

CASE N^o-06-4092

IN THE
UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

STEVEN WARSHAK,

Plaintiff – Appellee

v.

UNITED STATES OF AMERICA,

Defendant – Appellant

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE
SOUTHERN DISTRICT OF OHIO
AT CINCINNATI

PROOF BRIEF FOR DEFENDANT-APPELLANT
UNITED STATES OF AMERICA

For Defendant-Appellant:

GREGORY G. LOCKHART
UNITED STATES ATTORNEY

DONETTA D. WIETHE
BENJAMIN C. GLASSMAN
Assistant U.S. Attorneys
221 E. 4th St., Ste 400
Cincinnati, OH 45202

JOHN H. ZACHARIA
NATHAN P. JUDISH
U.S. Department of Justice
1301 New York Ave., N.W., Ste 600
Washington, D.C. 20005

TABLE OF CONTENTS

TABLE OF AUTHORITIES.....	iii
STATEMENT REQUESTING ORAL ARGUMENT.....	vii
STATEMENT OF SUBJECT MATTER AND APPELLATE JURISDICTION.....	1
STATEMENT OF ISSUES FOR REVIEW	2
STATEMENT OF THE CASE	3
STATEMENT OF FACTS	5
I. STATUTORY BACKGROUND	5
II. THE PRESENT CONTROVERSY	8
SUMMARY OF THE ARGUMENT	14
ARGUMENT	18
I. THE DISTRICT COURT LACKED SUBJECT MATTER JURISDICTION TO ISSUE THE PRELIMINARY INJUNCTION....	18
A. Appellee Lacks Standing.....	18
B. Appellee’s Claims Are Not Ripe.....	26
II. THE DISTRICT COURT ABUSED ITS DISCRETION IN ISSUING THE PRELIMINARY INJUNCTION	29
A. Standard of Review.....	29

B. The District Court Used an Erroneous Legal Standard in Issuing the Injunction by Holding the SCA Facially Unconstitutional..... 30

C. The District Court Used an Erroneous Legal Standard in Issuing the Injunction by Applying a Probable Cause Standard to the Compelled Disclosure of E-mail, Rather than a Reasonableness Standard 36

1. The Fourth Amendment Sets a Reasonableness Standard for Compelled Disclosure..... 38

2. The Fourth Amendment’s Reasonableness Standard Governs Compelled Disclosure from a Third Party..... 43

3. The Statutory Framework of the SCA and Industry Practice Support the Reasonableness of 2703(d) Orders. 46

4. The Fourth Amendment Does Not Require Notice to the Target of an Investigation of Third-Party Compelled Disclosure..... 50

D. The District Court Improperly Applied the Law in Balancing the Remaining Preliminary Injunction Factors..... 51

1. Warshak Would Not Suffer Irreparable Harm Absent The Preliminary Injunction. 51

2. The Preliminary Injunction Is Causing Substantial Harm to Others and Is Not Serving the Public Interest. 54

CONCLUSION..... 57

DESIGNATION OF JOINT APPENDIX CONTENTS..... 58

CERTIFICATE OF COMPLIANCE..... 59

CERTIFICATE OF SERVICE..... 60

TABLE OF AUTHORITIES

Cases

<i>Abney v. Amgen, Inc.</i> , 443 F.3d 540 (6th Cir. 2006).....	52
<i>Adult Video Ass'n v. U.S. Dept. of Justice</i> , 71 F.3d 563 (6 th Cir. 1995).....	26, 27, 28, 29
<i>Bohach v. City of Reno</i> , 932 F. Supp. 1232 (D. Nev. 1996).....	49
<i>Bonnell v. Lorenzo</i> , 241 F.3d 800 (6th Cir. 2000)	29
<i>Branzburg v. Hayes</i> , 408 U.S. 665 (1972)	41, 43
<i>California v. Ciraolo</i> , 476 U.S. 207 (1986)	32
<i>City of Los Angeles v. Lyons</i> , 461 U.S. 95 (1983)	passim
<i>Coleman v. DeWitt</i> , 282 F.3d 908 (6th Cir. 2002)	30
<i>Crowley v. Cybersource</i> , 166 F. Supp. 2d 1263 (N.D. Cal. 2001)	49
<i>Detroit Newspaper Publ's Ass'n v. Detroit Typographical Union No. 18</i> , 471 F.2d 872 (6th Cir. 1972)	30
<i>Doe v. Brodderick</i> , 225 F.3d 440 (4th Cir. 2000)	47
<i>Donovan v. Lone Steer, Inc.</i> , 464 U.S. 408 (1984)	39
<i>Florida v. Riley</i> , 488 U.S. 445 (1989).....	47
<i>Fraser v. Nationwide Mut. Ins. Co.</i> , 135 F. Supp. 2d 623 (E.D. Pa. 2001), <i>aff'd in part on other grounds</i> , 352 F.3d 107 (3d Cir. 2004)	6, 48, 49

<i>Friends of the Earth, Inc. v. Laidlaw Environ. Servs., Inc.</i> , 528 U.S. 167 (2000).....	23, 24
<i>FW/PBS, Inc. v. Dallas</i> , 493 U.S. 215 (1990).....	30
<i>Guest v. Leis</i> , 255 F.3d 325 (6th Cir. 2001).....	32
<i>Hana v. Gonzales</i> , 157 Fed. Appx. 880 (6th Cir. 2005)	37
<i>Hoffa v. United States</i> , 385 U.S. 293 (1966).....	35
<i>In re Administrative Subpoena John Doe, D.P.M.</i> , 253 F.3d 256 (6th Cir. 2001)	36, 40, 41
<i>In re Grand Jury Subpoena Issued Pursuant to 18 U.S.C. Section 2703(b)(1)(B)</i> , (M.D. Ga. Apr. 29, 2005).....	6
<i>In re Subpoena Duces Tecum</i> , 228 F.3d 341 (4th Cir. 2000).....	39
<i>Jerry T. O'Brien, Inc. v. SEC</i> , 704 F.2d 1065 (9th Cir. 1983).....	50
<i>Lujan v. Defenders of Wildlife</i> , 504 U.S. 555 (1992).....	passim
<i>Lyng v. Northwest Indian Cemetery Protective Ass'n</i> , 485 U.S. 439 (1988)	11
<i>Newfield v. Ryan</i> , 91 F.2d 700 (5th Cir. 1937).....	44
<i>Oklahoma Press Publishing Co. v. Walling</i> , 327 U.S. 186 (1946).....	39
<i>Overstreet v. Lexington-Fayette Urban County Gov't</i> , 305 F.3d 566 (6th Cir. 2002)	55
<i>Renne v. Geary</i> , 501 U.S. 312 (1991)	23, 24
<i>Rostker v. Goldberg</i> , 453 U.S. 57 (1981).....	47, 55

