

**FACSIMILE COVER SHEET**

**U.S. ATTORNEY'S OFFICE, SDNY
ONE ST. ANDREW'S PLAZA
NEW YORK, NY 10007**

AUSA Name: HOWARD MASTER
AUSA Telephone No.: 212 637 2248
AUSA Fax No.: 212 637 2527
Date: 4-4-08

No. pages (including cover sheet):

Date sent:

"FOR OFFICIAL USE ONLY" U.S. ATTORNEY FACSIMILE COMMUNICATION

The information contained in this facsimile message, and any and all accompanying documents, constitute "FOR OFFICIAL USE ONLY" information. This information is the property of the U.S. Attorney's Office. If you are not the intended recipient of this information, any disclosure, copying, distribution, or the taking of any action in reliance on this information is strictly prohibited. If you received this information in error, please notify us immediately by telephone at the above number and destroy the information.

To: KEVIN BANKSTON ESQ.
Fax No.: 415 - 436 - 9993

REMARKS: _____



U.S. Department of Justice

United States Attorney
Southern District of New York

*The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007*

April 4, 2008

BY HAND

Hon. Michael H. Dolinger
United States Magistrate Judge
Southern District of New York
United States Courthouse
500 Pearl Street
New York, New York 10007

Re: *In re Application of the United States for an Order
Pursuant to 18 U.S.C. § 2703(d),
No. 08 Mag. 499*

Dear Judge Dolinger:

The Government respectfully submits this letter brief pursuant to Your Honor's order dated March 7, 2008 (the "Order") directing the Government to provide a letter brief addressing two issues concerning the above-captioned application for an order pursuant to 18 U.S.C. § 2703(d) (the "Application"). The Application seeks, *inter alia*, an order requiring America Online, Inc. ("AOL") to disclose the content of certain e-mail communications stored on AOL's servers that were sent or received by an AOL e-mail account (the "Account") set forth in the Application, which was filed under seal. The Order directed the Government to brief: (1) whether opened e-mails are properly considered to be in "electronic storage" and thus not subject to disclosure without a search warrant, pursuant to Section 2703(a), *see Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004); and (2) whether the obtaining of e-mails by the Government from an Internet Service Provider ("ISP") without a search warrant violates the Fourth Amendment or other constitutional provision, *see Warshak v. United States*, 490 F.3d 455 (6th Cir. 2007), *vacated, reh'g en banc granted*, No. 06-4092 (6th Cir. Oct. 9, 2007).

For the reasons that follow, the Court should conclude that *Theofel* was incorrectly decided and that opened e-mails are not within "electronic storage," as the term is defined in 18 U.S.C. § 2510(17) and used in Section 2703(a). Thus, properly interpreted, Section 2703 permits the Government to obtain without a search warrant all opened e-mails that remain stored with third-party electronic communications providers such as AOL. The Court should also determine that *Warshak*, which no longer is entitled to any persuasive weight under the Sixth Circuit's own jurisprudence, *see Montgomery v. Carr*, 101 F.3d 1117, 1128 n.6 (6th Cir. 1996) (noting that

Hon. Michael H. Dolinger
April 4, 2008
Page 2 of 14

case that had been vacated and set for *en banc* rehearing “does not formally exist as persuasive authority”), incorrectly held that Section 2703 was constitutionally flawed. The procedures set forth in 2703(d) meet the Fourth Amendment’s reasonableness standard applicable to searches by subpoena or court order. Accordingly, the portion of the Application seeking an order compelling AOL to disclose the content of e-mail communications sent or received by the Account should be granted.

I. Background

As set forth in the Application, the Federal Bureau of Investigation (“FBI”) has obtained information indicating that the Account has been used to receive images containing child pornography, and has also been used to entice an individual whom the user of the Account believed to be a minor to have sexual intercourse with the holder of the Account. Accordingly, for the reasons set forth in the Application, the Government possesses “specific and articulable facts showing that there are reasonable grounds to believe that the contents of” the electronic communications in the Account “are relevant and material to an ongoing criminal investigation,” 18 U.S.C. § 2703(d), into whether the user of the Account has violated Title 18, United States Code, Sections 2251 (sexual exploitation of children), 2252 (shipment, receipt, or possession of material involving the sexual exploitation of minors), and 2252A (shipment, receipt, or possession of child pornography).

II. Discussion

A. Statutory Framework

Section 2703 of the Stored Communications Act, 18 U.S.C. §§ 2701-2712 (“SCA”), which was passed as part of the Electronic Communications Privacy Act of 1986 (“ECPA”), Pub. L. No. 99-508, sets forth the procedures that law enforcement officials must follow to compel disclosure of certain communications stored by an Internet Service Provider (“ISP”). The structure of Section 2703 is based on Congress’s recognition that an provider of e-mail services offers two conceptually distinct services to its customers. First, an e-mail provider transmits e-mail from one party to another, a service analogous to traditional mail service. Second, and unlike the traditional postal service, e-mail providers offer a storage service for e-mail that is no longer in the course of transmission. After a user sends or receives an e-mail, he or she may choose to have the e-mail service provider store a copy of the e-mail indefinitely on its servers.

The first subsection of Section 2703 sets forth the procedures that must be followed when law enforcement officials seek to obtain access to e-mails that are in the process of being transmitted pursuant to the first service offered by ISPs—the transmission of e-mails from sender to recipient. It states that the contents of e-mail communications that are “in electronic storage in an electronic communications system for one hundred and eighty days or less” may be obtained

Hon. Michael H. Dolinger

April 4, 2008

Page 3 of 14

“only pursuant to a warrant.” 18 U.S.C. § 2703(a). The term “electronic storage” is defined in 18 U.S.C. § 2510(17) as “(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.” See 18 U.S.C. § 2711(1) (stating that definitions set forth in § 2510 also govern definitions of terms in SCA).

