IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ARIZONA

In the Matter of the Search of, Yahoo, Incorporated 701 First Avenue Sunnyvale, California 94089	No. 07-3194-MB **ORDER**

This matter is before the Court on the motion of the United States for an order authorizing an out-of-district search warrant for the contents of electronically-stored communications pursuant to Title 18 U.S.C. § 2703(a).

I. Background

The United States asserts that on February 23, 2006, an unidentified individual obtained unauthorized access to a United States government computer (the "victim computer"), located in Yuma, Arizona, which is the property of a governmental agency. A forensic examination revealed that the unauthorized individual exfiltrated a text file from the victim computer to an e-mail address, xxxx_xxx@yahoo.com[1] (the "unauthorized e-mail account").

[1] Obviously, this is not the actual email address and is used to protect the pending criminal investigation.

The Government has subpoenaed Yahoo, Inc.'s ("Yahoo") records which indicate that the user is accessing the unauthorized e-mail account from computers assigned internet protocol ("IP") addresses in a southeastern European country.[2] On December 15, 2006 and March 9, 2007, the Government issued requests to Yahoo pursuant to Title 18 U.S.C. § 2703(f)[3] to preserve existing records associated with the unauthorized e-mail account pending issuance of more formal legal process. The Government contends that the Yahoo computer servers located in Sunnyvale, California contain data, including stored electronic mail communications, for a particular subscriber associated with the unauthorized e-mail account.

On May 8, 2007, the Government filed a motion seeking an out-of-district search warrant pursuant to Title 18 U.S.C. § 2703(a) to search and seize electronic information, including electronically-stored communications, associated with the unauthorized e-mail account stored on computer servers located in Sunnyvale, California. The Court granted that motion, issued the search warrant and now explains its ruling.

The question presented is whether the District Court of Arizona may properly issue a search warrant ordering the search and production of electronic evidence pursuant to § 2703(a) where the warrant is directed to an out-of-district internet service provider located in California.

II. Analysis

The relevant statute, Title 18 U.S.C. § 2703(a), provides, in pertinent part, that:

> A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued *using the*

---

[2] The Electronic Communications Privacy Act ("ECPA"), Title 18 U.S.C. §§ 2701-2712, permits the Government to compel production of certain types of information, including basic user information, using a subpoena. Title 18 U.S.C. § 2703(c)(2).

[3] To minimize the risk that electronic information will be lost, Title 18 U.S.C. § 2703(f) permits the Government to direct network service providers to preserve records pending the issuance of compulsory legal process. Title 18 U.S.C. § 2703(f).

> *procedures described in* the Federal Rules of Criminal Procedure *by a court with jurisdiction over the offense under investigation* or equivalent State warrant.

Id. (emphasis added). The Government argues that this provision authorizes this Court to issue a warrant to search and seize contents of electronically-stored communications which are contained on Yahoo's computer servers in Sunnyvale, California. As discussed below, the Court agrees that § 2703(a) grants this Court such authority.

A. Statutory Interpretation

In interpreting a statute, federal courts "'look first to the plain language of the statute, construing the provisions of the entire law, including its object and policy, to ascertain the intent of Congress.'" *United States v. Hockings*, 129 F.3d 1069, 1071 (9th Cir. 1997) (quoting *Northwest Forest Resource Council v. Glickman*, 82 F.3d 825, 830 (9th Cir. 1996)). If the provision is ambiguous, the court looks to legislative history. *Id.* Statutory language is ambiguous if it is capable of being understood by reasonably well-informed people in two or more different ways. *United States v. Quarrell*, 310 F.3d 664, 669 (10th Cir. 2002).

It is "a fundamental canon that the words of a statute must be read in their context and with a view to their place in the overall statutory scheme." *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 133 (2000) (quoting *Davis v. Michigan Dep't of Treasury*, 489 U.S. 803, 809 (1989)). If necessary to discern Congress' intent, the court may read statutory terms in view of the purpose of the statute. The structure and purpose of a statute may also provide guidance in determining the plain meaning of its provisions. *K-Mart Corp. v. Cartier, Inc.*, 486 U.S. 281, 291 (1988) ("In ascertaining the plain meaning of [a] statute, the court must look to the particular statutory language at issue, as well as the language and design of the statute as a whole."); *United States v. Lewis*, 67 F.3d 225, 228-29 (9th Cir.1995) ("Particular phrases must be construed in light of the overall purpose and structure of the whole statutory scheme."). To determine Congress' intent in enacting a statute, courts may also consult a variety of sources including rules of statutory construction

and interpretation, and extrinsic information such as the statute's expressed purpose, discussions in committee reports, accepted and rejected amendments, and statements made in congressional floor debates. *U.S. v. McNab*, 331 F.3d 1228, 1238 (11th Cir. 2003).