<i>Schwimmer v. United States</i> , 232 F.2d 855 (8th Cir. 1956).....	44
<i>SEC v. Jerry T. O'Brien, Inc.</i> , 467 U.S. 735 (1984)	36, 50, 51
<i>Smith v. Maryland</i> , 442 U.S. 735 (1979)	30
<i>Steel Co. v. Citizens for a Better Environment</i> , 523 U.S. 83 (1998).....	passim
<i>Texas v. United States</i> , 523 U.S. 296 (1998).....	28
<i>Theofel v. Farey-Jones</i> , 359 F.3d 1066 (9th Cir.), <i>cert denied</i> , 543 U.S. 813 (2004).....	6
<i>United States v. Allen</i> , 106 F.3d 695 (6th Cir. 1997).....	33
<i>United States v. Caymen</i> , 404 F.3d 1196 (9th Cir. 2005)	33
<i>United States v. Dionisio</i> , 410 U.S. 1 (1973).....	39
<i>United States v. Doe</i> , 457 F.2d 895 (2d Cir. 1972).....	39
<i>United States v. Gravel</i> , 408 U.S. 606 (1972).....	41
<i>United States v. Miller</i> , 425 U.S. 435 (1976).....	35, 45, 47
<i>United States v. Morton Salt Co.</i> , 338 U.S. 632 (1950).....	41
<i>United States v. Palmer</i> , 536 F.2d 1278 (9th Cir. 1976).....	45
<i>United States v. Phibbs</i> , 999 F.2d 1053 (6th Cir. 1993)	43, 44, 46
<i>United States v. R Enterprises, Inc.</i> , 498 U.S. 292 (1991).....	17, 42
<i>United States v. Salerno</i> , 481 U.S. 739 (1987)	31
<i>United States v. Zavakos</i> , No. 3:06-cr-03, 2006 WL 1697645 (S.D. Ohio June 19, 2006)	49

<i>University of Pennsylvania v. EEOC</i> , 493 U.S. 182 (1990)	43
<i>Warth v. Seldin</i> , 422 U.S. 490 (1975)	18
<i>Whitmore v. Arkansas</i> , 495 U.S. 149 (1990).....	20, 22
<i>Wilson v. United States</i> , 221 U.S. 361 (1911).....	38

Statutes

18 U.S.C. § 2510	6, 46
18 U.S.C. § 2701	5, 47, 48, 49
18 U.S.C. § 2702	5, 48
18 U.S.C. § 2703(a).....	6, 7, 46
18 U.S.C. § 2703(b).....	passim
18 U.S.C. § 2705	12, 51, 53
18 U.S.C. § 2705(a).....	7
18 U.S.C. § 2712	20, 53
28 U.S.C. § 1292	1
28 U.S.C. § 1331	1

Other Authorities

8 J. Wigmore, <i>Evidence</i> § 2192 (McNaughton rev. 1961)	41, 42
H.R. Rep. No. 103-827(I) (1996), <i>reprinted in</i> 1996 U.S.C.C.A.N. 3489	7

STATEMENT REQUESTING ORAL ARGUMENT

Oral argument may aid the decisional process because of the novelty of the issue presented; specifically, until this case, no court had ever declared unconstitutional the provisions of the Stored Communications Act. The United States therefore requests oral argument.

**STATEMENT OF SUBJECT MATTER AND APPELLATE
JURISDICTION**

Appellee Warshak brought this case before the United States District Court for the Southern District of Ohio on the premise that the district court was vested with jurisdiction by 28 U.S.C. § 1331. As set forth more fully in Argument Section I of this brief, Appellant United States disputes the district court's subject matter jurisdiction over the case. As this is an appeal from a preliminary injunction issued on July 21, 2006, this Court has appellate jurisdiction pursuant to 28 U.S.C. § 1292(a)(1). Appellant filed its Notice of Appeal on August 10, 2006.

STATEMENT OF ISSUES FOR REVIEW

1. Whether the district court lacked subject matter jurisdiction to issue the preliminary injunction.
2. Whether the district court used an erroneous legal standard in issuing the injunction by holding the Stored Communications Act, 18 U.S.C. §§ 2701-2712 (“SCA”), facially unconstitutional.
3. Whether the district court used an erroneous legal standard in issuing the injunction by applying a probable cause standard to the compelled disclosure of e-mail, rather than a reasonableness standard.
4. Whether the district court improperly applied the law in balancing the remaining preliminary injunction factors.

STATEMENT OF THE CASE

Congress set forth the procedures for compelled disclosure of stored communications in § 2703 of the SCA. In particular, § 2703(d) authorizes compelled disclosure of the contents of certain e-mail stored by providers of electronic communication service based on a court finding that “there are reasonable grounds to believe that the contents of a wire or electronic communication . . . are relevant and material to an ongoing criminal investigation.” On July 21, 2006, the district court held the SCA unconstitutional to the extent it authorizes compelled disclosure of e-mail without notice to the account holder on less than a showing of probable cause. Until this case, no court had ever declared § 2703 to be unconstitutional.

At the time he filed this suit, Appellee Steven Warshak (“Warshak”), the owner of Berkeley Premium Nutraceuticals, Inc. (“Berkeley”), was the target of an investigation into mail fraud, wire fraud, money laundering, and other federal crimes arising out of the marketing and sale of products by Berkeley. In the course of its investigation, the government sought and obtained two court orders pursuant to 18 U.S.C. § 2703(d) compelling NuVox Communications and Yahoo! to disclose the content of certain e-mails in accounts registered to Warshak. When Warshak learned of these 2703(d) orders, he filed suit against the government for declaratory and injunctive relief, alleging that compelled disclosure of his e-mail

without a judicial finding of probable cause violated the Fourth Amendment and the SCA. He then moved for a temporary restraining order or preliminary injunction barring the government from obtaining 2703(d) orders to compel disclosure of his e-mail.

On July 21, 2006, Judge Dlott of the United States District Court for the Southern District of Ohio issued a preliminary injunction enjoining the United States from using 2703(d) orders to compel disclosure of “the contents of any personal email account maintained by an Internet Service Provider in the name of any resident of the Southern District of Ohio without providing the relevant account holder or subscriber prior notice and an opportunity to be heard.” The government now appeals that decision.

On September 20, 2006, a federal grand jury indicted Warshak on 107 criminal counts of bank fraud, mail fraud, money laundering, and other federal crimes.

STATEMENT OF FACTS

I. STATUTORY BACKGROUND

Congress enacted the SCA in 1986 to create a system of statutory privacy rights for customers and subscribers of computer network service providers. It has three main substantive components, which protect and regulate the privacy interests of network users with respect to the government, network service providers, and the general public. First, § 2703 regulates government access to stored communications. It creates criminal procedures that federal and state law enforcement officers must follow in order to compel disclosure of stored communications. Second, § 2702 regulates voluntary disclosure by network service providers of customer communications and records, both to government and non-governmental entities. Third, § 2701 prohibits unlawful access to certain stored communications. Anyone who obtains, alters, or prevents authorized access to those communications is subject to criminal penalties. Until this case, no court has ever declared unconstitutional any of these provisions.

