IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR A SEARCH WARRANT FOR CONTENTS OF ELECTRONIC MAIL AND FOR AN ORDER DIRECTING A PROVIDER OF ELECTRONIC COMMUNICATION SERVICES TO NOT DISCLOSE THE EXISTENCE OF THE SEARCH WARRANT	No. 08-9131-MC No. 08-9147-MC OPINION & ORDER

MOSMAN, J.,

This is an appeal from Magistrate Judge Hubel's Order (#19) signed November 21, 2008, holding that all parts of Federal Rule of Criminal Procedure 41 ("Rule 41") apply to a warrant issued under 18 U.S.C. § 2703(a). Specifically, Judge Hubel ordered that "[t]he receipt required by Rule 41(f)(1)(C) must be provided to the subscriber of the e-mail accounts for the e-mails stored for 180 days or less which are seized." (Order (#19) 9.) This notice was delayed until the resolution of any appeal by the government. (*Id.*) The United States appealed Judge Hubel's order, arguing that they are not required to give notice to the e-mail subscribers because Rule 41(f) does not apply to warrants obtained under § 2703(a). Further, the government contends that even if it does apply, Rule 41(f)(1)(C) requires only that the Internet service provider ("ISP")

be served with the warrant, not that notice be given to the e-mail subscriber. This court asked the Federal Public Defender's office to respond to the United States's briefing as amicus curiae.

I find that § 2703(a) of the Stored Communications Act incorporates all procedural aspects of Rule 41, including the so-called "notice" requirement of Rule 41(f)(1)(C). I further find this notice provision is satisfied, in this context, by leaving a copy of the warrant with the third-party ISP. In any event, where no property is actually seized—as is true in this case and most cases involving search warrants for e-mail—the notice requirement of Rule 41(f)(1)(C) is not even triggered. For these reasons, as explained more fully below, I reverse the holding of the magistrate judge.

BACKGROUND

I. The Stored Communications Act

The Fourth Amendment protects our homes from unreasonable searches and seizures, requiring that, absent special circumstances, the government obtain a search warrant based on probable cause before entering. *See Kyllo v. United States*, 533 U.S. 27, 31 (2001) ("At the very core of the Fourth Amendment stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion. With few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no." (internal quotation marks and citations omitted)). This is strong privacy protection for homes and the items within them in the physical world.

When a person uses the Internet, however, the user's actions are no longer in his or her physical home; in fact he or she is not truly acting in private space at all. The user is generally accessing the Internet with a network account and computer storage owned by an ISP like

Comcast or NetZero. All materials stored online, whether they are e-mails or remotely stored documents, are physically stored on servers owned by an ISP. When we send an e-mail or instant message from the comfort of our own homes to a friend across town the message travels from our computer to computers owned by a third party, the ISP, before being delivered to the intended recipient. Thus, "private" information is actually being held by third-party private companies.

This feature of the Internet has profound implications for how the Fourth Amendment protects Internet communications—if it protects them at all. The law here remains unclear and commentators have noted that there are several reasons that the Fourth Amendment's privacy protections for the home may not apply to our "virtual homes" online. First, it is uncertain whether we have a reasonable expectation of privacy in information sent through or stored by ISPs because the Fourth Amendment does not protect information revealed to third parties. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1210-11 (2004) (citations omitted). Second, the government may obtain a court order, such as a grand jury subpoena, without a showing of probable cause for materials belonging to the target of an investigation but held by a third party, like e-mails stored by an ISP. *Id.* at 1211-12 (citations omitted). Third, most ISPs are private actors, therefore they can read all the files stored on their servers without violating the Fourth Amendment. *Id.* at 1212 (citations omitted).

Congress responded to this uncertainty by enacting the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701-2712, as part of the Electronic Communications Privacy Act of 1986. The SCA gives network account holders statutory privacy rights against access to stored

information held by ISPs. The statute also creates Fourth Amendment-like privacy protections regulating the methods by which government investigators may obtain users' private information in a service provider's possession. First, the SCA limits the government's ability to compel service providers to disclose information in their possession about their subscribers. *See* 18 U.S.C. § 2703. Second, it limits the service provider's ability to voluntarily disclose information about their subscribers to the government. *See id.* § 2702.

The SCA regulates two types of service providers, providers of electronic communication service ("ECS") and providers of remote computing service ("RCS"). Except as authorized by subsection (b), providers of ECS may not divulge the contents of communications in electronic storage. *Id.* § 2702(a)(1). Similarly, absent a statutory exception, providers of RCS may not divulge the contents of any communication carried or maintained on the service on behalf of a customer or subscriber for the purpose of providing storage or computer processing services to the customer or subscriber. *Id.* § 2702(a)(2).

