IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

STEVEN WARSHAK,	:	**Civil Action No. 01:06 CV 357-UNA**
Plaintiff,	:	
v.	:	**ORAL ARGUMENT REQUESTED**
UNITED STATES OF AMERICA,	:	
Defendant	:	

MOTION FOR ISSUANCE OF A
TEMPORARY RESTRAINING ORDER AND/OR PRELIMINARY INJUNCTION

Now comes the Plaintiff, Steven Warshak, by and through counsel, and hereby moves the Court, pursuant to Fed.R.Civ.P. 65, for a Temporary Restraining Order, with notice to the government and an opportunity to be heard, and/or the issuance of a Preliminary Injunction as requested in his Complaint in this matter. As grounds and reasons therefore, the Plaintiff respectfully states the following:

1. On or about June 3, 2006, the Plaintiff received a letter from the government dated May 31, 2006 that disclosed to the Plaintiff, for the first time, that the government had secured orders pursuant to the Stored Communications Act, 18 U.S.C. §2703(d), which compelled various Internet Service Providers ("ISP") to produce to the government the electronic mail ("email") of the Plaintiff.

2. The so-called §2703(d) orders sought and secured by the government, which caused various ISP's to produce thousands of the Plaintiff's emails, violated (1) the Fourth Amendment to the United States Constitution, insofar as they ordered the search

and/or seizure of private and closed email content communications on a showing of less than probable cause and without a warrant, and (2) the Stored Communications Act ("SCA"), codified at 18 U.S.C. §2701 et seq., itself, insofar as they ordered the search and/or seizure of the content of private email communications in electronic storage for less than 181 days on a showing of less than probable cause and without a warrant.

3. On or about June 12, 2006, Warshak filed a Complaint seeking declaratory judgment that the SCA is unconstitutional, on its face and as applied in this case, because it allows the government to seize and search a closed container—private email communications stored on an ISP server—without a search warrant and upon a showing of less than probable cause, in violation of the rights and guarantees afforded the Plaintiff by the Fourth Amendment to the United States Constitution, as well as declaratory judgment that the Orders issued in this case violate the SCA because the Orders specifically exclude from the definition of "electronic storage" "any email communications received by the specified accounts that the owner or user of the account has already accessed, viewed, or downloaded", without regard for whether the email communications were more or less than 180 days old, and the Orders therefore compelled the production of emails in "electronic storage" (as properly and lawfully defined and interpreted) less than 180 days without a warrant and upon a showing of less than probable cause.

4. In his Complaint, the Plaintiff also sought a preliminary and permanent injunction preventing the government from further unconstitutional and/or unlawful implementation and/or use of the SCA to access any email communications of the Plaintiff.

5. Since filing the Complaint, the Plaintiff has sought assurances from the government that it would voluntarily cease utilizing the SCA to secure similar orders in relation to the Plaintiff and his email communications. The government has advised that it will not provide any such assurances.

6. The Plaintiff respectfully contends that there is a substantial likelihood he will succeed on the merits of his Complaint, that irreparable harm will result if a Temporary Restraining Order and a Preliminary Injunction are not issued, that the impact on the public interests is significant in this case, and that there is a substantial possibility of grave harm to others if a Temporary Restraining Order and a Preliminary Injunction are not issued. Therefore, the Plaintiff respectfully requests that a balancing of these factors clearly warrants the issuance of a Temporary Restraining Order and Preliminary Injunction.

Wherefore, the Plaintiff respectfully requests that the within motion be granted.

The Plaintiff respectfully relies upon and incorporates herein the memorandum of law being filed herewith in support of the instant motion, as well as the memorandum filed in support of his Complaint.

The Plaintiff respectfully requests a hearing on the within motion at the Court's first opportunity.