The structure of § 2703 reflects congressional judgments about what kinds of information implicate greater or lesser privacy interests. In general, the SCA offers greater protection to categories of information perceived by Congress to implicate greater privacy interests. In setting forth this series of classifications, the SCA relies on a few key terms which are explicitly defined by statute. One such

term is “electronic storage,” which is defined by 18 U.S.C. § 2510(17) 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.” Undelivered e-mail stored on a service provider’s servers falls within the scope of “electronic storage,” but delivered e-mail, draft e-mail, and copies of sent e-mail do not. *See Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001), *aff’d in part on other grounds*, 352 F.3d 107, 114 (3d Cir. 2004); *In re Grand Jury Subpoena Issued Pursuant to 18 U.S.C. Section 2703(b)(1)(B)*, (M.D. Ga. Apr. 29, 2005) (attached as exhibit 1 to R. 16, Response in Opposition re Motion for TRO; JA ___). *But see Theofel v. Farey-Jones*, 359 F.3d 1066, 1077 (9th Cir.), *cert denied*, 543 U.S. 813 (2004) (holding that previously accessed e-mail remained in “electronic storage”).

Under § 2703(a) of the SCA, the government may compel production of electronic communications in “electronic storage” for fewer than 181 days only pursuant to a warrant based on probable cause. In contrast, § 2703(b) of the SCA allows the government to compel production of other stored communications that do not fall within the statutory definition of “electronic storage,” such as delivered e-mail, using a subpoena or a 2703(d) order issued pursuant to 18 U.S.C. § 2703(d). In addition, the government may compel disclosure of e-mail in

“electronic storage” for more than 180 days pursuant to a subpoena or a 2703(d) order. *See* 18 U.S.C. § 2703(a), (b).

Section 2703(d) orders are issued by courts on a finding that the government has offered “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). This standard is “higher than a subpoena, but not a probable cause warrant.” H.R. Rep. No. 103-827(I), at 31 (1996), *reprinted in* 1996 U.S.C.C.A.N. 3489, 3511. The entity receiving the 2703(d) order may move to quash the order if the records sought are “unusually voluminous . . . or compliance with such order otherwise would cause an undue burden.” 18 U.S.C. § 2703(d).

When the government uses a 2703(d) order or a subpoena to compel disclosure of the content of communications, it must provide the subscriber with prior notice unless there is reason to believe that such notification may have an adverse result, such as seriously jeopardizing an investigation. *See* 18 U.S.C. § 2705(a). In all such cases, the SCA requires that the subscriber must eventually receive notice of the 2703(d) order.

II. THE PRESENT CONTROVERSY

On September 20, 2006, a federal grand jury indicted Warshak on 107 counts (including mail fraud, bank fraud, money laundering, and other federal offenses) in connection with the nationwide marketing and sale of products by Berkeley.¹ In May 2005, in the course of its investigation, the government sought and obtained a court order pursuant to 18 U.S.C. § 2703(d) (hereinafter, a “2703(d) order”) compelling NuVox Communications (“NuVox”) to disclose the content of certain e-mail in accounts registered to Warshak. (R.1, Complaint Exhibit 1 at 2-3; JA ___). In particular, the order sought disclosure of both the content of all stored e-mail communications more than 180 days old and the content of all stored e-mail communications that Warshak had already “accessed, viewed, or downloaded.” (*Id.* at 3; JA ___). The issuing court found that the government had “offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation.” (*Id.* at 2; JA ___). In September 2005, the government sought and obtained a similar 2703(d) order compelling disclosure of the same categories of content for Warshak’s Yahoo! e-mail account. (*Id.* at 5-6; JA ___).

The issuing court found that prior notice of these 2703(d) orders “would seriously jeopardize the investigation.” (*Id.* at 2, 5; JA ___). It ordered that the

¹ See *United States v. Warshak et al.*, No. 1:06-cr-00111-SAS-1, Doc #1 (Indictment in S.D. Ohio, Sept. 20, 2006).

orders be “sealed until otherwise ordered by the Court,” that NuVox and Yahoo! not disclose the existence of the order or the investigation, and that “notification otherwise required under 18 U.S.C. § 2703(b)(1)(B) be delayed for ninety days.” (*Id.*)

The government informed Warshak of the 2703(d) orders by letter on May 31, 2006. (*Id.* at 1, 4; JA ___). When Warshak learned of these 2703(d) orders, he filed a civil suit in the United States District Court for the Southern District of Ohio raising two claims, one constitutional and one statutory. (R.1, Complaint; JA ___). On constitutional grounds, he claimed that the SCA was unconstitutional under the Fourth Amendment facially and as applied because it enabled the government to obtain his e-mail without a warrant based on probable cause. On statutory grounds, he argued that 18 U.S.C. § 2703 forbids compelled disclosure of e-mail less than 181 days old without a warrant. Warshak’s civil suit seeks only declaratory and injunctive relief, not damages. (*Id.* at 14-15; JA ___).

After filing his civil suit, Warshak asked the government whether it would refrain from seeking further 2703(d) orders compelling disclosure of his e-mail. (R.11, Memorandum in Support of Motion for TRO at 2; JA ___). The government, which in general does not promise to abstain from using its lawful investigative powers in the course of an investigation, refused to provide any such assurances. (*Id.*) On June 30, 2006, Warshak filed a motion for a temporary

restraining order and/or preliminary injunction seeking to enjoin the use of 2703(d) orders to obtain the content of e-mail. (*Id.* at 1; JA ____). He argued that compelled disclosure of his e-mail amounted to a warrantless search and seizure and that the only way to compel disclosure of his e-mail consistent with the Fourth Amendment was through a warrant based on probable cause.

The government opposed Warshak's motion because Warshak was not likely to prevail on the merits, would not be irreparably harmed, and because the balance of harms weighed decisively against enjoining the government from seeking 2703(d) orders. (R.15, Response in Opposition re Motion for TRO; JA ____). On the merits of Warshak's Fourth Amendment claim, the government explained that compelled disclosure under the Fourth Amendment was based on a reasonableness standard, not probable cause, and that the 2703(d) orders in this case complied with the Fourth Amendment's reasonableness standard. (*Id.* at 4-12; JA ____). On the merits of Warshak's statutory claim, the government explained that the SCA allowed compelled disclosure of previously opened or sent e-mail pursuant to a 2703(d) order, and also that injunctive relief was not available against the United States for a statutory violation of the SCA. (*Id.* at 12-16; JA ____).

The district court held a hearing on Warshak's motion on July 5, 2006. (R.23, Transcript of Proceedings held on 7/05/06; JA ____). The hearing is noteworthy for what Warshak did not present: evidence or testimony of any kind.

Warshak presented no evidence that he continued to maintain an e-mail account at all, let alone that he had a reasonable expectation of privacy in any particular e-mail account. He presented no evidence regarding how e-mail works, how service providers store e-mail on their computer systems, how service providers' freely access such stored e-mail, or about industry practices regarding access to stored e-mail and compelled discovery. His TRO motion is based entirely on the unsupported assertions of counsel.