A few definitions will help clarify exactly how the SCA protects electronic communications. The statute defines ECS as "any service which provides to users thereof the ability to send or receive wire or electronic communications." *Id.* § 2510(15) *incorporated by id.* § 2711(1). Electronic storage is "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an [ECS] for purposes of backup protection of such communication." *Id.* § 2510(17). An RCS is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system." *Id.* § 2711(2). Finally, an electronic communication system is "any wire, radio, electromagnetic, photooptical or

photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." *Id.* § 2510(14).

Today, most ISPs provide both ECS and RCS; thus, the distinction serves to define the service that is being provided at a particular time (or as to a particular piece of electronic communication at a particular time), rather than to define the service provider itself. The distinction is still essential, however, because different services have different protections.[1] Section 2703 governs the government's ability to compel service providers to disclose electronic communications held on their servers. *Id.* § 2703. The government may require disclosure of the contents of electronic communications in electronic storage of an ECS for 180 days or less, "only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure." *Id.* § 2703(a). The contents of those same communications in storage for more than 180 days and the contents of communications stored in an RCS may be obtained with a warrant, or with prior notice and an administrative subpoena or court order. *Id.* § 2703(b)(1).

---

[1] The distinction can be difficult to draw. In *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004), the Ninth Circuit was required to define what types of e-mails were protected under § 2701(a)(1), which outlaws unauthorized access to an ECS to obtain, alter, or prevent access to electronic communications in electronic storage. The court held that an e-mail is in electronic storage, and thus governed by the rules governing ECS, until the "underlying message has expired in the normal course." *Id.* at 1076. This definition has been roundly criticized for being unworkable. *See* Kerr, *supra*, at 1216-18, n.61 (explaining that e-mails that are in transit or have been delivered but not opened are stored in ECS, while e-mails that have been opened and left on the server, rather than saved to a hard drive and deleted from the server, are stored in RCS). In particular, this definition is difficult to apply to § 2703 as it would require the government to obtain warrants for the contents of all e-mails, just in case some of the e-mails have not yet expired (I presume that different e-mails expire after different amounts of time), even if the e-mails obtained are ultimately expired and obtainable under a lesser showing than probable cause under the rules applying to RCS.

II. The Search Warrants

In July, the United States requested two search warrants under § 2703(a) for e-mails belonging to certain subscribers to Google, an electronic communication service provider, and Webhost, Inc., an Internet website hosting service provider. The requests sought subscriber information, connection logs and data, and the contents of all electronic communications for the last nine months.[2] Magistrate Judge Hubel found that the affidavit supporting the applications established "probable cause to believe a crime had been committed and that the contents of the communications and [the] other information sought . . . would contain evidence of the crimes" and issued the warrants. (Order (#19) 1.)

In the warrant application, the government requested that the court "(1) seal the applications and warrants, (2) enter an order precluding notice of the existence of the warrants by the service providers to anyone, including the subscriber or customer, for such period as the Court determines is appropriate," and (3) delay any notification to the subscriber or customer that might be required by § 2703(b).[3] (*Id.* at 1-2.) Judge Hubel granted the motion to seal the warrants, the applications, and the returns on the warrants, as requested. He also entered an order precluding the service providers from informing anyone of the issuance of or the providers' compliance with the warrants.

---

[2] The facts provided to this court are insufficient to determine whether the United States was seeking the contents of electronic communications in ECS or in RCS. However, because the government applied for and received a search warrant based on probable cause, the distinction is immaterial. The contents of all electronic communications may be obtained with a search warrant. *See* 18 U.S.C. § 2703(a)-(b).

[3] It is unclear why notice required by § 2703(b) would be applicable to a warrant obtained under § 2703(a).

The government later changed its position regarding notice to the e-mail subscribers. Rather than seeking a delay of notice, the government argues that § 2703(a) and Rule 41 do not require any notice to the subscriber of the seized e-mail. First, the government argues that Rule 41(f) does not apply to warrants issued under § 2703(a) because only the portions of Rule 41 defining the procedures necessary to issue a warrant were incorporated by § 2703(a). Second, the government contends that even if Rule 41(f)(1)(C) is applicable in this case, it only requires that notice be given to the holder of the seized property, here the service providers.