Federal courts are advised to avoid interpreting a statute in such a way that renders a word or phrase redundant or meaningless. *Gustafson v. Alloyd Co., Inc.*, 513 U.S. 561, 562 (1995); *Kungys v. United States*, 485 U.S. 759, 778 (1988). Such courts should also presume that when Congress alters the words of a statute, it does so with an intent to change the statute's meaning. *U.S. v. Wilson*, 503 U.S. 329, 336 (1992). Mindful of these rules of statutory interpretation, the Court will consider the meaning, scope and limitations of § 2703(a).

B. Title 18 U.S.C. § 2703(a)

The issue before the Court requires analysis of § 2703(a), as amended by Section 220 of the Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism Act of 2001, PL 107-56 (HR 3162)(the "USA Patriot Act"). Before amendment by the USA Patriot Act in 2001, § 2703(a) provided that:

> A governmental entity may require the disclosure by a provider of electronic communications service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communication system for one hundred and eighty days or less, only pursuant to a warrant issued *under* the Rules of Criminal Procedure or equivalent State warrant.

18 U.S.C. § 2703 (1998) (emphasis added), amended by PL 107-56 (HR 3162), 2001.

Section 220 of the USA Patriot Act, entitled "Nationwide Service of Search Warrants for Electronic Evidence," amended § 2703(a) so it now provides that:

> A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant *issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation* or equivalent State warrant.

Title 18 U.S.C. § 2703(a) (emphasis added), as amended by PL 107-56 (HR 3162), 2001.

Section 220 of the Patriot Act made two changes to § 2703(a). First, search warrants may now be issued "*using the procedures described in* the Federal Rules of Criminal Procedure," rather than "*under*" those Rules. Second, search warrants may now be issued "by a court with jurisdiction over the offense." Title 18 U.S.C. § 2703(a). The Court will now analyze the meaning of these two statutory phrases.

1. "Jurisdiction over the Offense"

The Court first considers the meaning of the phrase "jurisdiction over the offense" as used in § 2703(a). The Supreme Court has recently noted that "[j]urisdiction is a 'word of many, too many, meanings.'" *Rockwell International Corp. v. United States*, ___ U.S.___, 127 S.Ct. 1397, 1405 (2007) (quoting *Steel Co. v. Citizens for Better Environment*, 523 U.S. 83 (1998)). Section 2703(a) does not specify whether Congress intended the word "jurisdiction" to mean subject-matter, personal, or territorial jurisdiction.

The issue *sub judice* appears to be an issue of first impression in the Ninth Circuit. In view of the lack of any controlling or persuasive case law in the Ninth Circuit discussing § 2703(a), the Court looks outside the Ninth Circuit to a District of Florida decision which held that § 2703(a) authorizes a federal district court where the crime allegedly occurred to issue out-of-district warrants for the seizure of stored electronic communications. *In Re Search Warrant*, 19 Fla.L.Weekly Fed. D. 309 at 13, No. 6:05-MC-168-Orl-31JGG (M.D. Fla, Dec. 23, 2005). Although this not a published order, it reversed a magistrate judge's published order that declined to authorize an out-of-district search warrant that sought to seize electronic data maintained by a "dot-com" web site located in the Northern District of California. See, *In Re: Search Warrant*, 362 F.Supp.2d 1298 (M.D. Fla. 2003).