The second subsection of § 2703 sets forth the procedures that must be followed to obtain access to e-mails held by ISPs pursuant to the second e-mail-related service that ISPs provide—storage of e-mail that is no longer in the course of transmission. Section 2703(b) requires “a provider of remote computing service to disclose the contents of any wire or electronic communication” that are received by an ISP on behalf of a subscriber, or that are stored on behalf of a subscriber, not only through a search warrant, but also through a subpoena or order under § 2703(d) (“2703(d) order”). 18 U.S.C. § 2703(b). The SCA defines “remote computing service” to mean “provision to the public of computer storage or processing services by means of an electronic communication system.” 18 U.S.C. § 2711(2). Communications that are in “electronic storage” for more than 180 days may also be disclosed pursuant to subpoena or 2703(d) order without requiring issuance of a warrant. 18 U.S.C. § 2703(a).

If the government uses a subpoena or a 2703(d) order to obtain the content of e-mail communications, it is required by § 2703(b)(1)(B) to give prior notice to the subscriber or to comply with delayed notice procedures set forth in Section 2705(a). A 2703(d) order requires the Government to offer “specific and articulable facts showing that there are reasonable grounds to believe that the contents of . . . [the] communication . . . are relevant and material to an ongoing criminal investigation.” 18 U.S.C. § 2703(d). Thus, prosecutors can obtain access to files stored with a remote computing service using a standard lower than probable cause.

B. Previously-Opened Electronic E-mail is Not in “Electronic Storage”

Under the scheme set forth above, only e-mails that are in “electronic storage” for 180 days or fewer are protected from compelled disclosure without a warrant. Analysis of the term “electronic storage,” as defined in Section 2510(17), makes clear that it does not cover e-mails that have been transmitted and opened, but that remain stored on ISPs’ servers.

1. Previously accessed e-mail is not in “electronic storage” as defined by § 2510(17)(A)

“Electronic storage” is defined to mean “(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.” 18 U.S.C. § 2510(17). Previously opened e-mail messages

Hon. Michael H. Dolinger
April 4, 2008
Page 4 of 14

stored by an ISP for a customer do not fall within the scope of subsection (A) of this definition because such e-mail messages are not in “temporary, intermediate storage,” and they are not stored incident to transmission. The courts are in accord that e-mail that has been transmitted to and accessed by the intended recipient is no longer in “temporary, intermediate storage.” See *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114 (3d Cir. 2004) (stating that e-mail in post-transmission storage was not in “temporary, intermediate storage”); *In re Doubleclick Inc. Privacy Litig.*, 154 F. Supp.2d 497, 512 (S.D.N.Y. 2001) (holding that protections for communications in “electronic storage” are “specifically targeted at communications temporarily stored by electronic communications services incident to their transmission—for example, when an e-mail service stores a message until the addressee downloads it”); *Snow v. DIRECT TV, Inc.*, No. 2:04-CV-515FTM33SPC, 2005 WL 1226158, at *3 (M.D. Fla. May 9, 2005) (report and recommendation of magistrate judge) (holding that communications are in “electronic storage” when “stored for a limited time in the middle of a transmission, i.e. when an electronic communication service temporarily stores a communication while waiting to deliver it”), *adopted*, 2005 WL 1226158 (M.D. Fla. May 09, 2005), *aff’d*, 450 F.3d 1314 (11th Cir. 2006); *see also Theofel*, 359 F.3d at 1075 (citing cases holding that subsection (A) of the definition of electronic storage “have limited the subsection’s coverage to messages not yet delivered to their intended recipient”). *Theofel* does not question this proposition. See *Theofel*, 359 F.3d at 1075. Accordingly, e-mail that has been delivered to and accessed by its intended recipient cannot be considered within “electronic storage” within the meaning of 18 U.S.C. § 2510(17)(A).

2. Previously accessed e-mail is not in “electronic storage” as defined by § 2510(17)(B)

Previously accessed e-mail which a subscriber chooses to leave on an ISP’s server also does not fall within the scope of § 2510(17)(B), the “backup” subsection of the definition of electronic storage, which protects “any storage of such communication by an electronic communication service for purposes of backup protection of such communication.”

Following established Supreme Court precedent, “[s]tatutory construction must begin with the language employed by Congress and the assumption that the ordinary meaning of that language accurately expresses the legislative purpose.” *Shi Liang Lin v. U.S. Dep’t of Justice*, 494 F.3d 296, 305 (2d Cir. 2007) (*en banc*) (quoting *Park ‘N Fly, Inc. v. Dollar Park & Fly, Inc.*, 469 U.S. 189, 194 (1985)). Here, an examination of the text and legislative purpose behind the statutory provision reveal that the provision references backup copies maintained by the ISP of the “temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof” referenced in subsection (A) of the statute, not to opened e-mails remaining on an ISP’s server that may or not serve a “backup” function for the subscriber. The language of subsection (B) explicitly references the definition of subsection (A) by stating that it is protecting “storage of *such communication* . . . for purposes of backup protection of *such communication*,” 18 U.S.C. § 2510(17)(B) (emphasis added)—i.e., the communication described

Hon. Michael H. Dolinger

April 4, 2008

Page 5 of 14

in subsection (A) of the same statute. Read in conjunction with subsection (A), subsection (B) thus references a backup copy made by an ISP (or other electronic communication service) of a communication that was *itself* in temporary, intermediate storage. *See Rabin v. Wilson-Coker*, 362 F.3d 190, 196 (2d Cir. 2004) (referencing canon of construction holding that “a statute is to be considered in all its parts when construing any one of them” (quoting *Lexecon Inc. v. Milberg Weiss Bershad Hynes & Lerach*, 523 U.S. 26, 36 (1998))).