Judge Hubel found that all of Rule 41 applies to warrants obtained under § 2703(a) and that the receipt required by Rule 41(f)(1)(C) must be to the subscriber to the e-mail service, not to the service provider. However, he temporarily delayed notice under § 3103a(b) and § 2705 because he found that there was reasonable cause to believe that providing immediate notice of the execution of the warrants would have an adverse effect on the criminal investigation.[4]

III. The Question Presented

Before my analysis begins, it is important to define exactly what I have been asked to do in this case. The SCA has already provided the owners of the electronic communications at issue the highest protection available under the Fourth Amendment, the requirement that the government obtain a warrant based on probable cause. I am merely being asked what, if anything, must be done after the warrant is issued.

The questions now before this court are: (1) does Rule 41(f)(1)(C) apply to warrants issued under § 2703(a) and (2) if so, does leaving a copy of the warrant with the service provider

---

[4] Section 2705 specifically allows a delay of the notice required under § 2703(b). 18 U.S.C. § 2705(a). It does not apply to notice under § 2703(a), if such notice is required.

satisfy the requirements of Rule 41(f)(1)(C) when the warrant is for the contents of stored e-mails? I hold that Rule 41(f)(1)(C) does apply to warrants issued under § 2703(a) and is satisfied by providing a receipt to the ISP. However, because no property was actually taken in this case, Rule 41(f)(1)(C) does not require that a receipt be provided. Judge Hubel's determination that the subscriber must be given a receipt is therefore REVERSED.

STANDARD OF REVIEW

Questions of law are reviewed de novo, *see United States v. Cabaccang*, 332 F.3d 622, 624-25 (9th Cir. 2003) (en banc), as is a court's interpretation of the federal rules, *see Mann v. American Airlines*, 324 F.3d 1088, 1090 (9th Cir. 2003). Thus, I review Judge Hubel's interpretation of § 2703(a) and Rule 41 de novo.

DISCUSSION

I. Incorporation of Rule 41

A. *Statutory Interpretation*

In federal statutory interpretation the "starting point in discerning congressional intent is the existing statutory text." *Lamie v. U.S. Trustee*, 540 U.S. 526, 534 (2004) (citing *Hughes Aircraft Co. v. Jacobson*, 525 U.S. 432, 438 (1999)). "The preeminent canon of [federal] statutory interpretation requires [a court] to 'presume that [the] legislature says in a statute what it means and means in a statute what it says there.'" *BedRoc Ltd. v. United States*, 541 U.S. 176, 183 (2004) (quoting *Conn. Nat'l Bank v. Germain*, 503 U.S. 249, 253-54 (1992)). Therefore, a court's "inquiry begins with the statutory text, and ends there as well if the text is unambiguous." *Id.* (citing *Lamie*, 540 U.S. at 534). However, the structure and purpose of a statute can 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."). Further, courts presume that when Congress alters the words in a statute, it intends to change the statute's meaning. *United States v. Wilson*, 503 U.S. 329, 336 (1992).

Statutory text is ambiguous if it is "capable of being understood in two or more possible senses or ways." *Chickasaw Nation v. United States*, 534 U.S. 84, 90 (2001) (quoting Webster's Ninth New Collegiate Dictionary 77 (1985)). If a statutory provision is ambiguous, a court looks to the legislative history. *SEC v. McCarthy*, 322 F.3d 650, 655 (9th Cir. 2003) (quoting *Nw. Forest Res. Council v. Glickman*, 82 F.3d 825, 834 (9th Cir. 1996)).

B. *Amendments to § 2703 by the USA PATRIOT Act*

Prior to 2001, § 2703(a) provided 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 under the Rules of Criminal Procedure or equivalent State warrant*.

18 U.S.C. § 2703(a) (1998) (emphasis added). The Patriot Act amended § 2703(a), allowing a government entity to require such disclosures "*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*."[5] *Id.* § 2703(a) (2006) (emphasis added).

---

[5] Section 220 of the Patriot Act amended § 2703 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 by a court with jurisdiction over the offense under investigation.'" USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

The government contends that the phrase, "pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure," incorporates only those procedural portions of Rule 41 related to the issuance of a warrant. Such a reading would mean that the statute does not incorporate any substantive portions of the Rule or any procedures occurring after the warrant has been issued by the magistrate. Magistrate Judge Hubel held, and the Federal Public Defender argues, that all of Rule 41 has been incorporated by § 2703(a).

