Lisa Hay
Federal Public Defender
Rich Federico
Assistant Federal Public Defender
101 SW Main Street, Suite 1700
Portland, Oregon 97204
(503) 326-2123 Telephone
(503) 326-5524 Facsimile
Lisa_Hay@fd.org
Rich_Federico@fd.org
Attorneys for Defendant Ryan Payne

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF OREGON

UNITED STATES OF AMERICA,	**Case No. 3:16-cr-00051-BR**
Plaintiff,	**DEFENDANT RYAN PAYNE'S MOTION TO SUPPRESS DROPBOX EVIDENCE**
v.	
RYAN PAYNE,	
Defendant.	

Pursuant to Fed. R. Crim. P. 12(b)(3)(C), defendant Ryan Payne, through Federal Public Defender Lisa Hay and Assistant Federal Public Defender Rich Federico, respectfully moves this Court to suppress all evidence obtained from the government's illegal search of a Dropbox account associated with Mr. Payne. The warrant authorizing the search and seizure violated the particularity requirement of the Fourth Amendment. The warrant was also issued by a magistrate judge in the District of Nevada to search and seize information located in San Francisco, California, in violation of Fed. R. Crim. P. 41 and 28 U.S.C. § 636(a). Suppression is required of all evidence obtained or derived from the Dropbox account associated with Mr. Payne.

RELIEF REQUESTED: That the Court suppress any and all evidence obtained from the search of the Dropbox account associated with Ryan Payne, including any and all evidence derived therefrom.

CERTIFICATION OF CONFERRAL: Defense counsel conferred with Assistant United States Attorney Geoffrey Barrow regarding this motion. The government opposes the requested relief.

STATEMENT OF FACTS

Dropbox, Inc. is an online file hosting service that allows individuals or businesses to store digital files on remote servers, synchronize those files to multiple computing devices so that the same files appear on all devices, and share those files with other individuals or businesses. Dropbox, Inc. is based in San Francisco, California, and the company advertises itself as follows: "Get to all your files from anywhere, on any device, and share them with anyone." Dropbox "About Us," https://www.dropbox.com (accessed July 9, 2016). This motion to suppress relates to a warrant that the Federal Bureau of Investigations obtained from a Magistrate Judge in the District of Nevada to search and seize any and all files "associated with Dropbox User No. 328858080 (Online Account to Be Searched) associated with Ryan Payne."

On March 31, 2016, the FBI submitted an Affidavit of Joel P. Willis in Support of an Application for a Search Warrant to the Hon. Nancy J. Koppe, Magistrate Judge of the United States District Court for the District of Nevada ("Nevada Warrant").[1] The affidavit and its attachments sought "any messages, records, files, logs, or information that have been deleted but are still available to Dropbox," including "all documents, digital files, audio files, images, and videos," from the Dropbox account. The warrant that issued authorized the government to search

[1] The Affidavit of Joel P. Willis in Support of an Application for a Search Warrant, the Search and Seizure Warrant, and the Return of Service are hereby filed Under Seal and incorporated as Exhibit 1 to this motion. These documents are under seal in the District of Nevada. The government has not provided the defense with a copy of the Application for Warrant, if one exists apart from the Affidavit of Joel P. Willis. The defense reserves the right to supplement this motion upon receipt of any Application.

and seize information associated with Dropbox Account No. 328858080, which was described as being stored at the premises owned, maintained, controlled, or operated by Dropbox, Inc. at 185 Berry Street, Suite 400, San Francisco, California.

The warrant ostensibly targeted information related to Mr. Payne's involvement in an "armed standoff" in Nevada in April of 2014 and subsequent involvement in a protest at the Malheur National Wildlife Refuge. The warrant also sought evidence that Mr. Payne was planning "additional actions against law enforcement and the federal government" with individuals associated with the group Operation Mutual Defense ("OMD"). *See* Ex. 1, Affidavit in Support of Warrant at p. 29. Attachment B, Section III of the warrant listed twelve categories of items to be seized. *See* Ex. 1, Search Warrant, Attachment B at pp. 38-40. Despite listing those twelve categories, the plain language of the warrant authorized the FBI to obtain from Dropbox and search through the *entirety* of the account associated with Mr. Payne without limitation. *See* Ex. 1, Search Warrant, Attachment B at pp. 37-38. The warrant likewise required Dropbox to provide the government with information on who accessed any Dropbox content, how it was accessed, and when it was accessed, among other information. The warrant failed to establish a search protocol governing how relevant data would be sorted from irrelevant data or how investigating agents would be screened from irrelevant data.

