facebook search warrant is set forth in more than two pages under the heading, "I. Information to be Disclosed by Facebook" in "Attachment B" of the warrant. (Ex. B, starting at page 4 of 8). The warrant is overbroad because Agent Summers' affidavit does not provide probable cause that evidence of criminal activity will be found in many of the private features listed in the warrant, including but not limited to, private messages, chat history, video calling history, photos, status updates, wall postings, friend lists, list of groups and networks of which the user is a member, user identifications of friends and groups, rejected "Friend" requests, pending "Friend" requests, comments, information about the user's access to and use of Facebook applications and services, history of the "like" feature, etc.[3] The district court in Kansas granted a motion to suppress similarly overbroad warrants on Yahoo and

[3] One measure of overbreadth is the sheer volume of data the government received from Facebook. Shawna Cox' production was over 5,000 pages in length; Joseph O'Shaughnessy's was 25,000 pages; Jon Ritzheimer's was 28,000 pages; Sean Anderson was more than 18,000 pages; Bundy Ranch is more than 5,000 pages; David Fry's is just under 800 pages.

HOEVET OLSON HOWES, PC
ATTORNEYS AT LAW
1000 S.W. BROADWAY, #1500
PORTLAND, OREGON 97205
(503) 228-0497

Apple because they included "emails, pictures, friends, and groups" within their scope. *United States v. Barthelman*, 2013 WL 3946084, at *11 (July 31, 2013, D. Kan).

Nor does the affidavit explain why a wholesale seizure of all Facebook data is necessary in order to obtain the one part for which there is probable cause, as required by *Hill*. For example, there is nothing to indicate that Facebook is technologically unable to separate and produce only parts of a user's account. Available evidence suggests the opposite. Facebook's direction to law enforcement, available on its website, provides that warrants must be specific as to which types of data must be produced. (Exhibit C – Information for Law Enforcement Authorities). Search warrants "must identify requested records with particularity" and not be "overly broad or vague." Search warrants are required to compel the disclosure of "stored contents of any account, which may include messages, photos, videos, timeline posts, and location information." If Facebook were unable to separate out these different services in response to a search warrant, it would not bother to require particularity and instead would simply instruct law enforcement to request entire accounts.

Also, a Facebook account does not present the same challenges that law enforcement confronts with a seized computer or digital storage device in which targeted evidence could reside in any number of hidden files, thus justifying a wholesale search of the entire device as described in *Hill*, *Hay*, and *Lacy*. A Facebook account is not susceptible to much doubt as to where particular types of files or data would be found. Each feature serves a specific, identifiable purpose that announces its content. Thus, the affiant's duty to explain why it is necessary to seize the entire account to find a document already known to exist in a specific place is more pronounced than it is with a computer system.

The only hint of a justification for a wholesale search and seizure of the Facebook accounts is found in paragraph 119. (Ex. A, page 87 of 98). Agent Summers

HOEVET OLSON HOWES, PC
ATTORNEYS AT LAW
1000 S.W. BROADWAY, #1500
PORTLAND, OREGON 97205
(503) 228-0497

argues that IP logs, communications, photos, tags, status updates, and associated meta-data, provide evidence of who accessed the account, and the time and location of the access, thus providing the "who, what, why, when, where, and how" of criminal conduct and enabling the government to prove its case. This "user attribution" evidence, Summers argues, is "analogous to the search for 'indicia of occupancy' while executing a search warrant at a residence." (Ibid).

The problem with this argument is that the defendants made no secret as to who they were, what they were doing, why they were doing it, where they were, and how they were doing it. The public Facebook postings summarized in the affidavit uniformly include the user's true name and the date of the posting. The photos are posted with captions identifying who is pictured and what is happening at the refuge. Several defendants exhort others in the outside world to join the protest. While it is theoretically possible that someone could open a Facebook page using another person's name, the affiant provides no reason to suspect that has occurred, and the photographs showing the named users virtually rules out that possibility.