This interpretation of Section 2510(17)(B) also accords with the intent of the drafters of the ECPA. *See Rabin*, 362 F.3d at 196-97 (referencing canon requiring that “the interpretation given to the statute must be consistent with the congressional purpose for enacting it” (citing *Holloway v. United States*, 526 U.S. 1, 9 (1999))). In 1986, providers of electronic communication services commonly stored copies of files to protect against system failure. It would have made little sense for Congress to have provided strong protections to e-mail stored during the course of transmission, while providing little protection for the backup copies of those e-mails made by the service providers while in transmission. Thus, Congress crafted § 2510(17) to protect backup copies made of e-mail being stored incident to transmission, as well as the e-mail communications themselves while in transmission. For example, the House Report on the ECPA states:

The Committee recognized that electronically stored communications can be of two types. The first type of stored communications are those associated with transmission and incident thereto. The second type of storage is of a back-up variety. Back up protection preserves the integrity of the electronic communication system and to some extent preserves the property of the users of such a system.

H.R. Rep. No. 99-647 (“House Report”), at 68 (1986). By including backup protections within the definition of “electronic storage,” Congress intended to ensure that backups made of communications in storage incident to transmission would receive the same degree of protection as the underlying communications. *See* 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, 1217 n.61 (2004) [hereinafter “Kerr”] (explaining why “the backup provision of the definition of electronic storage . . . exists only to ensure that the government cannot make an end-run around the privacy-protecting [rules protecting e-mail stored by an electronic communication service] by attempting to access backup copies of unopened e-mails made by the ISP for its administrative purposes” and noting that provision was likely inspired by Office of Technology Assessment

Hon. Michael H. Dolinger

April 4, 2008

Page 6 of 14

report highlighting privacy risks raised by "backup copies," which it referred to as copies retained by the ISP "for [a]dministrative purposes").¹

This interpretation of Section 2510(17)(B) was erroneously rejected by *Theofel*. In *Theofel*, the Ninth Circuit held that e-mail messages located on an ISP's server were in electronic storage, whether or not they had been previously accessed, because it concluded that retrieved e-mail left by a subscriber on an ISP's server could be considered storage by the subscriber "for purposes of backup protection," 18 U.S.C. § 2510(17)(B). According to the Ninth Circuit, "[a]n obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again—if, for example, the message is accidentally erased from the user's own computer." *Theofel*, 359 F.3d at 1075. Thus, the *Theofel* court concluded, "[t]he ISP copy of the message functions as a 'backup' for the user,"

¹ The language and legislative history of § 2704 of the SCA further confirm that the "backup" provision of § 2510(17)(B) references backup copies of electronic communications incident to their transmission. Section 2704, which was drafted contemporaneously with § 2510(17)(B), provides that a subpoena or court order may include a provision requiring a service provider to "create a backup copy" of the contents of targeted electronic communications. 18 U.S.C. § 2704(a)(1). This language demonstrates that the drafters of the SCA understood the term "backup copy" to mean a duplicate copy made by a service provider to ensure preservation of communications, not to any copy of an e-mail that the subscriber may choose to retain on the ISP's for the user's own "backup purposes," or for some other purpose unknown to the ISP or the Government. See Kerr, *supra*, at 1217 n.61 ("Section 2704 makes clear that the SCA uses the phrase 'backup copy' in a very technical way to mean a copy made by the service provider for administrative purposes.").

Moreover, subsequent legislative discussion of the statute confirms Congress's continued understanding that previously opened e-mail that the user chooses to retain on an ISP's server is not in "electronic storage." The House Report on the USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001), explained Congress's understanding that "2703(a) requires a search warrant to compel service providers to disclose *unopened* e-mails." H.R. Rep. No. 107-236(I), at 57 (2001) (emphasis added). Because warrants under § 2703(a) are required only for electronic communications in "electronic storage," this statement is further evidence that Congress did not intend opened e-mail to fall within the scope of "electronic storage." See *Hayden v. Pataki*, 449 F.3d 305, 320 (2d Cir. 2006) (*en banc*) (noting that while "the view of a later Congress does not establish definitively the meaning of an earlier enactment, . . . it does have persuasive value" (quoting *Gozlon-Peretz v. United States*, 498 U.S. 395, 406 (1991))).

Hon. Michael H. Dolinger

April 4, 2008

Page 7 of 14

and “storage under these circumstances thus literally falls within the statutory definition” of “electronic storage” set forth in Section 2510(17)(B). *Id.*

The Ninth Circuit’s holding is incorrect, and this Court should reject it. It does not accord with the plain meaning or legislative intent of Section 2510(17)(B), which make clear that “backups” are referenced as preserving “the integrity of the electronic *communication* system,” House Report at 68 (emphasis added), rather than the integrity of an individual subscriber’s system for backing up his or her own stored e-mail. Moreover, by making the determination of whether an e-mail is stored for “backup purposes” depend on the intent of the subscriber in retaining a copy of opened e-mail with the ISP (and on whether the subscriber also stores a copy of the e-mail on his own personal computer), *Theofel* would make it impossible for ISPs and investigators to determine which opened e-mails could be subject to search—an absurd result that plainly could not have been contemplated by Congress. See Kerr, *supra*, at 1217 n.61 (“The apparently subjective nature of the line [drawn by *Theofel*] makes it all the less likely from the standpoint of statutory interpretation: investigators must be able to classify a file before they know what legal process they must obtain to compel it, and normally they cannot tell when a user or service provider no longer needs the file or is storing it for backup purposes.”).