1. Substantive versus procedural portions of Rule 41

I look first at the current language of § 2703 to determine whether it incorporates the substantive portions of Rule 41. Unlike the original language, stating that the warrant must be issued "under" Rule 41, the current statutory language specifies that the warrant must be "issued using the procedures described in" Rule 41. 18 U.S.C. § 2703(a). The plain language thus specifies that only the procedures of Rule 41 are to be incorporated.

Other courts have come to the same conclusion. The District of Arizona specifically found that the provisions of 41(a), "Scope and Definitions," 41(b), "Authority to Issue a Warrant," 41(g), "Motion to Return Property," and 41(h), "Motion to Suppress," were not incorporated by § 2703 because they did not describe procedures related to the issuance of a search warrant. *In re Search of Yahoo, Inc.*, 2007 WL 1539971, *6 (D. Ariz. May 21, 2007) (unpublished); *see also United States v. Berkos*, 543 F.3d 392, 398 (7th Cir. 2008) ("Section 2703(a) refers only to the specific provisions of the Rules of Criminal Procedure, namely, Rule 41, that detail the *procedures* for obtaining and issuing warrants."); *In re Search Warrant*, 2005 WL 3844032, *5 (M.D. Fla. Feb. 13, 2006) (unpublished) (holding that "the 'using the

procedures' language seems more focused solely on the actual procedural aspects . . . of search warrants").

In reaching this conclusion, the district court focused on the language of the statute. First, the court noted that "'procedure' is defined as 'a series of steps taken to accomplish an action,' or 'a specific method or course of action,'" supporting 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." *In re Search of Yahoo*, 2007 WL 1539971 at *5 (citations omitted). Second, the court found that this interpretation gave meaning to the change in language from the broad word "under" to the more narrow phrase "using the procedures described in." *Id.* at *6. Third, the word "procedures" was modified by the phrase "described in," which the court found expressed "Congress's intent that only some aspects—the procedural aspects—of Rule 41 apply to § 2703(a)." *Id.* (citation omitted).

This reasoning is persuasive. I agree with the government that the substantive portions of Rule 41 are not adopted by § 2703(a). However, because Rule 41 describes procedures to be followed in both the issuance and the execution and return of a warrant, we must look further.

2. All procedures versus procedures for issuance

The United States contends that Congress went further than removing the substantive portions of Rule 41 from incorporation into § 2703(a); that Congress used the language "issued using the procedures described in" to incorporate only those procedures of Rule 41 that are related to obtaining and issuing search warrants. In fact, the United States also takes the position that even prior to the Patriot Act amendments, § 2703 did not incorporate any provision relating

to return of warrants. Because Rule 41(f) relates to the execution and return of search warrants, the government argues that its procedures are not required under § 2703(a).

The government's argument is attractive at first glance. It is certainly a reasonable reading of the plain language of the statute, which uses the word "issued." And it appears to be supported by the interpretations of the Seventh Circuit, the District of Arizona, and the Middle District of Florida. *See Berkos*, 543 F.3d at 398 ("[T]he procedures for issuing a warrant are enumerated at Rule 41(e)."), *In re Search of Yahoo*, 2007 WL 1539971 at *5 ("[T]he 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."), *In re Search Warrant*, 2005 WL 3844032 at *6 ("the prosecutor and the court must look to Rule 41 subsections (d) and (e) . . . in obtaining and issuing" a search warrant under § 2703(a)). However, none of these courts was faced with the question of which procedural portions of Rule 41 were incorporated by § 2703(a). All three courts were attempting to determine whether magistrates could issue search warrants under § 2703(a) for searches in other districts, contrary to Rule 41(b), which states that a magistrate may only "issue a warrant to search for and seize a person or property located within the district." Fed. R. Crim. P. 41(b)(1). Each court determined that Rule 41(b) was a substantive provision of the Rule because it limited a magistrate's power to issue a warrant, rather than describing the procedures to be used in obtaining and issuing a warrant.

The Federal Public Defender points to § 2703(b)(1)(A), as support for the incorporation of Rule 41(f)(1)(C) by § 2703(a). Section 2703(b)(1)(A) states that a governmental entity may obtain certain electronic communications "without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal

Rules of Criminal Procedure." 18 U.S.C. § 2703(b)(1)(A). The Federal Public Defender contends that using the phrase "without required notice" for warrants obtained under § 2703(b)(1)(A) but not making such an exception for warrants obtained under § 2703(a), indicates that warrants under § 2703(a) must require notice to the subscriber or customer of the ISP. The United States, in contrast, argues that "without required notice" contrasts § 2703(b)(1)(A) with § 2703(b)(1)(B), which specifies the method by which a governmental entity may obtain the contents of electronic communications without first obtaining a warrant. Under § 2703(b)(1)(B), prior notice to the subscriber or customer is required when the governmental entity uses an administrative subpoena or court order to obtain the contents of the electronic communications.