Under these circumstances, Agent Summers' "user attribution" argument is a red herring. But even if it were not, he still provides no grounds for going after private messages. The issue again is one of overbreadth. *See United States v. Timley,* 443 F.3d 615, 623 (8th Cir. 2006) (questioning the breadth of a warrant that authorized officers to seize "anything related to indicia of ownership"). The "who" can be established by targeting only the subscriber and billing information. The "where" and "when" can be established by obtaining the IP logs. The affidavit provides no basis – rooted in probable cause – to obtain private messages. Agent Summers states that Facebook activity may provide insight into the user's "motive and intent to commit the crime" or "consciousness of guilt" (Ex. B, page 87 of 98), but that is purely speculative

HOEVET OLSON HOWES, PC
ATTORNEYS AT LAW
1000 S.W. BROADWAY, #1500
PORTLAND, OREGON 97205
(503) 228-0497

and falls well short of probable cause that such evidence actually will be found in the private features of the user's Facebook account.

2. The Search and Seizure Protocols Do Not Narrow the Scope of the Warrant

The search warrant contains two features that, on the surface, appear to narrow the scope of the warrant by requiring a review for "responsive" material and a sequestration of "non-responsive" material. However, these features do not otherwise limit the scope of the warrant to parts of the Facebook accounts for which there was probable cause. Nor do they limit what can be searched and what can be seized in ways that might otherwise save an unconstitutionally overbroad warrant.

The Court looks favorably upon warrants containing search protocols that minimize the risk of overbreadth, for example by requiring initial review by only qualified experts who know where to find targeted material, or by describing the circumstances that would explain and justify the seizure and off-site search of digital evidence. *See Hay,* 231 F.3d at 636. However, the protocols must be closely examined to determine whether they serve the intended purpose of narrowing the scope of the warrant to only that which is supported by probable cause.

As the Court in *Adjani* put it:

> "The protocol [set forth in the search warrant affidavit], of course, does not eliminate the necessity that the protocol procedures and the materials seized or searched fall within the scope of a *properly issued* warrant supported by *probable cause*." *Adjani*, 452 F.3d at 1149 n7 (emphasis added).

The protocols in the Facebook warrant are in Attachment B under the headings, "Information to be Seized by the Government" (Section II) and "Search Procedure" (Section III). (Ex. B). Section II describes the information "to be seized" by the government as all information that "constitutes evidence of violations of 18 U.S.C. § 372" for specified time periods and "pertaining to" various types of communications and records. Section III describes the search procedure as authorizing law enforcement to

HOEVET OLSON HOWES, PC
ATTORNEYS AT LAW
1000 S.W. BROADWAY, #1500
PORTLAND, OREGON 97205
(503) 228-0497

review all information provided by Facebook and to separate "responsive" from "nonresponsive" material. Information deemed responsive to the warrant "will be copied onto a separate storage device or medium" and "may be used by law enforcement in the same manner as any other seized evidence." Information that is not responsive to the warrant "will be sealed and stored on a secure medium or in a secure location," and "will not be reviewed again without further order of the Court…" Section III further provides that the government will retain a "complete copy" of information provided by Facebook for any number of reasons, including "proving the authenticity of evidence to be used at trial."

These provisions do not narrow the scope of the overbroad warrant. As for Section II, despite the impression one might obtain from the heading "Information to be Seized by the Government," the search warrant does not provide for the seizure of anything less than all raw data provided by Facebook. Once Facebook complied with the search warrant by disclosing the entirety of defendants' accounts, the government thereby "seized" those accounts in their entirety. There is no separate act of "seizure" that occurs simply by virtue of defining a subset of all data and proclaiming only that subset "seized." Also, Section III provides that "nonresponsive" material will be placed in "secure medium" in a "secure location." But securing this material as described does not cause it to lose its character of having been "seized."

A magistrate judge in the District of Columbia rejected a similar warrant that required Apple to disclose the entirety of three months' worth of e-mails but explained that only specific items relating to the investigation would be "seized." *Matter of the Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.,* 25 F. Supp. 3d 1, 6-7 (D.D.C. 2014). The judge determined that any material turned over to the government in response to a search warrant for electronic data is "unquestionably 'seized' within the meaning of the Fourth

HOEVET OLSON HOWES, PC
ATTORNEYS AT LAW
1000 S.W. BROADWAY, #1500
PORTLAND, OREGON 97205
(503) 228-0497

Amendment." *Id.* at 6-7, *citing Brower v. Cnty. of Inyo,* 489 U.S. 593, 596 (1989) (a "seizure" occurs when an object is intentionally detained or taken). The judge stated that the government's two-step process of obtaining and "seizing" only that evidence that related to the investigation amounted to an admission that the government did not have probable cause to obtain all e-mails. *Id.* at 6.