Theofel’s interpretation would reduce protections available to the subscriber. Under the Ninth Circuit’s approach to “electronic storage,” backups made by an ISP to protect against system failure receive limited protection under the SCA. Providers of electronic communication service may make backups of their system and archive these backups for long periods of time. According to the Ninth Circuit’s reasoning, an e-mail message included in such a backup is in “electronic storage” only until the underlying message is deleted: “Where the underlying message has expired in the normal course, any copy is no longer performing any backup function.” *Theofel*, 359 F.3d at 1076. Thus, under *Theofel*, a user who has deleted an e-mail message will be unprotected from disclosure of copies of the e-mail which had been made previously for purposes of backup protection. In contrast, under the Government’s interpretation of the statute, if an ISP makes backup copies of e-mail being stored incident to transmission, such storage will remain “electronic storage” pursuant to § 2510(17)(B) that is protected from disclosure under the provisions of § 2703(a).

It is not surprising that *Theofel*’s overly expansive interpretation of “electronic storage” has been explicitly rejected by several courts and commentators. See *United States v. Jackson*, No. 07-0035(RWR), 2007 WL 3230140 (D.D.C. Oct. 30, 2007) (rejecting motion to quash 2703(d) order for content of text messages); *In re Grand Jury Subpoena Issued Pursuant to 18 U.S.C. Section 2703(b)(1)(B)*, slip op. at 6-7 (M.D. Ga. Apr. 29, 2005) (attached as Exhibit A) (stating that “this Court chooses not to follow the Ninth Circuit interpretation of this statutory scheme”); see also *In re Doubleclik*, 154 F. Supp. 2d at 512 (noting that statutory provision incorporating definition of “electronic storage” “only protects electronic communications stored for a limited time in the middle of a transmission”); *Bansal v. Russ*, 513 F. Supp. 2d 264, 276

Hon. Michael H. Dolinger
April 4, 2008
Page 8 of 14

(E.D. Pa. 2007) (concluding that “[t]he Stored Communications Act ... does not prohibit ... obtaining ‘opened’ emails”); *Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001) (“[R]etrieval of a message from post-transmission storage is not covered by the Stored Communications Act. The Act provides protection only for messages while they are in the course of transmission.”), *aff’d on other grounds*, 352 F.3d 107 (3d Cir. 2003); Kerr, *supra*, at 1217 (describing *Theofel* as “quite implausible and hard to square with the statutory text”). *But see Kaufman v. Nest Seekers, LLC*, No. 05 Civ. 6782, 2006 WL 2807177, at *7 (S.D.N.Y. Sept. 26, 2006) (citing *Theofel* with approval); *Bailey v. Bailey*, No. 07-11672, 2008 WL 324156, at *6 (E.D. Mich. Feb. 6, 2008) (same).

Accordingly, this Court should reject *Theofel* and confirm that the “backup” portion of the definition of “electronic storage” is limited to storage by an ISP for its own actual backup protection incident to transmission. Thus, the Government may obtain the content of opened e-mails in the Account that are less than 181 days old.

C. Section 2703 Does Not Violate the Fourth Amendment

Turning to the next issue on which the Court requested briefing, the obtaining of e-mails stored by a third-party ISP without a search warrant does not violate the Fourth Amendment or any other constitutional provision. *Warshak v. United States*, 490 F.3d 455 (6th Cir. 2007), *vacated, reh’g en banc granted*, No. 06-4092 (6th Cir. Oct. 9, 2007), which held that 2703(d) orders violated the Fourth Amendment to the extent they permitted a search of an e-mail subscriber’s account without notice to the subscriber, absent proof that the subscriber had no reasonable expectation of privacy in his e-mail account, *see id.* at 475-76, was wrongly decided and appropriately was vacated by the Sixth Circuit sitting *en banc*. Subpoenas and Section 2703(d) orders may properly be used to obtain e-mail communications left by subscribers on ISPs’ servers (other than unopened e-mail communications less than 180 days old, per Section 2703(a)) without violating the Constitution. Compulsory legal process directed at third parties is governed by a reasonableness standard, rather than the Warrant Clause’s “probable cause” standard. *See* U.S. Const. amend. IV (protecting against “unreasonable searches and seizures” and declaring that “no warrants shall issue, but upon probable cause”). Section 2703 strikes a reasonable balance between e-mail subscribers’ privacy interest in e-mails stored with third-party ISPs and the Government’s interest in enforcing criminal law. Accordingly, it should be enforced.

1. Legal Principles

The Court has long held that the Fourth Amendment’s reasonableness standard, rather than the probable cause standard of the Amendment’s Warrant Clause, applies to subpoenas or court orders compelling disclosure of information to the Government. *See Oklahoma Press Pub. Co. v. Walling*, 327 U.S. 186 (1946) (holding that cases, “in so far as they apply merely to the

Hon. Michael H. Dolinger

April 4, 2008

Page 9 of 14

production of corporate records and papers in response to a subpoena or order authorized by law and safeguarded by judicial sanction, . . . at the most guards against abuse only by way of too much indefiniteness or breadth . . . if also the inquiry is one the demanding agency is authorized by law to make and the materials specified are relevant. The gist of the protection is in the requirement . . . that the disclosure sought shall not be unreasonable.”); *see also Donovan v. Lone Steer, Inc.*, 464 U.S. 408, 413-15 (1984) (citing *Oklahoma Press* with approval).