Respectfully Submitted,

Steven Warshak,
By His Counsel,

/s/ Martin G. Weinberg
Martin G. Weinberg (Mass. Bar No.#519480)
Admitted Pro Hac Vice
MARTIN G. WEINBERG, P.C.
20 Park Plaza, Suite 905
Boston, MA 02116
Telephone: (617) 227-3700
Facsimile: (617) 338-9538

/s/ Martin S. Pinales
Martin S. Pinales (Ohio Bar No. 0024570)
Candace C. Crouse (Ohio Bar No. 0072405)
Sirkin, Pinales & Schwartz LLP
105 West Fourth Street, Suite 920
Cincinnati, Ohio 45202
Telephone: (513) 721-4876
Facsimile: (513) 721-0876

Dated: June 30, 2006

CERTIFICATE OF SERVICE

I hereby certify that a true copy of the foregoing document was served on the 29th day of June 2006 by electronic filing upon all parties in the above-captioned case, as well as by electronic mail on this date.

/s/ Martin G. Weinberg
Martin G. Weinberg

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

STEVEN WARSHAK,	:	**Civil Action No. 1:06 CV 357-UNA**
Plaintiff,	:	
v.	:	
	:	**ORAL ARGUMENT REQUESTED**
UNITED STATES OF AMERICA,	:	
Defendant	:	

MEMORANDUM IN SUPPORT OF ISSUANCE OF A TEMPORARY RESTRAINING ORDER AND/OR PRELIMINARY INJUNCTION

I. Introduction

The government sought and secured numerous orders pursuant to a section of the Stored Communications Act, 18 U.S.C. §2703(d), which compelled various Internet Service Providers ("ISP") to produce to the government the electronic mail ("email") of the Plaintiff, Steven Warshak ("Warshak"). The so-called §2703(d) orders sought and secured by the government, which caused various ISP's to produce thousands of Warshak emails, violated (1) the Fourth Amendment to the United States Constitution, insofar as they ordered the search and/or seizure of private and closed email content communications on a showing of less than probable cause and without a warrant, and (2) the Stored Communications Act ("SCA"), codified at 18 U.S.C. §2701 et seq., itself, insofar as they ordered the search and/or seizure of the content of private email communications in electronic storage for less than 181 days on a showing of less than probable cause and without a warrant.

Accordingly, on June 12, 2006, Warshak filed a Complaint seeking declaratory judgment that the SCA is unconstitutional, on its face and as applied in this case, because it allows the government to seize and search a closed container—private email communications stored on an ISP server—without a search warrant and upon a showing of less than probable cause, in violation of the rights and guarantees afforded Warshak by the Fourth Amendment to the United States Constitution, as well as declaratory judgment that the Orders issued in this case violate the SCA because the Orders specifically exclude from the definition of "electronic storage" "any email communications received by the specified accounts that the owner or user of the account has already accessed, viewed, or downloaded", without regard for whether the email communications were more or less than 180 days old, and the Orders therefore compelled the production of emails in "electronic storage" (as properly and lawfully defined and interpreted) less than 180 days without a warrant and upon a showing of less than probable cause. In his Complaint, Warshak also sought a preliminary and permanent injunction preventing the government from further implementation and/or use of the SCA to access any email communications of Steven Warshak unless pursuant to search warrant lawfully issued upon a showing of probable cause, pursuant to the first sentence of 18 U.S.C. §2703(a), or pursuant to 18 U.S.C. §2510 et seq., to the extent that the object of the Order is within the ambit of Title III protections.

Since filing his Complaint, in response to inquires by Warshak, the government has advised that it would not assure Warshak that it would not seek further orders similar to those that are the subject matter of Warshak's Complaint pending resolution of the Complaint or resolution of Warshak's request for a preliminary injunction. As such,

Warshak has now moved for a Temporary Restraining Order and/or Preliminary Injunction, and a hearing at the Court's first opportunity, and he submits the instant memorandum in support thereof.

II. *The Temporary Restraining Order and Preliminary Injunction should issue because the Plaintiff can prove each of the elements required*

"The Sixth Circuit has held that the standards for issuing a temporary restraining order or a preliminary injunction are: (1) the likelihood of success on the merits; (2) the irreparable harm that could result if the injunction is not issued; (3) the impact on the public interest; and (4) the possibility of substantial harm to others." Avery Dennison Corp. v. Kitsonas, 118 F.Supp.2d 848, 851 (S.D.OH.2000), citing Basicomputer Corp. v. Scott, 973 F.2d 507, 511 (6th Cir.1992). It is well established, however, that a movant need not satisfy each element, rather the "elements are factors to be balanced against other." Id., citing In re DeLorean Motor Co., 755 F.2d 1223, 1229 (6th Cir.1985); Dayton Area Visually Impaired Persons, Inc. v. Fisher, 70 F.3d 1474, 1480 (6th Cir.1995). For the following reasons, Warshak respectfully contends that a proper weighing of these elements clearly warrants the issuance of the requested Temporary Restraining Order.