Also, because "Section I" describes the full scope of the "seizure," the timeframe limitation contained in Section II is without effect in narrowing the scope of the warrant. Section I describes all information to be disclosed by Facebook, and it is not limited by a window of time. It requires Facebook to turn over the entirety of the accounts listed in Attachment A, which itself is not limited by a timeframe. The timeframe in Section II does not narrow the scope of the warrant because, as discussed above, in reality, Section I, not Section II, defines what is "seized."[4]

The warrant also contains no narrowing function when it comes to "searching" the Facebook accounts. Section III requires law enforcement to segregate nonresponsive material, but of course, law enforcement personnel must *search* all data provided by Facebook in order to cull out the nonresponsive material. Also, the government informs us that the FBI forensic agents conducting this review are working for the prosecution team; they are not walled off like a filter team. For Fourth Amendment purposes, this process is the equivalent of a prohibited general rummaging into every Facebook file. *See Coolidge v. New Hampshire*, 403 U.S. 443, 467 (a warrant may not allow for a "general, exploratory rummaging in a person's belongings."); *see also Florida v*. *Wells*, 495 U.S. 1, 4 (1990) ("Our view that standardized criteria … or established routine … must regulate the opening of

[4] The face of the warrant itself rules out a meaningful distinction between what is "disclosed" by Facebook and what is "seized" by the government. Above the Section I heading of Attachment B is the subheading, "Particular Things *to Be Seized*." (Ex. B, page 4 of 8) (emphasis added).

HOEVET OLSON HOWES, PC
ATTORNEYS AT LAW
1000 S.W. BROADWAY, #1500
PORTLAND, OREGON 97205
(503) 228-0497

containers found during inventory searches is based on the principle that an inventory search must not be a ruse for a general rummaging in order to discover incriminating evidence.").

The warrant directs that nonresponsive material will not be "reviewed again" without a court order, but it will be retained for any one of the non-exclusive list of reasons provided in paragraph 6. These provisions, again, do not meaningfully narrow the scope of the warrant. It is no concession by that government to promise that it won't "review again" material deemed "nonresponsive," because, by definition, the government has no need for this material. Moreover, nothing prohibits the reviewing agents to take notes of the content of "nonresponsive" material. If the government later develops a need for the nonresponsive material as the case proceeds, it can use the information stored in the agents' minds or from their notes of the initial overbroad search to seek a court order to re-open it. In that case, if permitted, the ultimate use of the evidence originally labeled nonresponsive will be the fruit of the overbroad search.

Furthermore, the review for "responsive" information should not be regarded as a cure to the problem that the search warrant affidavit does not provide probable cause to search private Facebook messages. The fact that an agent might find evidence supporting the Conspiracy in a private communication solely between the user and a third party does not mean that the government had the requisite probable cause to search those private communications in the first place. This may seem an elementary point to make, but it is one that risks getting lost in the smokescreen of Section III which a casual reader might misconstrue as a check on overbreadth.

In several published opinions, magistrate judges, including some within the Ninth Circuit, have rejected as unreasonable the "seize first, search second" methodology described herein and have denied applications for search warrants for email and related data that are very similar to the overbroad Facebook warrant at issue here. *See, e.g.,*

HOEVET OLSON HOWES, PC
ATTORNEYS AT LAW
1000 S.W. BROADWAY, #1500
PORTLAND, OREGON 97205
(503) 228-0497

In re [REDACTED]@gmail.com, 62 F. Supp. 3d 1100, 1102 (N.D. Cal. May 9, 2014); *In the Matter of the Search of Information Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.*, 25 F. Supp. 3d 1 (D.D.C. March 7, 2014); *In the Matter of Applications for Search Warrants for Information Associated with Target Email Accounts/Skype 9 Accounts*, 2013 WL 4647554 at *8 (D. Kan. 2013); s*ee also In the Matter of the Search of Google Email Accounts*, 2015 WL 926619 (D. Alaska, March 3, 2015) (rejecting the government's promise that it would search Google material only within the date range for which it had probable cause; the warrant still authorized the government to seize and search the entire account without regard to time frame).