On July 21, 2006, the district court issued an order granting in part and denying in part Warshak's motion and entered a preliminary injunction against the United States. (R.21, Order granting in part and denying in part Motion for TRO; JA __) (hereinafter, "Order"). In its Order, the district court did not address Warshak's statutory argument. (*Id.* at 11; JA __). Instead, it considered only Warshak's Fourth Amendment claim. The district court did not explain why it was ignoring the principle "that courts avoid reaching constitutional questions in advance of the necessity of deciding them." *Lyng v. Northwest Indian Cemetery Protective Ass'n*, 485 U.S. 439, 445 (1988).

The district court first considered whether Warshak had shown a strong likelihood of success on the merits. The court accepted Warshak's bald assertions that "the owner of the email can repossess a read-and-then-closed email at any moment, without any notice or permission from the ISP [Internet Service

Provider], can retake the email, delete the email from his mailbox, or do what she wants to do with the email.” (Order at 10; JA ___). The district court dismissed the government’s argument that ISPs reserve the right to open, delete, or disclose the content of e-mail, yet conceded that “the terms of service governing email accounts can vary from ISP to ISP.” (*Id.*) The district court concluded that “it is not persuaded – as an initial matter – that an individual surrenders his reasonable expectation of privacy in his personal emails once he allows those emails (or electronic copies thereof) to be stored on a subscriber account maintained on the server of a commercial ISP.” (*Id.* at 11; JA ___). From this finding, the district court concluded that “Warshak has shown a substantial likelihood of success on the merits of his Fourth Amendment claim.” (*Id.*) Based largely on its conclusion that Warshak had shown a likelihood of success on the merits, the district court concluded that the other factors used to determine whether to issue a preliminary injunction weighed in Warshak’s favor. (*Id.* at 11-16; JA ___).

Finally, the court turned to the scope of its injunction against the United States. It acknowledged that any expectation of privacy in an e-mail account “could turn in part on facts specific to the account in question.” (*Id.* at 16; JA ___). However, the court still found that the constitutional flaws in §§ 2703 and 2705 were “facial in nature.” (*Id.* at 18; JA ___). The district court focused on the delayed notice provisions of the SCA, and it stated that “the Court preliminary

[sic] holds that 18 U.S.C. subsections §§ 2703(b)(1)(B)(ii), 2703(d) and 2705 violate the Fourth Amendment of the United States Constitution to the extent they collectively authorize the *ex parte* issuance of search and seizure orders without a warrant and on less than a showing of a probable cause.” (*Id.*) Not limiting itself to the plaintiffs before it, the court then ordered that “The United States is accordingly **ENJOINED**, pending final judgment on the merits of Plaintiffs' claims, from seizing, pursuant to court order under 18 U.S.C. § 2703(d), the contents of any personal email account maintained by an Internet Service Provider in the name of any resident of the Southern District of Ohio without providing the relevant account holder or subscriber prior notice and an opportunity to be heard on any complaint, motion, or other pleading seeking issuance of such an order.” (*Id.* at 19; JA __).

On August 16, 2006, the government moved for a stay pending appeal in the district court. The district court has not ruled on that motion.

SUMMARY OF THE ARGUMENT

For twenty years, the Stored Communications Act has set forth the procedures that the government must follow to compel disclosure of e-mail, and no court has previously held it to be unconstitutional. In this case, on a nearly nonexistent factual record, the district court held the SCA facially unconstitutional to the extent it allows the government to compel disclosure of e-mail without prior notice to the account holder. The district court enjoined the United States from using 2703(d) orders to compel disclosure of the e-mail not only of Warshak, but of any resident of the Southern District of Ohio. It took this extraordinary action despite the fact that the government had neither sought nor served 2703(d) orders directed to the content of e-mail in accounts registered to Warshak since September 2005.

The United States respectfully submits that the district court erred for at least four reasons. *First*, the district court lacked subject matter jurisdiction to issue the preliminary injunction. Here, neither Warshak nor his e-mail accounts were subject to 2703(d) orders when Warshak filed his original complaint, and no such process is imminent. The district court made clear in its order that its purpose in mandating prior notice to Warshak before the government could obtain future 2703(d) orders was to enable him to present his constitutional challenge “in the ripe, concrete context of a specific email account targeted *but not yet seized by the*

United States.” (Order at 17; JA ___) (emphasis added). This finding highlights the fact that there is currently no “ripe, concrete context” in which to apply Warshak’s constitutional claims and demonstrates that Warshak has failed to allege facts sufficient to establish that the district court has subject matter jurisdiction to consider his claims for prospective relief. Thus, the district court lacked the subject matter jurisdiction to issue the preliminary injunction.

Second, even assuming justiciability, the district court ignored the law applicable to facial challenges. A facial challenge based on the Fourth Amendment can succeed only if there is no possible constitutional application of the statute. Thus, to demonstrate that the district court improperly applied existing law in enjoining the government from compelling disclosure of e-mail via 2703(d) orders, the government must show only that compelled disclosure of e-mail is constitutionally permissible in some circumstances. In addition to the instant application, there are many situations in which compelled disclosure of e-mail is plainly consistent with the Fourth Amendment. Many e-mail users explicitly agree to waive any possible expectation of privacy in their accounts. Others contractually agree to give their service providers full access to all the content stored in their accounts, or they agree that their service providers may disclose the content of e-mail from their accounts in response to legal process. Indeed, the district court itself recognized that the “extent of . . . privacy expectations in a

given email account – and hence the ultimate constitutionality of any warrantless seizure of emails stored in that account – could turn in part on facts specific to the account in question, such as the terms of the subscriber agreement.” (Order at 16; JA ___). Because the SCA is capable of constitutional application in a wide variety of circumstances, the district court abused its discretion in issuing its injunction.

Third, it is important to emphasize that although these specific circumstances are sufficient to demonstrate that the district court should have rejected Warshak’s facial challenge to the SCA, the government does not maintain that compelled disclosure of e-mail is proper only in these specific circumstances. Instead, the fundamental principle that controls this case is that compelled disclosure of e-mail pursuant to 2703(d) orders is proper because the Fourth Amendment imposes only a reasonableness challenge on compelled disclosure. In mandating a probable cause standard, the district court applied the wrong legal standard. Imposing a probable cause standard on the government’s use of compelled disclosure ignores a fundamental purpose for compelled disclosure: to determine whether probable cause exists. As the Supreme Court has explained in the context of subpoenas, “the Government cannot be required to justify the issuance of a grand jury subpoena by presenting evidence sufficient to establish probable cause because the very purpose of requesting the information is to

ascertain whether probable cause exists.” *United States v. R Enterprises, Inc.*, 498 U.S. 292, 297 (1991).

Fourth, the preliminary injunction should be vacated because the other preliminary injunction factors weigh against granting an injunction in this case. Warshak will not suffer irreparable harm if the preliminary injunction is vacated for at least two reasons. First, Warshak failed to show that there is a real and immediate threat that he will be subjected to 2703(d) orders in the future. Second, there is an adequate remedy at law to redress any alleged violation of Warshak’s rights caused by a 2703(d) order. Warshak has the right to file a damages claim, and if the government seeks to use any e-mail obtained via 2703(d) orders in the parallel criminal action against him, he will have the opportunity to challenge the constitutionality of 2703(d) orders through a motion to suppress.