The warrant was executed on April 1, 2016, and the FBI acquired all information associated with Dropbox Account No. 328858080 associated with Ryan Payne from August 18, 2014 to the present (including any data that had been deleted but was still accessible). The government has indicated in conversations with defense counsel that it intends to offer evidence obtained from Dropbox against Mr. Payne at trial, including audio, video, and other written information.

ARGUMENT

The Government's search of Mr. Payne's Dropbox account violated the Fourth Amendment. The warrant on which the search was based lacked sufficient particularity and failed to control and limit what information agents obtained and which agents and prosecutors accessed irrelevant data. The warrant also exceeded the jurisdictional powers of magistrate judges under Fed. R. Crim. P. 41 and 28 U.S.C. § 636(a), which confine a magistrate judge's authority to issue a search warrant solely to a location within the judicial district itself, with minor exceptions not applicable to the present scenario. The Court should suppress any and all information seized through the Dropbox warrant—and any investigative fruits derived therefrom.

I. The Dropbox Warrant Violated the Fourth Amendment's Particularity Requirement.[2]

The Fourth Amendment requires that warrants "particularly describe[e] the place to be searched, and the persons or things to be seized." U.S. Const., Amend. IV. Compelling an entity such as Dropbox to turn over an individual's digital documents, messages, audio files, and video files triggers the Fourth Amendment's protections. *See, e.g., Riley v. California*, 134 S.Ct. 2473, 2493 (2014) (rejecting Fourth Amendment analysis that would distinguish between digital and physical property); *United States v. Cotterman*, 709 F.3d 952, 957 (9th Cir. 2013) (en banc) (noting Fourth Amendment applies to digital form of "papers"). The "clear and precise words" of the Fourth Amendment "reflect the determination of those who wrote the Bill of Rights that the people of this new Nation should forever 'be secure in their persons, houses, papers, and effects' from intrusion and seizure by officers acting under the unbridled authority of a general warrant."

[2] There is significant overlap between the defects which appear in the Dropbox warrant and the defects detailed in Docket No. 711, Ryan Payne's Motion to Suppress Facebook Evidence (6/15/16). The arguments made in Docket No. 711 are incorporated herein by reference.

Stanford v. State of Texas, 379 U.S. 476, 481 (1965). It is the particularity requirement that is supposed to provide protection against general warrants, *Maryland v. Garrison*, 480 U.S. 79, 84 (1987), by prohibiting "general, exploratory rummaging in a person's belongings." *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971).

The Dropbox warrant in this case failed to state with any meaningful particularity which of the account's contents were subject to search and how only relevant contents would be seized—making the warrant itself akin to a general warrant and the process created by the warrant akin to the "seize first, search second" methodology rejected as unreasonable in *In re [REDACTED]@gmail.com*, 62 F. Supp. 3d 1100, 1102 (N.D. Cal. May 9, 2014). The manner in which the government proposed to search was to compel Dropbox to provide the entirety of the account's contents from August 2014 to the present (but potentially including material created before August 2014) to the government, and then to allow the government search the accounts for items relating to specified criminal activity without any particular search protocol authorized in advance by the Court. Similar procedures have been rejected:

> [This procedure] is best analogized to a warrant asking the post office to provide copies of all mail ever sent by or delivered to a certain address so that the government can open and read all the mail to find out whether it constitutes fruits, evidence or instrumentality of a crime. The Fourth Amendment would not allow such a warrant and should therefore not permit a similarly overly broad warrant just because the information sought is in electronic form rather than on paper.

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); *see also 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. 2014) ("having an electronic communication service provider perform a search, using a methodology based on search terms such as date stamps, specific words, names of recipients, or other methodology suggested by the government and

approved by the Court seems to be the only way to enforce the particularity requirement commanded by the Fourth Amendment.").