A. ***Likelihood of Success On the Merits***

1. Violation of Fourth Amendment

In this case, the Orders issued by the Court upon application by the government were based on a minimal showing of "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. §2703(d); see Exhibits 1 and 2 attached to Complaint. These Orders, which were premised upon a showing of less than probable cause, clearly do not

constitute a judicially issued search warrant pursuant to the Fourth Amendment and/or Rule 41 of the Federal Rules of Criminal Procedure.

Warrantless searches and seizures are presumptively unreasonable under the Fourth Amendment, Horton v. California, 496 U.S. 128, 110 S.Ct. 2301, 2306 & n. 4, 110 L.Ed.2d 112 (1990); Katz v. United States, 389 U.S. 347, 357, 88 S.Ct. 507, 514, 19 L.Ed.2d 576 (1967), as are any searches and seizures of closed containers based on less than probable cause, United States v. Ross, 456 U.S. 798, 809-812, 102 S.Ct. 2157, 2164-2166, 72 L.Ed.2d 572 (1982). As early as 1878, the Supreme Court has acknowledged that the contents of "[l]etters and sealed packages ... in the mail are as fully guarded from examination and inspection ... as if they were retained by the parties forwarding them in their own domiciles." Ex Parte Jackson, 96 U.S. 727, 733, 24 L.Ed. 877 (1878). So long as a package is "closed against inspection," the Fourth Amendment protects its contents, "wherever they may be," and the police must obtain a warrant to search it just "as is required when papers are subjected to search in one's own household." Id. Accord, United States v. Van Leeuwen, 397 U.S. 249, 90 S.Ct. 1029, 25 L.Ed.2d 282 (1970). Indeed, the Supreme Court has long recognized that individuals do not surrender their expectations of privacy in closed containers when they send them by mail or common carrier, and that "[l]etters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy; warrantless searches of such effects are presumptively unreasonable." United States v. Jacobsen, 466 U.S. 109, 114, 104 S.Ct. 1652, 1656-57, 80 L.Ed.2d 85 (1984), citing United States v. Chadwick, 433 U.S. 1, 10, 97 S.Ct. 2476, 2482, 53 L.Ed.2d 538 (1977); United States v. Van Leeuwen, 397 U.S. 249, 251, 90 S.Ct. 1029, 1031, 25 L.Ed.2d 282 (1970); Ex parte

Jackson, 96 U.S. 727, 733, 24 L.Ed. 877 (1878); United States v. Ross, 456 U.S. 798, 809-812, 102 S.Ct. 2157, 2164-2166, 72 L.Ed.2d 572 (1982); Robbins v. California, 453 U.S. 420, 426, 101 S.Ct. 2841, 2845, 69 L.Ed.2d 744 (1981) (plurality opinion); Arkansas v. Sanders, 442 U.S. 753, 762, 99 S.Ct. 2586, 2592, 61 L.Ed.2d 235 (1979), and other cases.

"As long as a package is 'closed against inspection,' the Fourth Amendment protects its contents 'wherever they may be' and the police must obtain a search warrant." United States v. Dowler, 940 F.2d 1539, 1991 WL 155987, at *3 (10th Cir.1991) (unpublished opinion), citing Ex parte Jackson, 96 U.S. at 733. The bottom line is that "unless the container is such that its contents may be said to be in plain view, those contents are fully protected by the Fourth Amendment." Robbins, 453 U.S. at 427.

