

Lisa Hay  
Federal Public Defender  
Rich Federico  
Assistant Federal Public Defender  
101 S.W. 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  
PORTLAND DIVISION**

**UNITED STATES OF AMERICA,**

**Case No. 3:16-cr-00051-BR**

**Plaintiff,**

**DEFENDANT RYAN PAYNE'S  
MOTION TO SUPPRESS  
FACEBOOK 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 his Facebook account. Search warrants were obtained in the Districts of Nevada and Oregon to search information located in 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 Facebook pursuant to search warrants that were void ab initio.

**RELIEF REQUESTED:** That the Court suppress any and all evidence obtained from the Facebook account of Ryan Payne, including any and all evidence derived therefrom.

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

### **STATEMENT OF FACTS**

In a letter dated June 6, 2016, the government provided notice in its “Factual Summary” that it intends to offer evidence obtained from Facebook and social media against Mr. Payne at trial. The government previously provided in discovery information obtained from Mr. Payne’s Facebook account and the search warrants issued and executed to acquire this information, as follows:

**A. Search Warrant Obtained in Nevada and Executed in Menlo Park, California.**

On December 1, 2015, the FBI submitted an Application for Search Warrant to the United States District Court for the District of Nevada (“Nevada Warrant”).<sup>1</sup> The application sought all information for the Facebook Account of Ryan Payne, Facebook User ID 100007711530105 that is stored at a premises controlled by Facebook, Inc., a company headquartered in Menlo Park, California. The Nevada Warrant was signed the same day by the Honorable George Foley, Jr., U.S. Magistrate Judge for the District of Nevada. The Nevada Warrant specifically provided authority to search the location of the premises owned, maintained, controlled, or operated by Facebook, Inc. at Menlo Park, California. The Nevada Warrant was executed on December 3, 2015, and acquired all information associated with User ID 100007711530105 for Ryan Payne from June 1, 2014 to present.

---

<sup>1</sup> The Nevada Warrant and Application for Warrant with supporting affidavit are hereby filed Under Seal and incorporated as Attachment A to this motion.

**B. Search Warrant Obtained in Oregon and Executed at Menlo Park, California.**

On April 8, 2016, the FBI submitted an Application for Search Warrant to the U.S. District Court, for the District of Oregon (“Oregon Warrant”).<sup>2</sup> The application sought information from several Facebook IDs, including the one for Ryan Payne and other co-defendants, stored at premises controlled by Facebook in Menlo Park, California. The Oregon Warrant was signed the same day by the Honorable Paul Papak, U.S. Magistrate Judge for the District of Oregon. The Oregon Warrant specifically provided the FBI authority to search property located in the Northern District of California, or to search the location of the premises owned, maintained, controlled, or operated by Facebook, Inc. at Menlo Park, California. The Oregon Warrant was limited in duration to be executed on or before April 23, 2016. The Oregon Warrant was executed on April 11, 2016, with two computer disks of data provided to defense counsel on May 16, 2016.

**ARGUMENT**

The Government’s search of the Facebook account of Mr. Payne violated the jurisdictional powers of magistrate judges under Fed. R. Crim. P. 41 and 28 U.S.C. § 636(a). These authorities allow a magistrate judge to issue a search warrant *only* for a location within the judicial district itself, with minor exceptions not applicable to the present scenario. These restrictions are not ministerial technicalities. Rather, Rule 41 and Section 636(a) serve as a critical line of protection against nationwide searches, like what occurred here. Suppression of all evidence seized from Facebook is required because the magistrate judges in Nevada and Oregon did not have jurisdiction to issue the respective warrants to search property located in Menlo Park, California. Thus, both the Nevada Warrant and the Oregon Warrants were void ab initio. *See, e.g., United States v.*

---

<sup>2</sup> The Oregon Warrant, Application for Warrant with supporting affidavit are hereby filed Under Seal and incorporated as Attachment B to this motion.

*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.”).

**A. The Nevada and Oregon Warrants Violated Rule 41.**

The Nevada and Oregon Warrants violated the jurisdictional limits of Fed. R. Crim. P. 41 by permitting government agents to conduct a borderless search in Menlo Park, California. In short, Rule 41 does not permit a magistrate judge in Nevada or Oregon to authorize the search of property located in California; rather, it provides authority to issue a warrant in five specific circumstances:

(b) Authority to Issue a Warrant. At the request of a federal law enforcement officer or an attorney for the government:

(1) a magistrate judge with authority in the district—or if none is reasonably available, a judge of a state court of record in the district—has authority to issue a warrant to search for and seize a person or property *located within the district*;

(2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property *outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed*;

(3) a magistrate judge—in an investigation of domestic terrorism or international terrorism—with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;

(4) a magistrate judge with authority in the district has authority to issue a warrant *to install within the district a tracking device*; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and

(5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for

property that is located outside the jurisdiction of any state or district, *but within any of the following*:

- (A) a United States territory, possession, or commonwealth;
- (B) the premises—no matter who owns them—of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission’s purposes; or
- (C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

(emphasis added). The warrants issued were not authorized under any of these sections and are 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”).