Finally, this Court should vacate the preliminary injunction because the preliminary injunction will cause substantial harm to others and does not serve the public interest. The preliminary injunction is already harming the criminal investigation process by requiring the government to give prior notice of 2703(d) orders, even in cases where such prior notice would jeopardize the investigation. Impairing lawful criminal investigations harms the public interest.

ARGUMENT

I. THE DISTRICT COURT LACKED SUBJECT MATTER JURISDICTION TO ISSUE THE PRELIMINARY INJUNCTION

Appellee Warshak has failed to allege facts sufficient to carry his burden of establishing that the district court had subject matter jurisdiction to issue the preliminary injunction. It is axiomatic that judicial power extends only to live cases or controversies. In an attempt to give meaning to Article III's case-or-controversy requirement, the courts have developed a series of justiciability doctrines, among which are standing and ripeness. *See Steel Co. v. Citizens for a Better Environment*, 523 U.S. 83, 102 (1998). Each of these doctrines presents an independent bar to the Court's consideration of Warshak's claims and its jurisdiction to issue the preliminary injunction.²

A. Appellee Lacks Standing.

Appellee Warshak lacks standing in this case because he has failed to allege that he is currently suffering (or will imminently suffer):

- (1) an injury-in-fact that invades (a) a "concrete" and "particularized" legally protected interest of plaintiff (b) that is "actual or imminent, not conjectural or hypothetical;"
- (2) that is fairly traceable to the challenged action of defendant; and

² Standing and ripeness are closely interrelated on the facts in this case and, indeed, to a degree, overlap. *Warth v. Seldin*, 422 U.S. 490, 499 n. 10 (1975).

- (3) is likely, as opposed to merely speculative, to be redressed by a favorable decision.

Steel Co., 523 U.S. at 102-04; *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992). These elements are the “irreducible constitutional minimum of standing” mandated by the case-or-controversy requirement of Article III. *Steel Co.*, 523 U.S. at 102; *Lujan*, 504 U.S. at 560. In this case, Warshak has failed to carry his burden of alleging facts sufficient to satisfy all of the elements of standing. *Steel Co.*, 523 U.S. at 104.

Most notably, Warshak has failed to allege the first standing requirement – an actual or imminent injury-in-fact – and the district court did not identify any such injury in its preliminary injunction. Nevertheless, the court issued the preliminary injunction based purely on speculation that “the United States may continue to invoke the SCA’s *ex parte* provisions” to seek 2703(d) orders harming Warshak in the future. (Order at 18; JA ____). The court justified its position because of “the United States’ past [*ex parte*] seizures of Warshak’s NuVox and Yahoo accounts and its refusal to commit not to undertake future seizures.” (*Id.* at 17-18; JA ____). It is undisputed, however, that the “past seizures” pursuant to § 2703(d) orders were no longer pending when Warshak filed his complaint and that “this [District] Court obviously cannot predict what the United States will do in the future.” (*Id.* at 17; JA ____).

To satisfy the “injury-in-fact” element of standing, the court must find that Warshak suffers harm that is “actual or imminent,” “concrete” and “particularized” when the complaint was filed. *See Steel Co.*, 523 U.S. at 103; *Lujan*, 504 U.S. at 560; *Whitmore v. Arkansas*, 495 U.S. 149, 155 (1990) (an injury-in-fact “must be concrete in both a qualitative and temporal sense”). Warshak’s standing to seek injunctive relief depends, *inter alia*, on whether he was likely to suffer future injury from future 2703(d) orders when he filed his original complaint. *See City of Los Angeles v. Lyons*, 461 U.S. 95, 105 (1983). Warshak’s claim that prior 2703(d) orders were unconstitutional may have afforded Warshak standing to claim damages against the government. *Lyons*, 461 U.S. at 105; *see, e.g.*, 18 U.S.C. § 2712. However, as the court correctly noted, Warshak seeks only *prospective* relief. (Order at 2; JA ___). Thus, Warshak’s allegations of past harm do nothing to establish a claim for *prospective* injunctive relief because they do not show a real and immediate threat that Warshak or his e-mail accounts would again be subject to legal process pursuant to the SCA. *See Lyons*, 461 U.S. at 105 (holding that the district court properly dismissed plaintiff’s claim for injunctive relief for lack of standing because plaintiff’s past injury “does nothing to establish a real and immediate threat that [the plaintiff] would again” suffer similar injury in the future). For Warshak to have standing to seek *prospective* injunctive relief, he must show a real threat of future injury from orders issued in the future, not an

indefinite threat based purely on his “subjective apprehensions” about the future. *Id.* at 107 n.8 (“It is the *reality* of the threat of repeated injury that is relevant to the standing inquiry, not the plaintiff’s subjective apprehensions. The emotional consequences of a prior act simply are not a sufficient basis for an injunction absent a real and immediate threat of future injury by defendant.”).

Warshak does not satisfy this standard when he merely alleges “an injury at some indefinite future time.” *Lujan*, 504 U.S. at 564, 564 n.2. Yet the district court relied on precisely these kinds of hypothetical allegations of injury in issuing the preliminary injunction. Whatever injury-in-fact Warshak may have been able to allege when past 2703(d) orders were pending, his alleged injury with respect to those orders ended when they were served in 2005. It is undisputed that the 2703(d) orders referenced in the preliminary injunction were no longer pending when Warshak filed his June 2006 complaint, and no new 2703(d) orders applicable to him or his e-mail accounts have been issued since 2005. In other words, Warshak does not (and indeed cannot) allege that he is subject to any pending 2703(d) orders that are causing him any alleged injury.

It is also undisputed that Warshak will not be “imminently” subject to such legal process in the future. Warshak’s allegation of harm is limited to his claim that the government has the *capability* of seeking additional legal process pursuant to the SCA, not that such process is imminent. (*E.g.* R.11; Memorandum in

Support of Motion for TRO at 16; JA ___). Warshak concedes that he can only guess as to whether such process will occur in the next week, month, or ever. (See R.30, Plaintiffs' Opposition to Government's Motion to Stay Pending Appeal at 22; JA ___). Indeed, as the district court noted, "this Court obviously cannot predict what the United States will do in the future." (Order at 17; JA ___). This is precisely the type of conjecture and speculation that the Supreme Court has held will not satisfy the injury-in-fact standard. "Although 'imminence' is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes – that the injury is 'certainly impending.'" *Lujan*, 504 U.S. at 564-65 n.2 (citing *Whitmore*, 495 U.S. at 158 ("Allegations of possible future injury do not satisfy the requirements of Article III. A threatened injury must be 'certainly impending' to constitute injury in fact.")). Thus, it is pure speculation that Warshak will allegedly suffer harm as a result of future, post-indictment 2703(d) orders since such legal process is clearly not "certainly impending."