Emails stored on an ISP's server are simply another form of a closed container. The contents of an email are not visible to the naked eye; rather, there are several intrusive searches that axiomatically precede one's ability to view the contents of an email stored on an ISP's server. First, an individual seeking to view the contents of an email stored on an ISP's server must gain access to that portion of the ISP's server that houses the subscriber's email; this is a search in and of itself. Even after one gains access to a subscriber's virtual mailbox, the contents of those emails remain shielded from public view, much like the contents of a first-class letter remain shielded from public view when you peer into a mailbox at the top of one's driveway. To view the contents of the email, an individual must take another intrusive physical act, he or she must unseal the email. To do so, one double-clicks on the email through the use of a computer mouse or perhaps uses the "open" function of the computer. Either way, the closed nature of the

email conceals its contents from plain view until somebody opens or unseals the email. This is no different from the physical act of unsealing a closed first-class envelope, unsealing a closed package, unlocking a closed footlocker, opening a closed filing cabinet, or opening a closed storage facility. From a doctrinal perspective, this incontrovertible fact compels a finding that an email is a closed package and, as such, there is no constitutional difference between unsealing a first-class letter and double-clicking an email, and both closed containers are entitled to the same constitutional protection.

In creating a relationship with an ISP, the subscriber does not relinquish a reasonable expectation of privacy in any unopened or opened-and-then-closed-again email communications stored on the ISP's server. Keeping a closed email on the server of an ISP does not relinquish one's interest in the email, or his reasonable expectation of privacy therein. Indeed, in the case of email, the subscriber perhaps maintains more control over the email letter than in any other traditional third party carrier context. In the latter scenarios, the sender or receiver of a closed letter or package actually relinquishes control of the container and cannot immediately repossess the letter or package—it is in the physical possession of the postal carrier and/or common carrier outside the dominion and control of the sender or recipient. In the email context, the owner of the email can repossess a read-and-then-closed email at any moment, without any notice or permission from the ISP, can retake the email, delete the email from his mailbox, or do whatever he or she wants to do with the email. It is, for all purposes, in that person's possession, dominion and control, at all times. The privacy interests should therefore be greater in the context of email than in the traditional carrier paradigm.

Additionally, the subscriber's relationship to the ISP adds to the reasonable expectation of privacy in the contents of closed emails contained on the ISP's server. Like an individual who rents a storage space at a local storage facility, an ISP subscriber typically secures a section of the ISP's storage facility, i.e., its server. See Nuvox website, www.nuvox.com (advising that a subscriber obtains access to 20M of storage on its server). Indeed, the Attachment to the Orders issued in this case specifically order the production of "contents of wire or electronic communications ... **that were placed or stored in directories or files owned or controlled by the accounts identified in Part A**...." See Exhibits 1 and 2 attached to Complaint (emphasis added). The very language of the Orders acknowledges that the subscriber has an ownership or controlling interest in the directories or files in which the closed emails were stored. Moreover, the subscriber's "storage space" within the ISP server is locked and inaccessible to the public at large, like the individual who places a lock on his storage space. While a physical storage space or a physical filing cabinet is protected by combination or key locks, the rented portion of the ISP's server is protected by a screen name and a password, precluding access to its contents by any member of the public. Additionally, like the owner of a physical storage facility, or a bailee who takes possession of another person's private documents, the ISP is not permitted to access the private mail contained on the server except for very limited circumstances—they are not permitted or expected to simply open and review private email at their whim and discretion.

It is well established that an individual manifests a subjective expectation of privacy that society views as objective reasonable when he or she places contents into a closed container, even when he or she places that closed container in the possession of a

private third party, such as within a friend's apartment, a leased house, a rented storage facility, or a third party common carrier. See, e.g., United States v. James, 353 F.3d 606, 614 (8th Cir.2003) (in deciding an issue of consent, court notes that Eighth Circuit law and law of other circuits indicates that one does not cede dominion over an item to another just by putting him in possession; for example a lessee does not have authority to consent to a search of the lessor's financial records stored at the leased house merely on account of the lessor-lessee relationship); United States v. Dowler, 940 F.2d 1539 (10th Cir.1991) (unpublished decision) (before leaving state, appellant placed documents in boxes, file cabinet and briefcases, which were then stored by apartment manager at request of appellant's agent; held that appellant manifested an expectation that the documents would remain private and free from inspection, the apartment manager was obligated to care for her property in the regular storage area and a new relationship was created, and that appellant's expectation of privacy and protection from a wrongful search and seizure continued into the creation of the bailment by the apartment manager and her agent); United States v. Fultz, 146 F.3d 1102 (9th Cir.1998) (defendant who lived "on and off" with his friend and stored many of his belongings in closed boxes in friend's garage had a reasonable expectation of privacy in his belongings, even though those belongings were kept in a place that was not exclusively controlled by him).