The Fourth Amendment violation resulting from the search and seizure of Mr. Payne's Dropbox account is particularly egregious because the warrant imposed no requirement on the government to follow any screening protocol in order to prevent the exposure to the government of the entire content of Mr. Payne's Dropbox account, no matter how personal or how unrelated that content might be to the allegations at issue in this case. *Cf. U.S. v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1180 (9th Cir. 2010) (en banc) ("Segregation and redaction of electronic data must be done either by specialized personnel or an independent third party. If the segregation is to be done by government computer personnel, the government must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant.") (concurring opinion of Kozinski, C.J.) (citations omitted). The Dropbox warrant simply allowed agents to rummage through the entirety of Mr. Payne's Dropbox account and then either return, destroy, or seal whatever evidence was deemed unrelated. *See* Attachment B, p. 40.[3] Based on these legal principles and the facts to be further adduced at a hearing, the Court should suppress all content obtained through the unconstitutional mechanism of the Dropbox warrant.

II. The Dropbox Warrant Violated Rule 41 and 28 U.S.C. § 636(a).[4]

The issuance of the Dropbox warrant violated the jurisdictional limits of Fed. R. Crim. P. 41 and 28 U.S.C. § 636(a) by permitting Nevada agents to conduct a search in San Francisco,

[3] As in Doc. 711, the defense reserves the right to brief additional issues related to the Dropbox warrant following an evidentiary hearing on the search and seizure.

[4] The same arguments made against the Facebook warrants in Doc. 710, Defendant Ryan Payne's Motion to Suppress Facebook Evidence (6/15/16) apply to the Dropbox warrant at issue here. Those arguments are incorporated herein by reference.

California. Rule 41 does not permit a magistrate judge in Nevada to authorize the search of property located in California. Instead, Rule 41 cabins a magistrate judge's authority to issue a warrant to five specific circumstances, none of which is present here. Therefore, the warrant is unlawful. *See In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 757 (S.D. Tex. 2013) (hereinafter "In re Warrant") ("Under the Government's theory, because its agents need not leave the district to obtain and view the information gathered from the Target Computer, the information effectively becomes 'property located within the district.' This rationale does not withstand scrutiny."); *United States v. Levin*, — F. Supp. 3d —, 2016 WL 2596010, at *15 n. 13 (D. Mass. May 5, 2016) (invalidating NIT warrants issued by a magistrate judge for software to be implanted in computers in an unknown location outside of the state).

Similar to Rule 41, the Federal Magistrate Act generally limits the reach of a magistrate judge's orders to the territory in which the magistrate sits. 28 U.S.C. § 636 (outlining the geographical scope of a magistrate judge's power: (1) "within the district in which sessions are held by the [district] court that appointed the magistrate judge," (2) "at other places where that [district] court may function," and (3) "elsewhere as authorized by law"); *see also Krueger*, 809 F.3d at 1118 (Gorsuch, J., concurring) (emphasizing that a violation of Rule 41(b)'s territorial limitations also implicates the statutory limitation of Section 636).

In response to Mr. Payne's suppression motion regarding a similarly defective warrant for emails, the government argued that 18 U.S.C. § 2703 authorized the Nevada Magistrate Judge to issue warrants for material stored in California. The defense expects the government to raise a similar argument here. Section 2703 does indeed allow the government to seek warrants from "courts of competent jurisdiction" commanding providers of electronic communications or remote

computing services to disclose "the contents of wire or electronic communication[s]."[5] 18 U.S.C. § 2711(3)(A) defines "court of competent jurisdiction" as "any district court of the United States (including a magistrate judge of such court)" but also requires the issuing court to have "jurisdiction over the offense being investigated." Magistrate judges may not preside over the trial of felony criminal cases. 28 U.S.C. § 636(a)(3). And, while district court judges may designate magistrate judges to handle certain pretrial matters under 28 U.S.C. § 636(b), upon information and belief there was no such order in place at the time the Drobox warrant was sought or issued. *See* Ex. 1, Search Warrant, Attachment B at 37 (felonies alleged). The clear jurisdictional confines of Rule 41 and Section 636(a) govern, and the warrant was issued beyond the geographical limitations of the magistrate judge's authority. Because the Dropbox warrant was issued without appropriate jurisdictional authority, it is void ab initio. *See, e.g.*, *United States v. Krueger*, 809 F.3d 1109, 1126 (10th Cir. 2015) (Gorsuch, J., concurring) ("The government asks us to resolve but one question, bold as it is: whether a warrant issued in defiance of positive law's jurisdictional limitations on a magistrate judge's powers remains a warrant for Fourth Amendment purposes. I would not hesitate to answer that question put to us and reply that a warrant like that is no warrant at all.").