The Court agrees with the district judge's conclusion in *In Re Search Warrant*, 19 Fla.L.Weekly Fed. D. 309 at 13, No. 6:05-MC-168-Orl-31JGG (M.D. Fla, Dec. 23, 2005), that Congress intended "jurisdiction" to mean territorial jurisdiction. Title 18 U.S.C. § 3231 gives federal district courts original subject matter jurisdiction over all violations of federal

law. Title 18 U.S.C. § 3231 (stating that "district courts of the United States shall have original jurisdiction, exclusive of the courts of the States, of all offenses against the laws of the United States."). Because all federal courts have subject-matter jurisdiction over violations of federal law, interpreting jurisdiction to mean "subject-matter jurisdiction" would render these words meaningless and contrary to the rule of statutory construction that a statute should "be so construed that, if it can be prevented, no clause, sentence, or word shall be superfluous, void, or insignificant." *TRW Inc. v. Andrews*, 534 U.S. 19, 31 (2001).

Federal district courts have territorial jurisdiction over those crimes that occur in their district. *U.S. v. Schiefen*, 139 F.3d 638, 639 (8th Cir. 1998). Concluding that "jurisdiction" means territorial jurisdiction is consistent with the legislative history of the USA Patriot Act. Legislative history of the USA Patriot Act indicates that Congress intended that amendments made by the Patriot Act to apply to "all types of criminal and foreign intelligence investigations." 147 Cong.Rec. S10990-02 at S10991, 107 Congress, 1st Session, October 25, 2001, 2001 WL 1297566. The legislative history indicates that Section 220 of the USA Patriot Act, "'Nationwide Service of Warrants for Electronic Evidence' - permits a single court having jurisdiction over the offense to issue a search warrant for e-mail that would be valid anywhere in the United States." 147 Cong.Rec. H7159-03 at H7197-98, 107th Congress, 1st Session, October 23, 2001, 2001 WL 1266413; USA Patriot Act § 220, 115 Stat. at 291.

Common sense dictates the result reached herein. Judicial and prosecutorial efficiency is better served by permitting the federal district court for the district where the crime allegedly occurred to preside over both the investigation and prosecution of that crime. Commentators have suggested that one reason for the amendments effected by Section 220 of the Patriot Act was to alleviate the burden placed on federal district courts in the Eastern District of Virginia and the Northern District of California where major internet service providers ("ISPs") AOL and Yahoo, respectively, are located. See, Paul K. Ohm, *Parallel Effect Statutes and E-mail "Warrants": Reframing the Internet Surveillance Debate*, 72

Geo.Wash.L.Rev. 1599, 1613-15 (Aug. 2004); Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 Geo.Wash.L.Rev. 1375, 1454 (Aug. 2004) (stating that the "effect of the change was to shift the responsibility for issuance of the order from the court where the service provider is located to the court with jurisdiction over the offense being investigated; prior to passage of the USA Patriot Act, a disproportionate number of such orders were issued in the Eastern District of Virginia, where AOL is located."); Franklin E. Fink, *The Name Behind the Screenname: Handling Information Requests Relating to Electronic Communications*, 19 No. 11 Computer & Internet Law 1, 6-7 (Nov. 2002) (stating that "[t]his provision was intended to relieve the burden on district courts in which major communications providers are located, such as the Northern District of California and Eastern District of Virginia."). Indeed, the House Judiciary Committee's Report accompanying the USA Patriot Act explains that § 2703(a) "attempts to address the investigative delays caused by the cross-jurisdictional nature of the Internet." Paul K. Ohm, *Parallel Effect Statutes and E-mail "Warrants": Reframing the Internet Surveillance Debate*, 72 Geo.Wash.L.Rev. at 1614-15, n. 80 (Aug. 2004) (citing H.R. Rep. No. 107-236, pt. 1 at 57 (2001)). The Committee's Report further explains that requiring an investigator to coordinate with agents, prosecutors, and judges in the district where the ISP is located would cause time delays that "could be devastating to an investigation, especially where additional criminal or terrorists acts are planned." *Id.* (emphasis added). Additionally, requiring an Arizona federal agent investigating a crime committed in Arizona to travel to California or Virginia to obtain an out-of-district search warrant from a California or Virginia magistrate judge for electronically-stored communications would, in my view, unnecessarily increase the cost of federal investigations.[4]

---

[4] Occasionally, an entity subject to a valid search warrant and an investigating agent located in a different district may mutually agree, similar to production of documents via a subpoena *duces tecum*, to production of the sought-after records by fax or mail without the necessity of the agent traveling to the outside district; provided, of course, the search warrant was properly authorized.