Despite the clear lack of an "actual or imminent" 2703(d) order that could allegedly harm Warshak, his motion for a preliminary injunction exclusively sought prospective relief. (Order at 2; JA ___). The 2703(d) orders referenced in the 2006 complaint were served no later than in 2005 – long before the original complaint was ever filed. Warshak's claims for *prospective* relief, therefore,

became non-justiciable *before* he filed his complaint. *See Renne v. Geary*, 501 U.S. 312, 320 (1991) (“Justiciability concerns not only the standing of litigants to assert particular claims, but also the appropriate timing of judicial intervention.”). The Supreme Court has uniformly held that a “live” Article III case or controversy ceases to exist where the dispute ends before a complaint is filed. *Friends of the Earth, Inc. v. Laidlaw Environ. Servs., Inc.*, 528 U.S. 167, 191 (2000); *Steel Co.*, 523 U.S. at 109 (same); *Renne*, 501 U.S. at 320 (same).

Moreover, even assuming *arguendo* that Warshak could allege that past 2703(d) orders were unconstitutional and had unlawfully harmed him *in the past*, it would not establish a threat of similar injury *in the future* sufficient to establish a case or controversy for prospective relief. *See Lujan*, 504 U.S. at 564 (“Past exposure to illegal conduct does not in itself show a present case or controversy regarding injunctive relief . . . if unaccompanied by any continuing, present adverse effects.”) (internal quotations omitted); *Lyons*, 461 U.S. at 105 (holding that the district court properly dismissed plaintiff’s claim for injunctive relief for lack of standing because plaintiff’s past injury “does nothing to establish a real and immediate threat that [the plaintiff] would again” suffer similar injury in the future). For example, in *Los Angeles v. Lyons*, the Supreme Court held that a plaintiff lacked standing to seek an injunction against enforcement of an allegedly unlawful police chokehold policy that had been applied to the plaintiff in the past

because he could not credibly allege that he faced a realistic threat from the police in the future at the time that he had filed his complaint. 461 U.S. at 105-06, 107 n.7. As *Lyons* emphasized, “it is surely no more than speculation to assert either that [plaintiff] himself will again be involved in one of those unfortunate instances, or that he will be arrested in the future and provoke the use of the chokehold by resisting arrest, attempting to escape, or threatening deadly force or serious bodily injury.” *Id.* at 108.³

³ In the same vein, the fact that the government has refused to abstain from using 2703(d) orders to compel disclosure of e-mail is not enough to establish a threat of imminent harm sufficient to satisfy standing’s injury-in-fact requirement. Unlike the mootness doctrine, the standing doctrine does not grant an exception for government conduct that is “capable of repetition, yet evading review.” Where, as here, a plaintiff lacks standing when the complaint is filed, even a case or controversy that is capable of repetition, yet evading review, will not entitle a plaintiff to a federal judicial forum. *Laidlaw*, 528 U.S. at 191. For this reason, the Supreme Court has long held that “the mootness exception for disputes capable of repetition yet evading review . . . will not revive a dispute which became moot before the action commenced.” *Steel Co.*, 523 U.S. at 109 (quoting *Renne*, 501 U.S. at 320). Most significantly, even if Warshak could present the court with facts satisfying the “capable of repetition, yet evading review” exception to mootness (and he cannot), that showing alone would not satisfy standing’s injury-in-fact requirement. *Laidlaw*, 528 U.S. at 190 (“there are circumstances in which the prospect that a defendant will engage in (or resume) harmful conduct may be too speculative to support standing, but not too speculative to overcome mootness.”).

In addition, Warshak cannot rely on the voluntary cessation exception to mootness to cure his lack of standing because “[i]t is an immense and unacceptable stretch to call the [voluntary cessation] presumption into service as a substitute for the allegation of present or threatened injury upon which initial standing must be based.” *Steel Co.*, 523 U.S. at 109; accord *Laidlaw*, 528 U.S. at 191 (same, citing *Steel Co.*).

The district court also lacked subject matter jurisdiction because Warshak cannot satisfy the redressability element of constitutional standing. A prospective preliminary injunction does not redress the alleged injuries caused by 2703(d) orders that were served before Warshak filed his complaint. Federal courts uniformly preclude plaintiffs from seeking prospective declaratory or injunctive relief for past injuries. *See, e.g., Steel Co.*, 523 U.S. at 108 (holding that plaintiff failed to satisfy the redressability requirement because prospective injunctive relief “cannot conceivably remedy any past wrong”).

As already noted, there are no pending or imminent 2703(d) orders that apply to Warshak that a preliminary injunction could redress. As a result, Warshak’s request for prospective injunctive relief simply attempts to redress “the vindication of the rule of law – the ‘undifferentiated public interest’ in faithful execution of” federal law. *Steel Co.*, 523 U.S. at 106, 106-07 (“This does not suffice” to establish redressability because “although a suitor may derive great comfort and joy from the fact that . . . the Nation’s laws are faithfully enforced, that psychic satisfaction is not an acceptable Article III remedy because it does not redress a cognizable Article III injury.”). Injunctive relief, however, must redress an on-going or imminent injury-in-fact particular to Warshak, not a generalized and undifferentiated interest in deterring the government from conduct that Warshak believes is unlawful. “[T]hat is the very essence of the redressability

requirement.” *Steel Co.*, 523 U.S. at 107. A generalized and undifferentiated interest in deterrence, therefore, is insufficient for purposes of Article III standing. *Id.* at 108-09. Here, a preliminary injunction will not redress any harm particularized to Warshak because his prospective interests in the constitutionality of 2703(d) orders are no different than those of any other U.S. citizen. Thus, the district court lacked subject jurisdiction to issue the preliminary injunction because it does not redress an on-going or imminent injury-in-fact.

B. Appellee’s Claims Are Not Ripe.

Even if Appellee Warshak could establish standing (and he cannot), the district court lacked subject matter jurisdiction to issue the preliminary injunction because Warshak’s claims are not ripe. The ripeness doctrine has both a constitutional component and a prudential one, and Warshak cannot satisfy the requirements of either. *See, e.g., Adult Video Ass’n v. U.S. Dept. of Justice*, 71 F.3d 563, 567 (6th Cir. 1995) (“[t]he ripeness doctrine not only depends on the finding of a case and controversy and hence jurisdiction under Article III, but it also requires that the court exercise its discretion to determine if judicial resolution would be desirable under all of the circumstances”) (citation omitted). The district court made clear in its preliminary injunction that its purpose in mandating prior notice to Warshak before the government could obtain future 2703(d) orders was to allow him to present his constitutional challenge “in the ripe, concrete context of

a specific email account targeted *but not yet seized by the United States.*” (Order at 17; JA __ (emphasis added)). This finding highlights the fact that there is currently no “ripe, concrete context” in which to apply Warshak’s constitutional claim and demonstrates that Warshak has failed to allege facts sufficient to establish a ripe claim.