The United States argues that the statute sets up a system where the government can either meet the higher standard of probable cause and obtain a warrant without notice or meet the lower standard of an administrative subpoena or court order, while providing notice to the subscriber or customer. Thus, both methods ensure the protection of the subscriber or customer's rights in different ways; one method ensures the full protections of the Fourth Amendment's requirement for probable cause and the other allows the subscriber or customer to challenge the subpoena or court order before it is executed.

The United States also points to two pre-Patriot Act cases that found that notice was not required when a warrant was obtained under § 2703(a). However, neither court was focused on Rule 41(f)(1)(C) warrant and receipt procedures. Instead, they were looking at the general requirements set forth in § 2703. *See Guest v. Leis*, 255 F.3d 325, 339 n.7 (6th Cir. 2001) (stating that the statute does not require notice to subscribers when police are operating with a warrant, but not mentioning Rule 41); *United States v. Hambrick*, 55 F. Supp. 2d 504, 507 (W.D.

Va. 1999) (stating that the government may require an ISP to provide stored communications under two conditions, with a warrant issued under the Federal Rules of Criminal Procedure or with prior notice and a subpoena or court order). In fact, the use of the word notice is a bit misleading. Rule 41(f)(1)(C) requires a copy of the warrant and a receipt be provided. Section 2703(b)(1)(B) focuses on prior notice but does not specify how the notice must be given.

Both of these interpretations of the phrase "without required notice" are reasonable, and give little guidance regarding how to interpret the word "issued." "Issued" may be read to limit the procedures that are applicable under § 2703(a), or it might merely have been used as shorthand for the process of obtaining, issuing, executing, and returning a warrant, as described in Rule 41. The statute is therefore ambiguous and I must turn to the legislative history for guidance regarding congressional intent.

a. The legislative history of the Patriot Act amendments

The legislative history of the Patriot Act indicates that Congress intended the amendments to § 2703 to allow magistrates to issue search warrants for e-mail that would be valid throughout the United States, rather than only in the district in which they were issued, as is normal under Rule 41(b). The House Judiciary Committee's Report accompanying the Patriot Act explains that:

> Title 18 U.S.C. § 2703(a) requires a search warrant to compel service providers to disclose unopened e-mails. This section does not affect the requirement for a search warrant, but rather attempts to address the investigative delays caused by the cross-jurisdictional nature of the Internet. Currently, Federal Rules of Criminal Procedure 41 requires that the "warrant" be obtained "within the district" where the property is located. An investigator, for example, located in Boston who is investigating a suspected terrorist in that city, might have to seek a suspect's electronic e-mail from an Internet service provider (ISP) account located in California. The investigator would then need to coordinate with agents, prosecutors

> and judges in the district in California where the ISP is located to obtain a warrant to search. These time delays could be devastating to an investigation, especially where additional criminal or terrorist acts are planned. Section 108 amends § 2703 to authorize the court with jurisdiction over the investigation to issue the warrant directly, without requiring the intervention of its counterpart in the district where the ISP is located.

H.R. Rep. No. 107-236, pt. 1, at 57 (2001); *see also* 147 Cong. Rec. H7197-98 (2001) (Section 220, "[p]ermits a single court having jurisdiction over the offense to issue a search warrant for e-mail that would be valid in [sic] anywhere in the United States."). The focus was squarely on allowing search warrants for property outside the district of issuance. Nothing in the legislative history indicates what other portions of Rule 41 might or might not be applicable. Thus, this legislative history gives us no guidance regarding the meaning of the word "issued."

b. The legislative history of the Electronic Communications Privacy Act

In passing the Electronic Communications Privacy Act in 1986, Congress expressed the need to expand the protections of the Fourth Amendment to new forms of communication and data storage. 132 Cong. Rec. H4039-01 (1986); S. Rep. No. 99-541, at 1-2 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3555-56. The legislative history indicates that Congress wished to encourage the development and use of these new methods of communication by ensuring that they were protected and private. S. Rep. No. 99-541, at 5. Congress recognized that courts had struggled with the application of the Fourth Amendment to the seizure of intangibles, like telephone conversations. *Id.* at 2. They therefore sought to strike a balance between the competing interests addressed by the Fourth Amendment in the world of electronic communications by "protect[ing] privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs." *Id.* at 3.