A series of Supreme Court decisions authorize as reasonable Government actions that compel third parties holding information that the target of an investigation deems confidential to disclose that information upon receipt of a subpoena or other lawful process. In *United States v. Miller*, 425 U.S. 435 (1976), the Court rejected a defendant’s argument that his Fourth Amendment rights were violated when the Government obtained by subpoena banking information that he asserted was private, stating that “[t]his 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.” *Id.* at 443; *see also Hoffa v. United States*, 385 U.S. 293, 302 (1966) holding that no Fourth Amendment rights were violated by informant’s disclosure of contents of conversation in hotel room on grounds that defendant “was not relying on the security of the hotel room; he was relying upon his misplaced confidence that [the informant] would not reveal his wrongdoing”).

In *SEC v. Jerry T. O’Brien, Inc.*, 467 U.S. 735 (1984), the Supreme Court unanimously reversed an appellate decision that had required the SEC to notify targets of an SEC investigation when it sent subpoenas to third parties seeking records concerning the targets. *See id.* at 740. Relying in part on *Miller*, the Court held that the targets of the investigation could not “invoke the Fourth Amendment in support of” a rule requiring notice when a third-party subpoena seeking records related to the targets issued because, “when a person communicates information to a third party *even on the understanding that the communication is confidential*, he cannot object if the third party conveys that information or records thereof to law enforcement authorities.” *Id.* at 743 (emphasis added) (citing *Miller*, 425 U.S. at 443). According to the Court, *Miller* and related cases “disable [the targets] from arguing that notice of subpoenas issued to third parties is necessary to allow a target to prevent an unconstitutional search or seizure of his papers.” *Id.*; *see United States v. Daccarett*, 6 F.3d 37, 50 (2d Cir. 1993) (stating that in *O’Brien*, the Court held “that a ‘target’ of an investigation has no right to notice of subpoenas issued to third parties”); *see also Couch v. United States*, 409 U.S. 322, 335-36 (1973) (finding no Fourth Amendment bar to obtaining defendant’s personal financial records left with her accountant through subpoena to accountant).

The Court also rejected the targets’ arguments that permitting the SEC to issue subpoenas to third-party recordholders without notifying them violated the Fifth Amendment’s Due Process

Hon. Michael H. Dolinger
April 4, 2008
Page 10 of 14

Clause or the Sixth Amendment's Confrontation Clause. *See id.* at 742 ("[N]either the Due Process Clause of the Fifth Amendment nor the Confrontation Clause of the Sixth Amendment is offended when a federal administrative agency, without notifying a person under investigation, uses its subpoena power to gather evidence adverse to him. The Due Process Clause is not implicated under such circumstances because an administrative investigation adjudicates no legal rights, and the Confrontation Clause does not come into play until the initiation of criminal proceedings.") (internal citations omitted). Nor, according to the Court, can a target who is not notified of subpoenas relating to the target served on third parties

seek shelter in the Self-Incrimination Clause of the Fifth Amendment. The rationale of this doctrine is that the Constitution proscribes only compelled self-incrimination, and, whatever may be the pressures exerted upon the person to whom a subpoena is directed, the subpoena surely does not "compel" anyone else to be a witness against himself. If the "target" of an investigation by the SEC has no Fifth Amendment right to challenge enforcement of a subpoena directed at a third party, he clearly can assert no derivative right to notice when the Commission issues such a subpoena.

Id. at 742-43 (internal footnote and citations omitted).

2. The Government's 2703(d) Application Complies with the Constitution

O'Brien and related cases establish that Section 2703 creates a fully constitutional framework governing the circumstances in which the Government may obtain the content of subscribers' e-mails from an ISP or other electronic communication service provider. Accordingly, the portion of the Government's Application seeking an order compelling AOL to disclose the content of e-mails held in the Account is fully lawful and should be granted.

As set forth above, the first two subsections of Section 2703 reflect the different e-mail-related services provided by an ISP and the different degrees of protection from Government investigations available to each. The first subsection, Section 2703(a), provides the highest level of protection to e-mails that are in transit or are not yet read by their intended recipients by prohibiting disclosure of e-mails that are in "electronic storage" for 180 days or fewer — *i.e.*, e-mails in "temporary, intermediate storage . . . incidental to the[ir] electronic transmission" and backups of those e-mails, 18 U.S.C. § 2510(17), *see supra* (discussing interpretation of Section 2510(17))—without a warrant that issues upon probable cause. The significant protections accorded to e-mail that effectively is "in transit" reflects the close analogy between e-mail traffic and traffic of mail or telephone communications, which the Supreme Court has held cannot be disclosed without a warrant. *See Berger v. New York*, 388 U.S. 41 (1967) (holding that no wiretapping of telephone conversations is permitted except pursuant to warrant based on

Hon. Michael H. Dolinger
April 4, 2008
Page 11 of 14

probable cause); *Katz v. United States*, 389 U.S. 347 (1967) (applying warrant requirement to eavesdropping on telephone conversation in telephone booth); *United States v. Van Leeuwen*, 397 U.S. 249, 251 (1970) ("It has long been held that first-class mail such as letters and sealed packages subject to letter postage . . . is free from inspection by postal authorities, except [with a warrant].").