As this Court is aware, the exclusionary rule is properly applied to cases involving "deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." *Herring v. United States*, 129 S. Ct 695, 702 (2009). When the government violates Rule 41 and Section 636 and the defendant is prejudiced by that violation, the remedy is to suppress all evidence resulting from the illegality. *See United States v. Burgos-Montes*, 786 F.3d 92, 109

[5] The defense does not concede that digital files stored in Mr. Payne's Dropbox account constitute wire or electronic communications. The defense reserves the right to explore this issue at an evidentiary hearing where Dropbox employees may be examined.

(1st Cir.), cert. denied, 136 S. Ct. 599 (2015); *United States v. Schoenheit*, 856 F.2d 74, 76–77 (8th Cir. 1988); *United States v. Burke*, 517 F.2d 377, 386–87 (2d Cir. 1975) (reasoning that rule violations should only lead to suppression where "(1) there was prejudice in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed or (2) there is evidence of an intentional and deliberate disregard" for the rule by the government); *see also United States v. Radlick*, 581 F.2d 225, 228 (9th Cir. 1978) (same). Mr. Payne is prejudiced by the violation due to the intentional and deliberate disregard for the jurisdictional limitations of Rule 41 and Section 636(a). In addition, the exclusionary rule reaches not only primary evidence obtained as a direct result of an illegal search or seizure, *see Weeks v. United States*, 232 U.S. 383 (1914), but also evidence later discovered and found to be derivative of an illegality, or "fruit of the poisonous tree." *Nardone v. United States*, 308 U.S. 338, 341 (1939). All fruits gained from the Dropbox warrant are now poisonous and must be suppressed.

III. The Good Faith Exception Does Not Apply Because the Warrants Were Void Ab Initio.

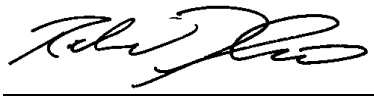
A good faith exception to an otherwise unlawful search and seizure may apply if the executing officers act in objectively reasonable reliance on the warrant's validity. *See United States v. Leon*, 468 U.S. 897 (1984). The Supreme Court observed that "[r]easonable minds frequently may differ on the question whether a particular affidavit establishes probable cause, and we have thus concluded that the preference for warrants is most appropriately effectuated by according great deference to a magistrate judge's determination." *Id*. at 914 (internal quotation marks and citations omitted). However, *Leon* does not extend the same deference when magistrate judges determine their own jurisdiction. *See Levin*, 2016 WL 2596010, at *10. In other words, the *Leon* good faith exception has been applied to warrants invalidated for lack of probable cause but not to warrants void for lack of jurisdiction. *Id*. at *10, n.17 (collecting cases where courts have

held that when a warrant is issued without jurisdiction, there is no need to conduct a good faith analysis). To apply the good faith exception to these facts would collapse the distinction between "judicial error"—where mistakes of sufficiency or misunderstanding statutory requirements might warrant a good faith exception if the public interest outweighs the violation—and "judicial authority"—where a judge acts outside of his or her authority altogether. *Id*. at *12.

CONCLUSION

The Dropbox warrant at issue in this motion authorized the government to obtain and rummage through the entirety of a Dropbox account associated with Mr. Payne, seizing information ostensibly related to the crimes he was suspected of having committed. The search and seizure of Mr. Payne's Dropbox account was overbroad and violated the particularity requirement of the Fourth Amendment. In addition, the warrant was issued by a magistrate judge without the jurisdictional authority to allow the government to search and seize material stored and controlled by a company in California and was, therefore, void ab initio. Mr. Payne respectfully requests that the Court suppress all of the evidence obtained through or derived from the illegal search and seizure of his Dropbox account.

Respectfully submitted this 11th day of July, 2016.



Rich Federico
Assistant Federal Public Defender

Lisa Hay
Federal Public Defender

Attorneys for Defendant Ryan Payne