It is clear that Congress wished to apply the protections associated with search warrants to searches authorized under § 2703(a). *See id.* at 38 (stating that "[a] government entity can only gain access to the contents of [electronic communications in electronic storage for 180 days or less] pursuant to a warrant"). However, the legislative history tells us nothing about exactly how the search warrant requirement is to be applied practically, nor does it discuss whether some provisions do not apply. *See id.* at 36-39 (summarizing the provisions of § 2703, but not adding any explanation beyond the language of the statute).

The United States asks me to conclude that Congress intended to incorporate only some of the procedures applicable to ordinary search warrants into § 2703(a). Endorsement of such a narrow view of what otherwise looks like a wholesale adoption of the search warrant procedures must be premised on some legislative history or textual support. Neither the text of § 2703(a), nor the original legislative history, lends such support. In my view, the most sensible reading of the combination of text and legislative history is that Congress—perhaps without much careful attention—incorporated all the procedures dictated by Rule 41 into the § 2703(a) warrant requirement.

The United States argues that such wholesale incorporation is messy, requiring incorporation of elements that do not easily fit searches conducted under § 2703. That is because several elements of Rule 41(f)(1) presuppose a search for items in the physical, rather than the electronic, world. For example, Rule 41(f)(1)(B) requires that an officer present during the execution of the warrant prepare and verify an inventory of property seized "in the presence of another office and the person from whom, or from whose premises, the property was taken."

Fed. R. Crim. P. 41(f)(1)(B).[6] But the fact that some of the pieces of Rule 41 do not fit neatly into searches under § 2703 is not necessarily a contraindication of Congressional intent. In any event, some of this messiness is resolved by the careful application of the procedures to the particular situation at hand in this case, the search of e-mail stored on computers held by third-party ISPs, as discussed below.

C. ***What does Rule 41(f)(1)(C) require?***

The word "notice" has been used by the United States, the Federal Public Defender, and Magistrate Judge Hubel in this case with reference to Rule 41(f)(1)(C). But the Rule does not require notice, as such. Rather, the Rule requires that an officer executing a warrant "give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken or leave a copy of the warrant and receipt at the place where the officer took the property." Fed. R. Crim. P. 41(f)(1)(C). The word "notice" is never used. There are three ways to fulfill Rule 41(f)(1)(C)'s requirement: (1) a copy of the warrant and a receipt may be given to the owner of the property searched and/or seized; (2) a copy of the warrant and a receipt may be given to the person from whose premises the property was seized, even if they are

---

[6] The Eighth Circuit addressed concerns regarding the application of physical world rules to search warrants authorizing the seizure of e-mails held on third-party ISP servers in *United States v. Bach*, 310 F.3d 1063 (8th Cir. 2002). The defendant in *Bach* argued that the search was conducted in violation of the Fourth Amendment because no officer was present for the search of the ISP's files. *Id.* at 1066. The court explained that the search of an ISP's server was not like an ordinary search because "no warrant was physically 'served,' no persons or premises were searched in the traditional sense, and there was no confrontation between Yahoo! technicians and Bach." *Id.* at 1067. The court held that Bach's Fourth Amendment rights were not violated because, among other reasons, the presence of the officer would not have aided in the search, the technical expertise of the ISP's employees exceeded that of the officers, and the items seized were on the ISP's property. *Id.*

not the owner of the property; or (3) a copy of the warrant and a receipt may be left where the property was seized.

Notice of the search and seizure is an effect of this rule, but it is not the rule's only purpose. Providing a copy of the warrant informs the citizen of the legality of the search and seizure and informs the citizen of the scope of what may be seized. *See, e.g.*, *United States v. Gantt*, 194 F.3d 987, 990-91 (9th Cir. 1999) (analyzing the policies underlying the warrant requirement as support for requiring service of warrant under Rule 41 at outset of search absent exigent circumstances). The receipt is also necessary for those persons who wish to have property returned under Rule 41(g), and is intended to protect their property interests more than any privacy interest.

1. Third Party Context

As discussed above, Rule 41 allows the copy of the warrant and the receipt to be given to the person from whose premises the property at issue was seized, even if that person is not the owner of the property. There is no separate requirement that the officer provide the warrant, a receipt, or any other form of notice to the owner of the property. Thus, when police seize a package from Federal Express ("FedEx"), they may leave a copy of the warrant and receipt at the FedEx facility and do not need to inform the sender or recipient of the package of the seizure. *United States v. Zacher*, 465 F.3d 336, 339 (8th Cir. 2006) (holding that North Dakota Rule of Criminal Procedure 41(d), which the court noted was virtually identical to Rule 41(f)(3), now 41(f)(1)(C), was satisfied by leaving a copy of the warrant at the FedEx facility).