As to e-mails that have been opened by their intended recipients or stored by the ISP for more than 180 days, however, ISPs serve as a storage service for e-mail that is no longer in the process of transmission. E-mails in this category may be obtained, not only on the basis of a warrant, *see* 18 U.S.C. § 2703(b)(1)(A), but also on the basis of a subpoena or court order pursuant to Section 2703(d), *see id.* § 2703(b)(1)(B). Furthermore, notice to the subscriber may be delayed under Section 2705(a), and an ISP may be compelled pursuant to Section 2705(b) to delay its notice to a subscriber. The lesser protections accorded to e-mail of this type reflect the close analogy between ISPs serving in this role and other third parties that are entrusted with information but that are nonetheless compelled to disclose that information in response to a subpoena or other compulsory process—for example, the targets of the investigation in *O'Brien* and *Couch*. *See Kerr, supra*, at 1234 (noting that "[t]he apparent thinking behind the lower thresholds for government access of both permanently stored files and unretrieved files stored for more than 180 days is that the lower thresholds track Supreme Court precedents interpreting the Fourth Amendment"). Section 2703 tracks the relevant Supreme Court precedents because a subscriber voluntarily leaves e-mails with an ISP once they are received and read. Instead of doing so, the subscriber could, for example, delete e-mails once they are read or store them on a computer or other backup facility maintained by the subscriber. By voluntarily choosing to store opened e-mails with an ISP, a subscriber assumes the risk that the third-party ISP will disclose the content of those communications under *O'Brien* and related cases.

In summary, the structure of Section 2703 reflects Congress's considered and reasonable judgment concerning the different procedural protections available for different forms of search methods, and as such should be found fully constitutional. *See* S. Rep. 99-541, at 5 (1986) *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3559 (noting committee's view that the ECPA "represents a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies"). "Because there is a strong presumption of constitutionality due to an Act of Congress, especially when it turns on what is reasonable, obviously the Court should be reluctant to decide that a search thus authorized by Congress was unreasonable and that the Act was therefore unconstitutional." *United States v. Watson*, 423 U.S. 411, 416 (1976) (internal alterations and quotation marks omitted). This Court should not disrupt the delicate balance struck by Congress in crafting the SCA by holding that the presumption of its constitutionality has been overcome.

The Court should be particularly reluctant to upset the balance struck by Congress in this case, in which the subscriber to the Account does not have a reasonable expectation that opened

Hon. Michael H. Dolinger

April 4, 2008

Page 12 of 14

e-mails which he or she voluntarily stored on AOL's server will remain shielded from disclosure pursuant to a 2703(d) order or other lawful process. This is so because of the explicit warning to subscribers set forth in AOL's Privacy Policy, which is posted prominently on its website and which warns users that:

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); in other circumstances in which AOL believes the AOL Network is being used in the commission of a crime; when we have a good faith belief that there is an emergency that poses a threat to the safety of you or another person; or when necessary either to protect the rights or property of AOL, the AOL Network or its affiliated providers, or for us to render the service you have requested.

Privacy Policy, America Online, Inc., available at http://about.aol.com/aolnetwork/aol_pp (last visited Mar. 28, 2008); see also *Terms of Use*, America Online, Inc., available at http://about.aol.com/aolnetwork/aolcom_terms (last visited Apr. 4, 2008) ("Your ongoing use of AOL.COM signifies your consent to the information practices disclosed in our Privacy Policy."). AOL's privacy policy, which users of AOL agree to follow, thus warns users that any expectation of privacy that they may have in communications they choose to store with an ISP is constrained by their consent to disclosure of those communications pursuant to the Government and to AOL itself in a variety of circumstances. See also *United States v. Jacobsen*, 466 U.S. 109, 117 (1984) (holding that Federal Express employees could search a package entrusted to it by a customer and provide resulting evidence of criminal activity to Government without violating Fourth Amendment, noting that "[o]nce frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information"); *United States v. Young*, 350 F.3d 1302, 1308-09 (11th Cir. 2003) (holding that Federal Express's terms of service, which allowed it to inspect customers' packages, gave it authority to consent to a warrantless government search of a package).

To the extent that the Court considers the Sixth Circuit's vacated decision in *Warshak*, the above discussion makes clear that *Warshak* misconstrued Fourth Amendment law by conflating the heightened Fourth Amendment protections available to private communications transmitted through third-party ISPs with the lesser Fourth Amendment protections afforded to already-transmitted communications voluntarily stored with third-party ISPs. The *Warshak* court found that "individuals maintain a reasonable expectation of privacy in e-mails that are stored with, or sent or received through, a commercial ISP," 490 F.3d at 473, but it failed to give proper deference to Congress's determination in Section 2703 that e-mails that are voluntarily "stored with" a third-party ISP after being read are entitled to lesser Fourth Amendment protections than e-mails that are "sent or received through" an ISP.

Hon. Michael H. Dolinger

April 4, 2008

Page 13 of 14

In addition, *Warshak*'s holding that when an ISP engages in automated scanning of the content of e-mail "for signs of pornography or a virus," it "does not invade an individual's content-based privacy interest" in e-mail, 490 F.3d at 475, was wrong for two reasons. First, whether an e-mail contains viruses, spam, or pornography is fundamentally a content-based distinction; it concerns the "substance, purport, or meaning" of the communication. 18 U.S.C. § 2510(8). Second, in *Smith v. Maryland*, 442 U.S. 735 (1979), the Supreme Court rejected the argument that for Fourth Amendment purposes, a communication provider's receipt of information—in this case, telephone numbers—via automated equipment differed from receipt via live operator. Instead, the Court decided that all information voluntarily conveyed to the communications provider was subject to disclosure. *See id.* at 744-45 ("The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber. Petitioner concedes that if he had placed his calls through an operator, he could claim no legitimate expectation of privacy. We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate.") (internal citation omitted).