Finally, for all of these reasons, email communications retained on an ISP server are not analogous to the line of cases wherein individuals knowingly expose communications to a third party, which are then conveyed to law enforcement authorities pursuant to subpoenas. In United States v. Miller, 425 U.S. 435, 443, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976), the Court held that a customer of a bank cannot challenge on Fourth

Amendment grounds the admission into evidence in a criminal prosecution of financial records obtained by the government from his bank pursuant to allegedly defective subpoenas, despite the fact that he was given no notice of the subpoenas. Miller, 425 U.S. at 441-443. See also Donaldson v. United States, 400 U.S. 517, 522, 91 S.Ct. 534, 538, 27 L.Ed.2d 580 (1971) (Internal Revenue summons directed to third party does not trench upon any interests protected by the Fourth Amendment). In Miller, the Court ruled that no Fourth Amendment interests of the depositor were implicated because the depositor knowingly exposed those documents to the bank's employees in the ordinary course of business, and that "checks are not confidential communications but negotiable instruments to be used in commercial transactions." Miller, 425 U.S. at 442. As such, the Court ruled that the case was governed by the general rule 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. Miller, 425 U.S. at 443.

In the context of emails stored on an ISP server—whether they have been previously opened by the addressee or not—the emails remain closed to the public and to the ISP (except, perhaps, for limited, defined circumstances that are either inapplicable to the facts of this matter and/or that do not diminish the customer's reasonable expectation of privacy regarding the content of their email communications). Most importantly, they have not been provided to the ISP for their exposure, review or consumption. Unlike the checks at issue in Miller, which the Supreme Court noted are conveyed to bank and exposed to their employees in the ordinary course of business, email communications are closed containers and, even if an ISP contract provides limited circumstances in which they may be viewed by the ISP (and even if the subscriber ever reads that contract),

subscribers have an objectively reasonable expectation that those emails will remain absolutely private and concealed subject to those very limited circumstances. In other words, it is not as if the subscriber understands that all employees of an ISP will be privy to his emails but expects the ISP will not share the contents with other parties; rather, it is the subscriber's expectation that the ISP will not review the contents of his emails, except, perhaps, in very limited circumstances. Moreover, while the Supreme Court specifically noted that the documents at issue in Miller were "not confidential communications," Miller, 425 U.S. at 442, emails obviously are confidential communications. In short, an email subscriber does not knowingly expose the contents of his or her emails to any third party and the ISP does not have the right or discretion to review a subscriber's email in the ordinary course of its business.

For all of these reasons, as well as those articulated in Warshak's memorandum filed in support of his Complaint and request for preliminary and permanent injunctions, which he respectfully incorporates herein, Warshak contends that there is a very strong and substantial likelihood of success on the merits.

2. *Orders as drafted violated the Stored Communications Act*

The Attachments to the Orders, attached as part of Exhibits 1 and 2 to Warshak's Complaint, order Yahoo and NuVox to provide the following materials, amongst others:

> The contents of wire or electronic communications (not in electronic storage unless greater than 181 days old) that were placed or stored in directories or files owned or controlled by the accounts identified in Part A at any time during the hosting of the electronic communications and through the date of this Order … Included in [the definition of "electronic storage"] are unopened incoming communications less than 181 days old. **Communications not in "electronic storage" include any email communications received by the specified accounts that the owner or user of the account has already accessed, viewed, or downloaded**.

See Exhibits 1 and 2 attached to Complaint (emphasis added).

Section 2703 of Title 18 of the United States Code sets forth certain conditions pursuant to which a governmental entity may require the disclosure by a provider of electronic communication service or remote computing service of the contents of a wire or electronic communication. Pursuant to the first sentence of §2703(a), 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 an 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 offenses under investigation or equivalent State warrant. 18 U.S.C. 2703(a). Pursuant to the second sentence of §2703(a), a governmental entity may require disclosure of content that has been in electronic storage for more than one hundred and eighty days without a warrant; but, instead, by the means available under subsection (b) of the statute, which includes the use of administrative subpoenas or court orders under §2703(d). 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". 18 U.S.C. §2510(17).