In light of the foregoing discussion, the Court concludes that when Congress amended Section 2703(a) via Section 220 of the USA Patriot Act to add the phrase "a court with jurisdiction over the offense," Congress intended to authorize the federal district court located in the district where the alleged crime occurred to issue out-of-district warrants for the seizure of electronically-stored communications. This Court has jurisdiction over alleged crimes that occurred in Yuma, Arizona which, of course, is within the District of Arizona. Thus, § 2703(a) authorizes this Magistrate Judge to issue an out-of-district warrant for the search and seizure of electronically-stored communications located in California.

2. Federal Rule of Criminal Procedure 41

Section 2703(a), however, should not be viewed in isolation. Section 2703(a) provides that when "a court with jurisdiction over the offense" issues an out-of-district warrant for the seizure of electronic communications, it must do so "*using the procedures described in* the Federal Rules of Criminal Procedure." Title 18 U.S.C. § 2703(a) (emphasis added). Although § 2703(a) references the Federal Rules of Criminal Procedure generally, in view of the purpose of that section, it is clear that Congress intended that the specific provisions of the Federal Rules which govern search warrants would apply to § 2703(a). Federal Rule of Criminal Procedure 41 addresses the issuance of search warrants. Thus, the Court must consider the interplay between Federal Rule of Criminal Procedure 41, which discusses the issuance of search warrants, and § 2703(a).

Having concluded that § 2703(a)'s reference to the "Federal Rules of Criminal Procedure" means Rule 41, the phrase "using the procedures described in" the Federal Rules remains ambiguous. A reasonable person could conclude that this phrase requires compliance with *all* of the provisions contained in Rule 41 as the Florida Magistrate Judge did in *In Re: Search Warrant*, 362 F.Supp.2d 1298 (M.D. Fla. 2003). Alternatively, a reasonable person could also conclude that the "procedures described in" refers only to the provisions of Rule 41 which are procedural in nature. Because both interpretations are reasonable, the phrase "using the procedures described in the Federal Rules" is ambiguous. *Quarrell*, 310 F.3d at

669 (stating that statutory language is ambiguous if reasonable minds could interpret the same language in two or more ways.)

In view of this ambiguity, the Court must determine which interpretation aligns with Congress' intent in amending § 2703(a). *Id.* For the reasons discussed below, the Court concludes that the phrase "using the procedures described in" only refers to the specific provisions of Rule 41 which detail the procedures for obtaining and issuing search warrants. A fundamental canon of statutory construction provides that "unless otherwise defined, words will be interpreted as taking their ordinary, contemporary, common meaning." *United States v. Smith*, 155 F.3d 1051, 1057 (9th Cir.1998) (quoting *Perrin v. United States*, 444 U.S. 37, 42 (1979)). The word "procedure" is defined as "a series of steps taken to accomplish an action." American Heritage Dictionary, 4th Ed. (2000),[5] or "a specific method or course of action." Black's Law Dictionary, 7th Ed. (1999). The common definition of "procedure" supports the conclusion that § 2703(a) incorporates only those provisions of Rule 41 which discuss "steps to be taken" or the "specific method" of issuing a warrant.

Interpreting "using the procedures" to refer only to the provisions in Rule 41 that describe "steps" or a "specific method" related to issuing a warrant gives meaning to Congress' amendment of § 2703(a) by the USA Patriot Act. Prior to the USA Patriot Act, § 2703(a) authorized the issuance of a warrant "under" the Rules of Criminal Procedure. See, PL 107-56, § 220(a)(1)(amending § 2703(a) by "striking 'under the Federal Rules of Criminal Procedure' every place it appears and inserting using the procedures described in the Federal Rules of Criminal Procedure. . . ."). The use of the word "under", a broad term,[6] in the prior version of § 2703(a), required that the issuance of a warrant comply with all of

---

[5] This definition found in the American Heritage Dictionary can be accessed electronically at education.yahoo.com/reference.