Moreover, *Warshak* is conceptually incoherent. *Warshak* affirmed, as modified, a preliminary injunction prohibiting disclosure of the content of e-mails "pursuant to a court order issued under 18 U.S.C. § 2703(d), without either (1) providing the relevant account holder or subscriber prior notice and an opportunity to be heard, or (2) making a fact-specific showing that the account holder maintained no expectation of privacy with respect to the ISP, in which case only the ISP need be provided prior notice and an opportunity to be heard." 490 F.3d at 482. But if the problem with Section 2703 is that it would permit disclosure of the content of stored e-mail communications without a warrant and on less than probable cause, then permitting an account holder with "prior notice and an opportunity to be heard" would do little to rectify this alleged violation. Instead, all that the injunction in *Warshak* accomplishes is a violation of the Fourth Amendment principles set forth in *O'Brien*, in which the Court unanimously rejected an analogous judicially-imposed requirement that the Government notify targets of an investigation whenever it subpoenaed third parties for records concerning the targets. *See* 467 U.S. at 741-43.

Hon. Michael H. Dolinger

April 4, 2008

Page 14 of 14

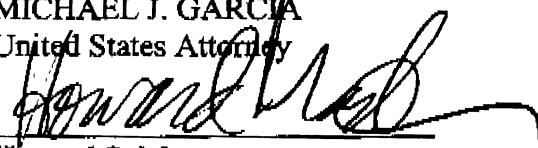
III. Conclusion

For the reasons stated above, the Court should grant the portion of the Application seeking an order compelling AOL to disclose the content of e-mails held in the Account.

Respectfully submitted,

MICHAEL J. GARCIA
United States Attorney

By:


Howard S. Master
Assistant United States Attorney
Southern District of New York
(212) 637-2248

cc: Kevin Bankston, Esq., Electronic Frontier Foundation (by facsimile)

EXHIBIT A

FILED
U.S. DISTRICT COURT
FOR THE MIDDLE DISTRICT OF GEORGIA
ALBANY DIVISION

06 JUN 21 AM 9:45

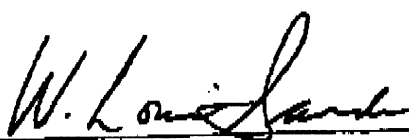
WKS
DEPUTY CLERK

IN THE MATTER OF A GRAND :
JURY SUBPOENA ISSUED :
PURSUANT TO TITLE 18, : CASE NO:
UNITED STATES CODE, :
SECTION 2703(b)(1)(B) : UNDER SEAL

ORDER GRANTING MOTION TO UNSEAL

The United States of America having moved to unseal the Court's Order dated April 29, 2005, and the same having been read and considered, the same is hereby GRANTED. The clerk is directed to unseal the Motion to Compel Compliance, the Court's Order, together with this Motion to Unseal and Order, and to mark the same "Unsealed" as of this date.

SO ORDERED this 21st day of June, 2006.



W. LOUIS SANDS
CHIEF UNITED STATES DISTRICT JUDGE
MIDDLE DISTRICT OF GEORGIA

PRESENTED BY:

/S JIM CRANE
ASSISTANT U.S. ATTORNEY

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF GEORGIA
ALBANY DIVISION

IN THE MATTER OF A GRAND JURY :
SUBPOENA ISSUED PURSUANT TO :
TITLE 18, UNITED STATES CODE, :
SECTION 2703(b)(1)(B) :

CASE NO:
UNDER SEAL

ORDER

The United States of America (the "Government") moves this Court to issue an order compelling the compliance by MSN Hotmail ("Hotmail") with a grand jury subpoena issued pursuant to 18 U.S.C. § 2703(b)(1)(B) for the subscriber information listed in Exhibit 1 to the subpoena.

Hotmail opposes complying with the subpoena.¹ Hotmail argues that the files in question are located in California and that controlling Ninth Circuit precedent requires a search warrant in order for the Government to obtain the items in question. As explained in more detail below, the Government argues to the contrary that the material sought is subject to a grand jury subpoena. Hotmail states that it has every desire to cooperate in the Government's criminal investigation but believes in good faith that a search warrant is required. Hotmail, however, has stated that if ordered to comply with the subpoena it would not otherwise object. See, Letter from Hotmail.

The current investigation involves the offering and transmission of child pornography via

¹ Technically, Hotmail has not filed a pleading in opposition to the subpoena, but has responded by letter to the Government wherein it explains its position. The Government attached a copy of the letter to its instant motion.

the internet. On November 30, 2004, Michael Aaron O'Keefe ("O'Keefe") was convicted by a jury in the United States District Court for the Middle District of Georgia of offering and advertising child pornography in violation of 18 U.S.C. § 2251(c), receiving child pornography in violation of 18 U.S.C. § 2252(a)(2), and possessing child pornography in violation of 18 U.S.C. § 2252(a)(4). Essentially, O'Keefe formed a website containing images of child pornography. In order for a third party to have access to the images, the third party would have to email O'Keefe three images of child pornography. Upon receipt the third party would have access to all of the images on O'Keefe's website. O'Keefe's website was in operation for approximately 18 days before a federal investigation ensued and the internet service provider ("ISP") shut down the site. During that period there were more than 350 requests for membership of which O'Keefe granted membership to the site to 38 individuals. In other words, those 38 individuals allegedly provided O'Keefe with at least three images of child pornography in order to attain membership.

Five of those 38 members were discovered by agents of Immigration and Customs Enforcement ("ICE") to have utilized email accounts provided by MSN Hotmail. The five accounts, and the accounts subject to the grand jury subpoena, are:

jbanka6969@hotmail.com
kdejrhgodsilkikth@hotmail.com
mpeutherland@hotmail.com
euals12@hotmail.com
umnygodess@hotmail.com

On January 24, 2005, a grand jury sitting in the Middle District of Georgia issued a subpoena to Hotmail seeking the contents of wire or electronic communications in those Hotmail accounts. The subpoena, however, excepted from its scope unopened incoming communications not more than 180 days old. The Government also complied with the delayed notice procedure

of 18 U.S.C. § 2705(a)(1).