In this case, the warrant was served on Google and Webhost for electronic information stored on the companies' servers. The ISP's are analogous to FedEx in *Zacher*; the electronic

information was stored on the servers at Google and Webhost the same way the package was stored at FedEx. Requiring notice to the subscriber ignores this third-party context. When the property to be seized is in the possession of a third party, Rule 41(f)(1)(C) requires no more than what was already accomplished in this case.

2. No Property Was Taken

An additional twist in the case of electronic information is that no property is actually taken or seized as that term is used in the Fourth Amendment context. The Supreme Court has stated that "[a] 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (citations omitted). Here, there was no such meaningful interference due to the nature of electronic information, which can be accessed from multiple locations, by multiple people, simultaneously. More specifically for the purposes of Rule 41, if no property was taken, there is no person from whom, or from whose premises, the property was taken. Thus, under the plain language of Rule 41 there would not appear to be any requirement that a warrant be left with or a receipt be provided to anyone.

II. The Constitutional Notice Requirement is Met by Executing the Warrant on a Third Party

As discussed earlier, the SCA was intended to codify overarching Fourth Amendment protections into a specific statute. What Fourth Amendment protections, if any, conferred on e-mail and other electronic communication independent of the SCA is, to date, unclear. *See* Kerr, *supra*, at 1210-12. Assuming, for the sake of argument, that the e-mails at issue in this case are

protected under the Fourth Amendment, it is necessary to determine whether there is a constitutional requirement for notice to the subscriber of the e-mail account.

Although the Fourth Amendment does not prohibit surreptitious entries, per se, the absence of a notice requirement in a warrant "casts strong doubt on its constitutional adequacy." *United States v. Freitas (Freitas I)*, 800 F.2d 1451, 1456 (9th Cir. 1986) (internal citations omitted). The Supreme Court has noted that failing to require notice and return procedures for a warrant allows the government full discretion regarding what to seize, and thus allows searches and seizures "without adequate judicial supervision or protective procedures." *Berger v. New York*, 388 U.S. 41, 60 (1967) (striking down a New York law that permitted any judge to issue an ex parte order for eavesdropping upon oath or affirmation of an attorney or officer, as violating the Fourth Amendment due to lack of requirement for particularity as to the related crime, the place to be searched or conversations sought, and a failure to require exigent circumstances). The sanctity of the home is often cited as the central purpose for this notice requirement, but the requirement has not been explicitly limited to searches of homes. *See, e.g.*, *Freitas I*, 800 F.2d at 1456 (stating that "[t]he mere thought of strangers walking through and visually examining the center of our privacy interest, our home, arouses our passion for freedom as does nothing else").

Notice does not always have to be provided before a search or seizure occurs. *See Dalia v. United States*, 441 U.S. 238, 248 (1979) (holding that "[t]he Fourth Amendment does not prohibit *per se* a covert entry performed for the purpose of installing otherwise legal electronic bugging equipment"). "[O]fficers need not announce their purpose before conducting an otherwise authorized search if such an announcement would provoke the escape of the suspect or the destruction of critical evidence." *Katz v. United States*, 389 U.S. 347, 355 n.16 (1967) (citing

Ker v. California, 374 U.S. 23, 37-41 (1963)); *see also Nordelli v. United States*, 24 F.2d 665, 666-67 (9th Cir. 1928) (holding that Rule 41(d), now Rule 41(f)(1)(C), does not invariably require that the copy of the warrant and receipt be served before a search takes place). However, when there is no advance notice, a substitute must exist to satisfy the Fourth Amendment, as in Title III, which has been held to provide "a constitutionally adequate substitute for advance notice by requiring that once the surveillance operation is completed the authorizing judge must cause notice to be served on those subjected to surveillance." *Dalia*, 441 U.S. at 248.

It is clear that notice is an essential part of the reasonableness calculus in judging searches and seizures under the Fourth Amendment. The Federal Public Defender has argued that this constitutional notice requirement supports Judge Hubel's determination that the copy of the warrant and receipt (what the parties refer to as notice) must be provided to the subscriber to the e-mail account, rather than just to the ISP. The notice must be provided to the subscriber because the ISP "has a far lesser privacy interest in the content of its subscriber's e-mails than the subscribers themselves." (Amicus Br. (#28) 21.)