[6] "Under" is defined as "in view of," such as "under these conditions," American Heritage Dictionary, 4th Ed. (2000), and as "inferior" or "subordinate." Black's Law Dictionary, 7th Ed. (1999).

the provisions of Rule 41. Rules of statutory construction require the Court to assume that by changing "under" to "using the procedures described in" the Federal Rules, Congress intended to change the scope of Rule 2703(a). *Wilson*, 503 U.S. at 336. The phrase "using the procedures described in" narrowly focuses on the procedural aspects of obtaining and issuing a search warrant. The word "procedures" is modified by "described in," which expresses Congress' intent that only some aspects — the procedural aspects — of Rule 41 apply to § 2703(a). See, *Jarecki v. G.D. Searle & Co.*, 367 U.S. 303, 307 (1961) (stating that under the doctrine of *noscitur a sociis*, the meaning of a word in a statute may be ascertained in reference to the meaning of the accompanying words. This rule avoids assigning a word a meaning that is so broad that it is inconsistent with accompanying words and, thus gives "unintended breadth to the Acts of Congress."). If all parts of Rule 41 were procedural, the phrase "described in" would be surplusage and contrary to the rule of construction that provides that a court should avoid interpreting a statute in a manner that renders a word or phrase meaningless or redundant. *Gustafson*, 513 U.S. at 562; *Kungys*, 485 U.S. at 778.

Applying this interpretation of § 2703(a), the Court finds that several portions of Rule 41 do not concern the procedures related to the issuance of a search warrant and, therefore, do not apply to the issuance of a warrant under § 2703(a). First, Rule 41(a), "Scope and Definitions," does not describe any procedure. Rule 41(g) and (h) discuss "Motion[s] to Return Property" and "Motion[s] to Suppress." These subsections do not contain any procedures relevant to issuing a search warrant. Similarly, Rule 41(b), entitled "Authority to Issue a Warrant," does not discuss the procedure by which a search warrant is to be issued. Rather, Rule 41(b) discusses the authority of a magistrate judge to issue a warrant in three circumstances. Specifically, Rule 41(b), provides in part that:

> (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 the 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) in an investigation of domestic or international terrorism (as defined in section 2331 of title 18, United States Code), by a Federal magistrate judge in any district in which activities related to the terrorism may have occurred, for a search of property or for a person within or outside the district.

Fed.R.Crim.P. 41(b), as amended December 1, 2007. This subsection only discusses whether a warrant may issue in certain circumstances, and does not discuss *procedures* for issuing a warrant. Rule 41(b) is not procedural in nature and, therefore, does not apply to § 2703(a). This conclusion is supported by Rule 41(a)(1) which provides that "[t]his rule does not modify any statute regulating search or seizure, or the issuance and execution of a search warrant in special circumstances." Fed.R.Crim.P. 41(a). Section 2703(a) which authorizes out-of-district search warrants on internet service providers is a statute which regulates the issuance of warrants in "special circumstances." Accordingly, Rule 41(a) expresses Congress' intent that Rule 41(b) does not limit a district court's authority granted in § 2703(a).

In contrast to the foregoing subsections, several other provisions in Rule 41 specifically discuss procedures related to issuing a warrant. For example, Rule 41(e) enumerates procedures for issuing a warrant. Rule 41(e) describes the contents of the warrant and the manner in which a warrant should be executed. Fed.R.Crim.P. 41(e). Similarly, Fed.R.Crim.P. 41(d) describes procedures for requesting a warrant in the presence of a magistrate judge. *Id.* Thus, these procedural aspects of Rule 41 apply to § 2703(a).

III. Conclusion

In conclusion, the Court finds that Title 18 U.S.C. § 2703(a) authorizes a federal district court, located in the district where the alleged crime occurred, to issue search warrants for the production of electronically-stored evidence located in another district. The warrant must be issued in compliance with the procedures described in Federal Rule of Criminal Procedure 41. Federal Rule of Criminal Procedure 41(b), however, does not limit

the authority of a district court to issue out-of-district warrants under § 2703(a) because Rule 41(b) is not procedural in nature and, therefore, does not apply to § 2703(a). Thus, this Court concludes that § 2703(a) authorizes an Arizona magistrate judge to issue an out-of-district search warrant for the contents of communications electronically-stored in California when the alleged crime occurred in the District of Arizona.

Accordingly,

IT IS ORDERED that the Government's motion to authorize an out-of-district search warrant for the contents of electronically-stored communications held by Yahoo in Sunnyvale, California is **GRANTED**. The subject search warrant is issued.

Dated this 21st day of May, 2007

Lawrence O. Anderson
United States magistrate Judge