In essence, by excluding from the definition of "electronic storage" "any email communications received by the specified accounts that the owner or user of the account has already accessed, viewed, or downloaded", regardless of whether those email communications are more than or less than 180 days old, the Orders sought and secured

by the government eviscerates the spirit and language of §2703(a), which requires a search warrant for any emails in electronic storage for 180 days or less. While the definitional language included within the Attachments to the Orders reflects the Department of Justice's interpretation of the SCA as contained in their internal manual, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," it is an interpretation that was squarely rejected by the Ninth Circuit in the fairly recent opinion styled Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir.2004), and, frankly, is an interpretation that firmly undercuts Congress' intent in enacting the SCA.

Theofel concerned a commercial litigation dispute amongst private parties, during which Farey-Jones sought access to his adversary's email by serving NetGate with a subpoena pursuant to the Federal Rules of Civil Procedure. Theofel, 359 F.3d at 1071. In response to the subpoena, which sought all emails sent or received by anyone, with no limitation as to time or scope, NetGate provided Farey-Jones with a "free sample" of 339 email messages. Theofel, 359 F.3d at 1071. The plaintiffs eventually filed a separate action against Farey-Jones, claiming that the defendants subpoena violated the Stored Communications Act, as well as various other laws. Theofel, 359 F.3d at 1072.

After rejecting the defendant's argument that NetGate had "consented" or authorized the defendants' access to the emails, the defendants argued that emails that remain on an ISP's server after delivery no longer fall within the definition of "electronic storage" contained in 18 U.S.C. §2510(17). Theofel, 359 F.3d at 1075. The United States, as amicus curiae, joined the defendant's argument, asserting the legal rationale that underlies the language in the Attachments to the Orders entered in this case: emails that

are downloaded, accessed and/or viewed are no longer in "electronic storage." Theofel, 359 F.3d at 1075-77.

The Ninth Circuit concluded that "[t]here is no dispute that messages remaining on [an ISP's] server after delivery are stored 'by an electronic communication service' within the meaning of 18 U.S.C. §2510(17)(B)." Theofel, 359 F.3d at 1075. "The only issue, then," according to the Ninth Circuit, "is whether the messages are stored 'for purposes of backup protection.'" Theofel, 359 F.3d at 1075, quoting 18 U.S.C. §2510(17)(B). Concluding that an "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. "The ISP copy of the message functions as a 'backup' for the user." Theofel, 359 F.3d at 1075. The Ninth Circuit rejected the contention that "backup protection" includes only temporary backup storage pending delivery, and not any form of "post-transmission storage", see Fraser v. Nationwide Mut. Ins. Co., 135 F.Supp.2d 623, 635-36 (E.D.Pa2001), holding such a view "as contrary to the plain language of the Act." Theofel, 359 F.3d at 1075. The Ninth Circuit did "not lightly conclude that the government's reading is erroneous," but it held that "prior access is irrelevant to whether the messages at issue were in electronic storage" and, ultimately, that the plaintiffs' emails were in electronic storage regardless of whether they had been previously delivered. Theofel, 359 F.3d at 1077. Hence, according to the Ninth Circuit, email communications accessed by the user but stored on an ISP server for 180 days or less for backup purposes cannot be seized by the government without a warrant, pursuant to 18 U.S.C. §2703(a).

Of course, the Ninth Circuit's decision in Theofel comports with the underlying purpose of the Electronic Communications Privacy Act of 1986 ("ECPA"), which included a broad definition of electronic storage to enlarge privacy protections for stored data. See Councilman, 418 F.3d at 76 (finding that "the purpose of the broad definition of electronic storage was to enlarge privacy protections for stored data under the Wiretap Act, not to exclude e-mail messages stored during transmission from those strong protections."). Congress added the Stored Communications Act to the ECPA (Title II) to halt potential intrusions on individual privacy, not with an intent to limit or curtail individual privacy. Councilman, 418 F.3d at 80-81. "While drafting the ECPA's amendments to the Wiretap Act, Congress [] recognized that, with the rise of remote computing operations and large databanks of stored electronic communications, threats to individual privacy extended will beyond the bounds of the Wiretap Act's prohibition against the 'interception' of communications", and so Congress added Title II to the ECPA. Councilman, 418 F.3d at 80-81.