Hotmail partially complied with the subpoena. Hotmail produced all communications that were more than 180 days old. Hotmail has failed to produce opened communications that were less than 181 days old. Hotmail's failure to produce is premised on the holding of Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004), cert. Denied, 125 S.Ct. 48 (2004), which requires a search warrant for the unproduced communications.

DISCUSSION

The question before the Court is whether the an ISP can be compelled to produce copies of previously opened email communications pursuant to a grand jury subpoena issued pursuant to 18 U.S.C. § 2703(b)(1)(B). The key to resolving this issue is understanding the meaning of "electronic storage" as that term is defined in 18 U.S.C. § 2510(17).

This case involves the intersection of two statutory provisions; the Wire and Electronic Communications Interception and Interception of Oral Communications Act ("Wiretap Act"), 18 U.S.C. §§ 2510 *et. seq.*, and the Stored Wire and Electronic Communications and Transactional Records Access Act ("Stored Communications Act"), 18 U.S.C. §§ 2701 *et. seq.* The Stored Communications Act governs the disclosure by subpoena or warrant electronic communications maintained on computers. The Wiretap Act governs the prohibition of disclosure of electronic and wire communications in general. Section 2711 of the Stored Communications Acts refers the reader to § 2510 of the Wire Tap Act for definitions. 18 U.S.C. § 2711.

Section 2703 provides the statutory authority for government access to electronic communications (emails) maintained or transmitted by computer. Section 2703(a) provides that the government may require disclosure of emails from a internet service provider ("ISP"):

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. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

18 U.S.C.A. § 2703.

Subsection (b) provides:

(b) Contents of wire or electronic communications in a remote computing service.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

(A) 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 by a court with jurisdiction over the offense under investigation or equivalent State warrant; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

18 U.S.C.A. § 2703(b).

Section 2703(b)(2) provides:

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

18 U.S.C.A. § 2703(b)(2).

Under § 2703, a plain reading of the statute reveals that a warrant is required if the communication sought by the government "is in electronic storage." 18 U.S.C. § 2703(a). A warrant can be used but is not required for communications that are "held or maintained" by the ISP "on behalf of ... a subscriber or customer" and the ISP provider maintains the communication "solely for the purpose of providing storage or computer processing services to such subscriber or customer." 18 U.S.C. § 2703(b)(2).

At first glance it seems that the phrase "electronic storage" and "storage" in § 2703(a) and § 2703(b)(2) mean the same thing. "Electronic storage," however, has a distinct definition and that definition is found in the Wiretap Act. Section 2510(17) defines "electronic storage" as:

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

18 U.S.C. § 2510(17).

"Electronic storage," therefore, is the storage of an email that is incidental to transmission and for the purposes of backup protection of the ISP. "Storage" as used in § 2703(b) is storage provided solely for the purpose of storage for the customer or subscriber. Therefore, a warrant is required for emails held by the ISP that are maintained as an incident of transmission

and for the purposes of backup of the system. A subpoena can be used to obtain emails of a subscriber that are maintained by the ISP for storage for the customer.

In Theofel v. Farley-Jones, 359 F.3d 1066 (9th Cir. 2004), cert. denied, 125 S.Ct. 48 (2004), the Ninth Circuit while recognizing the distinctive definition of "electronic storage" found that storage of any email, after access, for backup, either for the ISP or the subscriber constituted electronic storage, and thereby, requiring a warrant for its production. The Court noted that other courts and the government had taken a contrary view. Fraser v. Nationwide Mutual Ins. Co., 135 F.Supp.2d 623 (E.D. Pa. 2001); In re Doubleclick Inc. Privacy Litigation, 154 F.Supp.2d 497 (S.D.N.Y. 2001).² It does not appear that any court in the Eleventh Circuit has addressed this issue.

Further evidence that the Government's interpretation of this statutory scheme is illustrated by further code sections. Section 2704 allows the government to request the ISP to create a backup copy of the "contents of the electronic communications sought" in order to preserve the evidence. 18 U.S.C. § 2704(a). If the information sought was maintained for purposes of backup of the ISP system this section would be redundant. Likewise, Section 2702 which provides for limited voluntary disclosure also makes the distinction between emails in "electronic storage" and emails stored on behalf of the customer and subscriber. 18 U.S.C. § 2702.


Therefore, this Court chooses not to follow the Ninth Circuit interpretation of this

² Though not an issue, these Courts and the Government draw a distinction between "opened" and "unopened" emails, stating essentially that unopened emails may require a warrant. The Government is not seeking disclosure of unopened emails, and therefore, the Court does not opine on whether such emails are accessible via a subpoena or a warrant.

statutory scheme as persuasive authority. The unopened emails in question and maintained by Hotmail are not in "electronic storage" and therefore, may be compelled to produce the emails through a grand jury subpoena. Further, the Court finds that the Ninth Circuit interpretation of whether the emails are accessible via a subpoena is not controlling in this situation as the grand jury subpoena was issued pursuant to this Court's authority and can be enforced through its authority.

The Government's request to enforce the grand jury subpoena is GRANTED. Further, Hotmail is ordered not to notify the customers or subscribers of the enforcement of the subpoena or the production of the emails in question, unless such notification is in compliance with the delayed notification provisions of 18 U.S.C. § 2705.

SO ORDERED, this 2nd day of April, 2005.


W. LOUIS SANDS, CHIEF JUDGE
UNITED STATES DISTRICT COURT