Defendants ask the Court to adopt the reasoning of these magistrates and find that Sections II and III do not cure the fact that the Facebook warrant authorizes an overbroad seizure and search of defendants' entire Facebook accounts. The narrowing effect of these provisions is illusory.

3. Total Suppression is the Appropriate Remedy

In some cases involving an overbroad warrant, the court can sever the infirm portions of the warrant from the valid portions, and thereby suppress evidence seized under the overbroad sections but not the valid parts. *See Andresen v. Maryland*, 427 U.S. 463, 482, n11 (1976). However, "severance is not always possible. If no portion of the warrant is sufficiently particularized to pass constitutional muster, then total suppression is required. * * * . Otherwise the abuses of a general search would not be prevented." *United States v. Cardwell*, 680 F.2d 75, 78 (9th Cir. 1982) (citation omitted). The severance doctrine requires "that identifiable portions of the warrant be sufficiently specific and particular to support severance." *Spilotro*, 800 F.2d at 967.

Severance is not available here to save some part of the warrant. As described above, Section I of Attachment B describes the full extent of what is seized from Facebook and what is searched. It is not narrowed by time frame, subject matter, or

HOEVET OLSON HOWES, PC
ATTORNEYS AT LAW
1000 S.W. BROADWAY, #1500
PORTLAND, OREGON 97205
(503) 228-0497

types of documents for which arguably there is probable cause. It is, at its core, a general warrant reviled by the Founders and expressly prohibited by the Fourth Amendment. Therefore, all evidence from the search must be suppressed.

Cardwell is instructive. The search warrant issued in the tax investigation directed the authorities to seize all "corporate books and records, including but not limited to" a long list of documents relating to the defendant's corporation. The court found the warrant was overbroad particularly in light of how the IRS investigation to date had focused on specific, identifiable parts of the defendant's business records. Addressing whether any part of the warrant could be saved, the Court held:

> "In this case even the most specific descriptions (checks, journals, ledgers, etc.) are fairly general. No time or subject matter limitations existed as to these items. Nor does the affidavit, even if properly relied upon to limit the scope of the warrant, provide the information needed to limit the general nature of the warrant. * * *. It does not refer to specific records, either in terms of their character or date. Thus, we do not have the information necessary to salvage any portion of the search. * * *. Therefore, all the materials seized under the defective warrant should be suppressed." *Cardwell*, 680 F2d at 78-79 (citations omitted).

Similarly, the Court in *United States v. Kow*, 58 F.3d 423 (9th Cir. 1995), upheld the suppression of all evidence seized from a business in a tax fraud case. Arguably, one category of evidence described in the warrant was not overbroad, but the Court ruled that "severance is not available when the valid portion of the warrant is a relatively insignificant part of an otherwise invalid search." *Kow*, 58 F3d at 428 (internal citations omitted). Also, the Court in *Spilotro* rejected the severance doctrine as a means to save part of the overbroad, non-particularized warrant. Some of the words used in the warrant to describe what could be seized were seemingly specific – *i.e.,* cash, scanning devices, and safe deposit box keys. But these items were not described in the context of any particular criminal activity and were simply "lumped in" with other categories of

HOEVET OLSON HOWES, PC
ATTORNEYS AT LAW
1000 S.W. BROADWAY, #1500
PORTLAND, OREGON 97205
(503) 228-0497

items. The items were not "set forth in textually severable portions," making severance inappropriate. *Spilotro*, 800 F2d at 968.

Based on these authorities, the warrant at issue in this case is not severable. Assuming the government had probable cause to obtain one or more parts of the Facebook accounts, these parts are "insignificant" compared to the parts for which there was no probable cause, as in *Kow.* Moreover, the task of severing out any valid part from the invalid parts of the warrant is rendered impossible by the affidavit's failure to describe where in each person's Facebook account the evidence for which there is probable cause might be found. The affidavit describes "postings," "links," and "shares," but it does not say where they were discovered. Therefore, the court cannot identify those parts for which there was probable cause on list of seized items in Section I in order to sever out and save them. Thus, all evidence obtained from Facebook must be suppressed.