The government's interpretation of "electronic storage" essentially guts the warrant requirement of §2703(a). Under the government's view of the statute, the only emails protected by the 180 day warrant requirement of §2703(a) are those emails that reach a subscriber's mailbox, but the subscriber decides to leave the email on his mailbox, untouched and unread, for 180 days. Of course, in reality, this hardly, if ever, occurs. If the government's view is accepted, a subscriber would have Title III protection for an email up to the point it is moved from the ISP server to his or her mailbox, see Councilman, 418 F.3d 67, 76, 77 (1st Cir.2005), a subscriber would have §2703(a) warrant protection only until he or she opens or accesses his email, and from that point

on, whether or not 180 days expire, the subscriber will have no more protection of his content email than an individual has in his telephone numbers under the pen register provisions and/or account information, all of which is knowingly exposed to thousands of employees of various companies. C.f. Smith v. Maryland, 442 U.S. 735 (1979) (holding that the installation and use of a pen register does not constitute a Fourth Amendment search because a caller has no reasonable expectation of privacy in the numbers dialed from his or her phone). In short, the government's interpretation of "electronic storage" significantly curtails individual's privacy interests in their stored communications, which cuts directly against the intent of Congress in enacting the SCA.

Wherefore, for all of the reasons discussed in Theofel, the Orders issued in this case violated the SCA because the Attachments ordered the production of "any email communications received by the specified accounts that the owner or user of the account has already accessed, viewed, or downloaded", the Orders therefore explicitly advised that such emails were outside the definition of "electronic storage" regardless of whether they were more or less than 180 days old, and the Orders therefore called for the production of email communications that fall within the first sentence of §2703(a), which requires a search warrant in order to disclose email communications in electronic storage for 180 days or less. 18 U.S.C. §2703(a).

For all of these reasons, as well as those articulated in Warshak's memorandum filed in support of his Complaint and request for preliminary and permanent injunctions, which he respectfully incorporates herein, Warshak contends that there is a very strong and substantial likelihood of success on the merits on this prong of the Complaint as well.

B. *Irreparable harm will result if the injunction is not issued.*

With each passing day the government has the capability of seeking additional orders pursuant to 18 U.S.C. §2703(d) without first securing a search warrant or establishing probable cause, as required by the Fourth Amendment, and/or compelling companies to provide opened and then closed emails on their servers regardless of whether they were more or less than 180 days old without a warrant. The government has refused to voluntarily stay any further requests and would not provide Warshak with any assurance that they will not seek similar Orders in the future or, indeed, whether there are similar Orders outstanding at this very moment in time. Indeed, perhaps the government's incentive to utilize these unconstitutional and unlawful Orders is at its apex now that Warshak has filed the subject Complaint and the government is on notice that its ability to secure these orders absent probable cause and a search warrant may soon terminate. In any event, it seems beyond reasonable dispute that with each new order sought, granted and executed a new irreparable violation of the Warshak's rights will occur should the Court ultimately rule that the government's conduct constitutes a violation of the Fourth Amendment or the CSA itself. These violations, which inflict a flagrant intrusion to Warshak's privacy rights and expectations, cannot thereafter be effectively remedied. Even suppressing evidence that flows from the constitutional and/or statutory violations does not remedy the violation occasioned when the government, without any right to do so, reads our most private communications, in secret and without notice. Respectfully, a Temporary Restraining Order is necessary to prevent the government from causing further irreparable harm to Warshak pending resolution of his motion for a Preliminary Injunction and/or resolution of the Complaint.