This argument fails to take into account the third party context in this case. If a suspect leaves private documents at his mother's house and the police obtain a warrant to search his mother's house, they need only provide a copy of the warrant and a receipt to the mother, even though she is not the "owner" of the documents. *See* Fed. R. Crim. P. 41(f)(1)(C) (stating that the officer executing the warrant "must give a copy of the warrant and a receipt . . . to the person from whom, or from whose premises, the property was taken"). In such a case, it is irrelevant that the suspect had a greater privacy interest in the content of the documents than did his mother. When he left the documents in her possession he no longer has a reasonable expectation

of privacy in their contents. *See California v. Greenwood*, 486 U.S. 35, 41 (1988) (holding that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties" (quoting *Smith v. Maryland*, 422 U.S. 735, 743-44 (1979))); *see also United States v. Miller*, 425 U.S. 435, 443 (1976) ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." (citing *United States v. White*, 401 U.S. 745, 752 (1971))). In fact, the suspect in such a case, were he to become a defendant in court, would not have standing to object if there were constitutional deficiencies in the warrant used to search his mother's home. *United States v. Payner*, 447 U.S. 727, 731-32 (1980) (holding that a defendant had no standing to object to the illegal seizure of his financial records from his banker); *see also Rawlings v. Kentucky*, 448 U.S. 98, 105-06 (1980) (holding that defendant did not have standing to object to search of a third party's purse, despite the fact that he claimed ownership of the drugs found in that purse, because he had no legitimate expectation of privacy in someone else's purse); *Rakas v. Illinois*, 439 U.S. 128, 149 (1978) (holding that defendants could not make a Fourth Amendment claim regarding a search of someone else's car because they had no "legitimate expectation of privacy in the glove compartment or area under the seat of the car in which they were merely passengers").

Similarly, in the third party subpoena context, the "general rule [is] that the issuance of a subpoena to a third party to obtain the records of that party does not violate the rights of a defendant, even if a criminal prosecution is contemplated." *Miller*, 425 U.S. at 444. In *Miller*, the Court held that bank records obtained from a bank pursuant to a subpoena were admissible

against the bank depositor whose records had been seized. *Id.* at 445. The Court first determined that the depositor had no legitimate expectation of privacy in the records because they were instruments used in commercial transactions and the information was "voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." *Id.* at 442-43. When no expectation of privacy was found, the court applied the general rule for third party subpoenas, affirming the district court's denial of the motion to suppress the bank records. *Id.* at 444-45.

Here, the defendants voluntarily conveyed to the ISPs and exposed to the ISP's employees in the ordinary course of business the contents of their e-mails. The Google privacy policy explicitly states that Google will share personal information of its subscribers when it has "a good faith belief that access, use, preservation or disclosure of such information is reasonably necessary to . . . satisfy any applicable law, regulation, legal process or enforceable governmental request." Google Privacy Policy, http://www.google.com/privacypolicy.html (last visited May 13, 2009). The court understands that other ISPs have similar privacy policies. *See, e.g.*, Microsoft Online Privacy Statement, http://privacy.microsoft.com/en-us/fullnotice.mspx (last visited May 13, 2009) (stating that personal information may be shared to "comply with the law or respond to lawful requests or legal process"); AOL Network Privacy Policy, http://about.aol.com/aolnetwork/aol_pp (last visited May 13, 2009) ("The contents of your online communications, as well as other information about you as an AOL Network user, may be accessed and disclosed in response to legal process (for example, a court order, search warrant or subpoena); [and] in other circumstances in which AOL believes the AOL Network is being used in the commission of a crime . . . ."). Thus subscribers are, or should be, aware that their

personal information and the contents of their online communications are accessible to the ISP and its employees and can be shared with the government under the appropriate circumstances. Much of the reluctance to apply traditional notions of third party disclosure to the e-mail context seems to stem from a fundamental misunderstanding of the lack of privacy we all have in our e-mails. Some people seem to think that they are as private as letters, phone calls, or journal entries. The blunt fact is, they are not.

In this third party context, the Fourth Amendment notice requirement is satisfied when a valid warrant is obtained and served on the holder of the property to be seized, the ISP. In this case, the ISPs were served with the warrants to obtain the relevant e-mails. The requirements of the Fourth Amendment were satisfied.

CONCLUSION

Based on the foregoing, Magistrate Judge Hubel's determination that the subscriber must be given a receipt is REVERSED.

IT IS SO ORDERED.

DATED this 19th day of June, 2009.

/s/ Michael W. Mosman
MICHAEL W. MOSMAN
United States District Judge