In *In Re Warrant*, the government sought a warrant from the magistrate judge to search a “Target Computer” with whereabouts unknown. The government argued that the search warrant was valid and complied with the territorial limits of Rule 41 because the contents of the computer’s information would first be reviewed in the district where the warrant issued. *Id.* at 756. The court squarely rejected the government’s argument. *Id.* (“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.”). Roughly five months after *In Re Warrant*, the Department of Justice sought a modification to Rule 41 that would allow law enforcement to obtain warrants to hack computers in unknown locations. *See United States v. Levin*, — F. Supp. 3d —, 2016 WL 2596010, at \*15 n. 13 (D. Mass. May 5, 2016) (noting comments from the Department of Justice to Hon. Reena Raggi on Sept. 18, 2013, requesting a rule change which would add a new Rule 41 subsection);<sup>3</sup> *see also* Letter from Assistant Attorney General Mythili Raman to Hon. Reena Raggi

---

<sup>3</sup> A variety of professors, media outlets, and non-profit organizations have levied harsh criticisms at the government’s proposed amendments because they “will provide law enforcement

(Sept. 18, 2013) (containing the actual comments from the Department of Justice requesting the amendment to Rule 41 in order “to update the provisions relating to the territorial limits for searches of electronic storage media”) (available online at <http://www.uscourts.gov/rules-policies/archives/suggestions/hon-mythili-raman-13-cr-b>).

The United States Supreme Court ultimately approved an amendment to Rule 41, which will take effect on December 1, 2016. Absent contrary Congressional action, the amendment will grant magistrate judges the “authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district.” *See* Letters from Chief Justice John Roberts to Paul D. Ryan and Joseph R. Biden, Jr. (April 28, 2016) (with copies of the Rule 41 amendment approved by the Supreme Court) (available online at: [http://www.supremecourt.gov/orders/courtorders/frcr16\\_mj80.pdf](http://www.supremecourt.gov/orders/courtorders/frcr16_mj80.pdf)). The Rule 41 amendment will only increase the authority of magistrate judges in limited circumstances that are not applicable here—i.e. where (1) “the district where the media or information is located has been concealed through technological means” or (2) in limited computer fraud hacking cases covering five or more districts. *Id.* The amendment will shore up the jurisdictional footing of future magistrate-issued warrants like that found in the *Levin* case (i.e. in scenarios where the location of electronic data is concealed) but will have no impact whatsoever on other magistrate-issued warrants like those relevant here (i.e. where the government knows the location of data no one has attempted to conceal). Nevertheless, at the time the warrants were issued for the contents of Mr. Payne’s Facebook account, the government knew about the territorial limitations of magistrate

---

agencies with mechanisms to bypass the Fourth Amendment and lead to a circumvention of other legal oversight regimes.” Zach Lerner, *A Warrant to Hack: An Analysis of the Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure*, 18 Yale J. L. & Tech. 26, 29 (2016).

judges but did not seek a warrant from either a California magistrate or a Nevada or Oregon Article III judge. The Oregon and Nevada Facebook warrants were thus issued in violation of Rule 41.<sup>4</sup>

**B. The Issuance of the Warrants Violated 28 U.S.C. § 636(a).**

The Nevada and Oregon warrants also violated the Federal Magistrate Act (28 U.S.C. § 636), which generally limits the reach of a magistrate judge's orders to the territory in which the magistrate sits. *See 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). Section 636(a) outlines 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." None of Section 636(a)'s geographical descriptions can rescue the deficiencies in the warrants at issue here, as the Nevada and Oregon warrants sought property held outside of Nevada and Oregon. Nothing would have prevented the government from seeking warrants from a U.S. District Court Judge, which would have made the Section 636 statutory argument inapposite. Likewise, nothing would have prevented the government from seeking authorization from a magistrate judge in the Northern District of California. The government's choice to seek authority from courts without jurisdiction rendered the Nevada and Oregon Warrants void ab initio.

---

<sup>4</sup> The Stored Communications Act does not rescue the deficiencies in the warrants the government obtained, as that statute is also limited by the territorial limitation of Rule 41 and the regular powers of a "court of competent jurisdiction." *See* 18 U.S.C. 2703(a) ("[P]ursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure ... by a court of competent jurisdiction.").

**C. The Evidence Obtained from Facebook in Violation of Rule 41 and Section 636(a) Should be Suppressed.**

Despite knowing the limitations of magistrate judges' geographical authority, the government sought the warrants at issue from magistrate judges in Nevada and Oregon—and not in California. Suppression of all information is required because the search warrants issued to Facebook violated Rule 41 and Section 636(a). 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 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 (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).

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); *see also United States v. Shetler*, 665 F.3d 1150 (9th Cir. 2011). As the Nevada and Oregon Warrants that permitted a search of information on Facebook



servers in California were void ab initio, all fruits gained therefrom are now poisonous and must be suppressed.

**D. 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, as the *Levin* court noted, *Leon* does not extend the same deference when magistrate judges determine their own jurisdiction. *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 FBI and DOJ were on notice that Rule 41 and Section 636(a) contained territorial limitations when they obtained the Nevada and Oregon Warrants to search and seize evidence they knew to be located in Menlo Park, California. As the magistrate judges lacked jurisdiction to issue warrants for property in California, the underlying Facebook Warrants were void ab initio. All Facebook evidence, or evidence derived from the Facebook account, must be suppressed.

Respectfully submitted this 15th day of June, 2016.



---

Lisa Hay  
Federal Public Defender

Rich Federico  
Assistant Federal Public Defender

Attorneys for Defendant (Payne)