C. *The impact on the public interest involved is great.*

For all of the reasons discussed *supra*, the unconstitutional and unlawful Orders issued in this case have a significant impact on the public interest. If the government has issued the orders in this case, which were issued pursuant to the guiding policy of the Department of Justice, then similar orders are surely being issued and executed throughout the United States of America. If the Court ultimately rules that the Orders are unconstitutional and/or violate the CSA as drafted, this ruling will have a dramatic, substantial impact on the public interest. Certainly, the public at large is not sensitive to the notion that their private electronic communications have been accorded such a diminished expectation of privacy by the government. There is an important public interest at stake, therefore, in the resolution of this case. Preserving the status quo while the Court resolves the grave issue of whether a statute violates the United States Constitution, and/or whether the government's conduct violates a statute, is a valid public interest, especially considering that it has been held that preservation of business competition and basic contracts principals are a valid public interest to be served by the issuance of a preliminary injunction. See Avery Dennison Corp. v. Kitsonas, 118 F.Supp.2d at 855.

D. *If the injunction is not issued the possibility of substantial harm to others is severe.*

For the reasons already stated, the issuance of a Temporary Restraining Order will prevent the severe and real possibility of substantial harm to two categories of people, other than Warshak. The first group includes those who had business dealings with the Plaintiff and his company. The second group includes other citizens of this country who

will continue to be subjected to the unconstitutional and unlawful orders imposed in this case.

The government's ability to unconstitutionally search emails on a showing of less than probable cause, and/or its ability to bypass the statutory requirements by drafting Attachments that contradict the terms and spirit of the statute, clearly imposes substantial harm to our entire citizenry. The mere potential of this ability could have a chilling effect on the use of email as a form of communication because people and businesses would regard it as unsecured, which would have a significant impact on the daily affairs of the country, both personally and business. As noted in his memorandum in support of the Complaint, email has quickly become the backbone of our country's communication system. Without communication, the marketplace cannot operate either effectively or efficiently.

More particularly, the people who communicated with Warshak may be harmed because their communications are not solely between themselves and Warshak. By the Government opening—without a constitutionally sufficient showing and in violation of the CSA—what they reasonably believed to be private their thoughts, feelings, opinions, and plans, these individuals have been harmed and will continue to be substantially harmed. The intent of the Fourth Amendment is to protect people, not simply places. It not only protects Warshak in this case, but also those with whom he has communicated and will communicate in the future. Moreover, the issuance of a Temporary Restraining Order will prevent he government from further unconstitutional and/or unlawful use of the orders and will therefore protect others that the Government may have hoped to use such orders against in the future.

E. ***The balancing of the four elements shows that the Temporary Restraining Order should be granted.***

As argued, a proper balancing of these factors clearly warrants the issuance of a Temporary Restraining Order. The government will not provide any assurances that it will cease employing these unconstitutional and unlawful orders in this case, reasonable grounds therefore exist to believe the government will utilize these orders in this case and others, a substantial likelihood exists that the government's conduct violates the Fourth Amendment, irreparable harm has been occasioned and continues to be inflicted, it is a matter that significantly impacts the public interest, and there exists a significant possibility of severe harm to others in the absence of a Temporary Restraining Order. Wherefore, Warshak respectfully contends that a balancing of the four factors clearly warrants the issuance of a Temporary Restraining Order.

III. *Conclusion*

WHEREFORE, for all of the foregoing reasons, the Plaintiff respectfully requests that the Court issue the requested Temporary Restraining Order and/or Preliminary Injunction.

Respectfully Submitted,
Steven Warshak,
By His Counsel,

/s/ Martin G. Weinberg
Martin G. Weinberg (Mass. Bar No.#519480)
Admitted Pro Hac Vice
MARTIN G. WEINBERG, P.C.
20 Park Plaza, Suite 905
Boston, MA 02116
Telephone: (617) 227-3700
Facsimile: (617) 338-9538

/s/ Martin S. Pinales
Martin S. Pinales (Ohio Bar No. 0024570)
Candace C. Crouse (Ohio Bar No. 0072405)
Sirkin, Pinales & Schwartz LLP
105 West Fourth Street, Suite 920
Cincinnati, Ohio 45202
Telephone: (513) 721-4876
Facsimile: (513) 721-0876

Dated: June 30, 2006

CERTIFICATE OF SERVICE

I hereby certify that a true copy of the foregoing document was served on the 29th day of June 2006 by electronic filing upon all parties in the above-captioned case, as well as by electronic mail on this date.

/s/ Martin G. Weinberg
Martin G. Weinberg