Thus, as with standing, Warshak’s claims are not constitutionally ripe because Warshak has failed to allege injuries that are concrete, not hypothetical, and may actually come to pass. *Adult Video*, 71 F.3d at 568 (holding that “even if we assume that Adult Video has alleged an unconstitutional harm, it has not established that the harm will come to pass”). Neither Warshak nor the district court have identified any action or statement by the government indicating that it intends to seek, or that a court will issue, any new 2703(d) orders directed at Warshak or his e-mail accounts. *See id.* (affirming holding that case is not ripe for review and that “it [was] far from clear that any harm will occur . . . [to the plaintiff] in the future” because the plaintiff “can point to no action or statement by the federal government indicating that it intends to take action” against the plaintiff). Indeed, as the district court stated in its preliminary injunction order, “this Court obviously cannot predict what the United States will do in the future.” (Order at 17; JA __). Hence, because Warshak’s claims are completely contingent on a court authorizing a 2703(d) order sometime in the future, Warshak’s claims

are not constitutionally ripe. *Texas v. United States*, 523 U.S. 296, 300 (1998) (holding that plaintiff's claim is not ripe "if it rests upon contingent future events that may not occur as anticipated, or indeed may not occur at all") (citation omitted); *Adult Video*, 71 F.3d at 568 (same).

In addition, prudential ripeness bars jurisdiction because Warshak's claims would cause this Court to entangle itself in abstract disagreements prematurely. In analyzing prudential ripeness, courts apply a two-part test: (1) the fitness of the issues for judicial decision and (2) the hardship of the parties of withholding consideration. *Texas*, 523 U.S. at 300-01. Warshak's constitutional challenge to 2703(d) orders is not ripe under this test. Here, the preliminary injunction bars the United States from issuing *ex parte* 2703(d) orders in the future based on Warshak's claim that when Defendant serves a 2703(d) order, it does so unlawfully. Such claims, however, are not fit for judicial review because neither the parties nor the district court have any idea whether or when (or in what factual context) such legal process will occur. *See id.* at 300 (holding that "where 'we have no idea whether or when such [a sanction] will be ordered,' the issue is not fit for adjudication") (internal citations omitted, brackets in original). Similarly, withholding consideration of Warshak's abstract constitutional claims does not constitute a hardship on Warshak because unless and until he is subject to a new 2703(d) order, Warshak is not subject to any hardship. *Id.* at 301 (holding that

plaintiff's claim of an immediate hardship of a "threat to federalism" was an abstraction because plaintiff was not yet "required to engage in, or refrain from, any conduct"); *cf. Adult Video*, 71 F.3d at 568 (noting that "[i]ndividuals who choose to conduct their affairs along the boundaries of the criminal law will necessarily incur some risks concerning the legality of their conduct").

Accordingly, the district court did not have subject matter jurisdiction to issue the preliminary injunction because Warshak's claims are not ripe.

II. THE DISTRICT COURT ABUSED ITS DISCRETION IN ISSUING THE PRELIMINARY INJUNCTION

A. Standard of Review

A grant of a preliminary injunction is reviewed for abuse of discretion, which will be found "if the district court relied upon clearly erroneous findings of fact, improperly applied the governing law, or used an erroneous legal standard." *Bonnell v. Lorenzo*, 241 F.3d 800, 809 (6th Cir. 2000). In addressing a motion for preliminary injunction, a district court should consider whether (1) the movant has a strong likelihood of success on the merits; (2) the movant would suffer irreparable injury without the injunction; (3) issuance of the injunction would cause substantial harm to others; and (4) the public interest would be served by issuance of the injunction. *Id.* A preliminary injunction should not be granted in cases which are doubtful or do not come within well-established principles of law.

See Detroit Newspaper Publ's Ass'n v. Detroit Typographical Union No. 18, 471 F.2d 872, 876 (6th Cir. 1972).

B. The District Court Used an Erroneous Legal Standard in Issuing the Injunction by Holding the SCA Facially Unconstitutional

The district court held the SCA facially unconstitutional to the extent it authorizes compelled disclosure of e-mail without notice to the account holder on less than a showing of probable cause. This holding ignores the law applicable to facial challenges.⁴ Facial challenges to statutes are disfavored. *See FW/PBS, Inc. v. Dallas*, 493 U.S. 215, 223 (1990). This Court has held that “[o]utside the First Amendment context, we will only uphold a facial challenge to a statute if the challenging party can demonstrate that there is no constitutional application of the statute.” *Coleman v. DeWitt*, 282 F.3d 908, 914 (6th Cir. 2002) (citing *United States v. Salerno*, 481 U.S. 739, 745-46 (1987)). In *Coleman*, this Court noted that “facial constitutional challenges are universally unsuccessful as defenses to criminal prosecutions for non-expressive conduct. If the statute is constitutional as

⁴ The District Court did not – and could not – uphold Warshak’s “as applied challenge” seeking prospective injunctive relief, as Warshak did not present sufficient evidence to support such a challenge. Warshak presented no evidence that he continued to maintain an e-mail account at all, let alone that he continued to maintain a reasonable expectation of privacy in any particular e-mail account. An individual seeking to establish a Fourth Amendment violation must exhibit a “subjective” expectation of privacy, and this expectation must be “one that society is prepared to recognize as reasonable.” *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (citations and quotations omitted). There is no evidence in the record establishing Warshak’s subjective expectation of privacy in any e-mail account.

applied to the defendant's activities, it a fortiori fails the Salerno standard.” *Id.* at 914 n.3. Thus, the district court’s injunction would be proper only if the Fourth Amendment is always violated when the government compels disclosure of the content of e-mail without notice to the account holder on less than a showing of probable cause.⁵

In order to demonstrate that the district court abused its discretion in upholding a facial challenge to the SCA, the government need only demonstrate that the SCA is capable of constitutional application. The district court conceded that it can be. In its order, the district court recognized that the “extent of . . . privacy expectations in a given email account – and hence the ultimate constitutionality of any warrantless seizure of emails stored in that account – could turn in part on facts specific to the account in question, such as the terms of the subscriber agreement.” (Order at 16; JA ___). Under such circumstances, a facial challenge to the SCA cannot succeed, as the statute will unquestionably have constitutional application in many situations. The district court’s injunction must be reversed.

⁵ It should be noted that the government does not maintain that compelled disclosure of e-mail is proper only in the specific circumstances described in this section. As set forth in Section II.C. below, the Fourth Amendment imposes only a reasonableness standard on compelled disclosure, and 2703(d) orders are consistent with this standard.

In addition, the statute plainly can be applied constitutionally whenever the subscriber has no reasonable expectation of privacy. “The touchstone of Fourth Amendment analysis is whether a person has a constitutionally protected reasonable expectation of privacy.” *California v. Ciraolo*, 476 U.S. 207, 211 (1986) (quotation marks omitted). Law enforcement seeks 2703(d) orders in a variety of situations in which e-mail account holders have no reasonable expectation of privacy, and thus in which compelled disclosure of e-mail cannot possibly violate the Fourth Amendment.