4. The Government Cannot Claim Good Faith to Save the Search Because Reliance on a Patently Overbroad Warrant Was Objectively Unreasonable

Pursuant to *United States v. Leon*, 468 US 897, 926 (1984), evidence seized pursuant to a facially valid search warrant which later is held to be invalid may nevertheless be admissible if officers conducting the search acted in good faith and in reasonable reliance on the warrant. The government bears the burden of proving that reliance upon the warrant was objectively reasonable. *United States v. Michaelian*, 803 F2d 1042, 1048 (9th Cir. 1986). In *Leon,* the Court recognized that good faith would not apply to a warrant that 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." *Leon*, 468 US at 923. The extent of the overbreadth in this warrant rules out application of the good faith exception.

HOEVET OLSON HOWES, PC
ATTORNEYS AT LAW
1000 S.W. BROADWAY, #1500
PORTLAND, OREGON 97205
(503) 228-0497

In *Kow*, the Court stated that this Circuit has "been 'vigilant in scrutinizing officers' good faith reliance on such illegally overbroad warrants." *Kow*, 58 F3d at 428. The Court in *Kow* looked back to its decision in *United States v. Stubbs*, 873 F2d 210, 211 (9th Cir. 1989), which involved a facially overbroad warrant that contained a restriction regarding the dates of records to be seized. Despite that limiting feature, the Ninth Circuit still held that the agents could not reasonably rely on it. The warrant at issue in *Kow* was less particular than that in *Stubbs*. "Because the warrant in this case was facially invalid, no reasonable agent could have relied on it 'absent some exceptional circumstances.'" *Kow*, 58 F.3d at 428, *citing Center Art Galleries – Hawaii, Inc.*, 875 F.2d at 753. The Court repeatedly has rejected claims of good faith in the context of overbroad warrants. *See Center Art Galleries*, 875 F.2d at 753 ("We are unaware of any Ninth Circuit or Supreme Court case which has applied [the good faith exception] to a warrant approximating the degree of facial overbreadth which would preclude reasonable reliance."); *Spilotro*, 800 F.2d at 968 (*Leon* good faith exception does not apply to facially overbroad warrant); *United States v. Washington*, 782 F.2d 807, 819 (9th Cir. 1986) (overbroad warrants so facially deficient that reliance not reasonable); *United States v. Crozier*, 777 F.2d 1376, 1381-82 (9th Cir. 1985) (same).

The rule of particularity and specificity in warrants is not a hyper-technical court-made piece of Fourth Amendment jurisprudence. The rule against general warrants was a central concern of the Founders, and that is why they expressly made it part of the Fourth Amendment itself, to end a colonial practice that they found so pervasive and offensive. As Chief Justice Roberts wrote in *Riley,* "[o]pposition to such searches was in fact one of the driving forces behind the Revolution itself." *Riley*, 134 S Ct at 2494.

Any officer applying for a warrant to search a person's papers – whether in tangible or digital form – must be aware of this fundamental principle and cannot reasonably rely on a magistrate's approval to avoid suppression. There is nothing

HOEVET OLSON HOWES, PC
ATTORNEYS AT LAW
1000 S.W. BROADWAY, #1500
PORTLAND, OREGON 97205
(503) 228-0497

unique about seizures from electronic communication service providers, like Facebook, that would suggest this principle does not apply. In fact, in the face of (1) the heightened scrutiny that pertains to warrants for "books and papers" as per *Stanford*, (2) the Ninth Circuit cases discussed herein relating to overbreadth in computer searches, and (3) the express rejection by several magistrate judges across the country of warrants materially the same as the Facebook warrant at issue here, the government cannot rely on the good faith exception to avoid suppression.

Conclusion

The Court must grant this motion to suppress, because the Facebook warrant is overbroad in violation of the Fourth Amendment, and the good faith exception does not apply.

HOEVET OLSON HOWES, PC

DATED: 06/20/2016

s/ Per C. Olson
Per C. Olson, OSB 933863
Attorney for Defendant David Fry

HOEVET OLSON HOWES, PC
ATTORNEYS AT LAW
1000 S.W. BROADWAY, #1500
PORTLAND, OREGON 97205
(503) 228-0497