For example, this Court has held that any expectation of privacy in a computer can be waived. *See Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001) (holding that a privacy disclaimer on an electronic bulletin board “defeats claims to an objectively reasonable expectation of privacy”). Many employees are provided with e-mail and Internet service by their employers. Often, those employees are required to waive any expectation of privacy in their e-mail each time they log on to their computers. In order to access their computers, employees may be required to click on a banner and agree to the following: “By accessing and using this computer, you acknowledge that you have no reasonable expectation of privacy in any information (including e-mail) stored on or accessed through this computer system, and you consent to monitoring of your use of this system and disclosure of information stored on this system for law enforcement or other purposes.” Section

2703(d) orders directed to the e-mail of employees who have waived any possible expectation of privacy do not violate the Fourth Amendment. Because the government may constitutionally seek 2703(d) orders directed to the e-mail in this circumstance, Warshak's facial Fourth Amendment challenge must fail.

Law enforcement also seeks 2703(d) orders in other situations in which e-mail account holders have no reasonable expectation of privacy. Some e-mail accounts are abandoned, as when an account holder stops paying for the service and the account is cancelled. There is no reason why the Fourth Amendment doctrine of abandonment does not include e-mail accounts, and thus there can be no reasonable expectation of privacy in such accounts. *See United States v. Allen*, 106 F.3d 695, 699 (6th Cir. 1997) (holding that “[o]nce a hotel guest's rental period has expired or been lawfully terminated, the guest does not have a legitimate expectation of privacy in the hotel room”) (quotation marks omitted). Other e-mail accounts are procured through fraudulent means. For example, hackers may obtain Internet services and e-mail accounts using stolen credit cards. Hackers maintain no reasonable expectation of privacy in such accounts. *See United States v. Caymen*, 404 F.3d 1196, 1201 (9th Cir. 2005) (“Because, as the district court found, Caymen obtained the laptop computer by fraud, he had no legitimate expectation of privacy in the contents of the hard drive.”). The SCA may be

applied constitutionally in such cases, and a facial challenge to the SCA is therefore improper.

Compelled disclosure of e-mail pursuant to 2703(d) orders is also often permissible under the terms of service of many commercial service providers. The Internet is frequently used by hackers, spammers, scammers, and child pornographers. Service providers usually do not want such criminals as customers, so they often have terms of service agreements stipulating that they may cooperate with law enforcement and respond to legal process. For example, Yahoo! (the recipient of one of the two 2703(d) orders issued for e-mail of Warshak) explicitly reserves the right to access stored e-mail and comply with legal process:

You acknowledge that Yahoo! may or may not pre-screen Content, but that Yahoo! and its designees shall have the right (but not the obligation) in their sole discretion to pre-screen, refuse, or move any Content that is available via the Service. . . .

You acknowledge, consent and agree that Yahoo! may access, preserve and disclose your account information and Content if required to do so by law or in a good faith belief that such access preservation or disclosure is reasonably necessary to: (a) comply with legal process; (b) enforce the TOS; (c) respond to claims that any Content violates the rights of third parties; (d) respond to your requests for customer service; or (e) protect the rights, property or personal safety of Yahoo!, its users and the public.

(R. 16, Response in Opposition re Motion for TRO at 10; JA __). Because a customer acknowledges that Yahoo! has unlimited access to her e-mail, and because she consents to Yahoo! disclosing her e-mail in response to legal process,

compelled disclosure of e-mail from a Yahoo! account does not violate the Fourth Amendment. *See United States v. Miller*, 425 U.S. 435, 443 (1976) (“the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed”) (citing *Hoffa v. United States*, 385 U.S. 293, 302 (1966)).

To demonstrate that the district court’s facial injunction against compelled disclosure of e-mail is improper, the government must show that the SCA is capable of constitutional application in some circumstance. The government has far surpassed this standard: it has described a myriad of situations in which compelled disclosure of e-mail pursuant to a 2703(d) order does not violate the Fourth Amendment. E-mail account holders may waive their expectation of privacy, abandon their accounts, waive their rights by procuring their accounts through fraud, agree that the service provider may access their accounts, or agree that the service provider may comply with compelled disclosure orders. The district court’s injunction – which extends beyond Warshak to every resident of the Southern District of Ohio – forbids the government from compelling disclosure of

e-mail in a wide variety of circumstances in which compelled disclosure is proper.⁶

It should therefore be reversed.

C. The District Court Used an Erroneous Legal Standard in Issuing the Injunction by Applying a Probable Cause Standard to the Compelled Disclosure of E-mail, Rather than a Reasonableness Standard

The district court's injunction in this case should be reversed because it is based on the wrong legal standard: it applied a probable cause standard to compelled disclosure of e-mail, but the Fourth Amendment sets a reasonableness standard for compelled disclosure. *See In re Administrative Subpoena John Doe, D.P.M.*, 253 F.3d 256, 265 (6th Cir. 2001). A century of Supreme Court case law underlies the principle that compelled disclosure is based on a reasonableness standard. In addition, to the extent that the district court's injunction is based on the concern that e-mail account holders receive prior notice, the Supreme Court has explicitly rejected the proposition that the target of an investigation is entitled to such notice. *See SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984).

⁶ The District Court limited its injunction against compelled disclosure of e-mail to cases in which the government did not provide the account owner with prior notice. However, as discussed more fully in Section II.C.4 below, the Supreme Court has explicitly held that the target of an investigation has no Fourth Amendment right to notice of third-party compelled disclosure. *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984). Because the Constitution does not require notice to the target of third-party compelled disclosure, the District Court erred in holding the SCA's delayed notice provision unconstitutional.

The district court did not explain why it ignored the established principle that compelled disclosure is based on a reasonableness standard. It stated that it was not persuaded “that an individual surrenders his reasonable expectation of privacy” in e-mail stored by a commercial ISP. (Order at 11; JA ___). Based on this determination, the district court enjoined the government from using 2703(d) orders to compel disclosure of e-mail without prior notice to the subscriber. (Order at 19; JA ___). As an initial matter, the record in this case does not support the district court’s determination that e-mail account owners maintain a reasonable expectation of privacy in their accounts. Indeed, Warshak presented no evidence or testimony on this point whatsoever. His argument that an e-mail account holder maintains a reasonable expectation of privacy is based solely on the unsupported assertions of counsel, but the unsupported assertions of counsel do not constitute evidence. *See Hana v. Gonzales*, 157 Fed. Appx. 880, 885 (6th Cir. 2005). With no factual record to support the district court’s injunction, this Court must reverse.

More fundamentally, however, even if some e-mail account owner did maintain a reasonable expectation of privacy, 2703(d) orders for the content of e-mail still comply with the Fourth Amendment. The fundamental principle that controls this case is that compelled disclosure is judged under a reasonableness standard, not a probable cause standard. This principle is robust and well-established, and there is simply no basis for not applying it to e-mail accounts. As

set forth below, existing case law also demonstrates: (1) that a reasonableness standard governs not only compelled disclosure from a targeted individual but also from a third party; (2) that a target's reasonable expectation of privacy affects only his standing to challenge the reasonableness of compelled disclosure; and (3) that the government may compel a third party to disclose anything that the third party can access. In seeking an injunction, Warshak did not argue and the district court did not find that 2703(d) orders violate the reasonableness standard applicable to compelled disclosure. Thus, because service providers may access the e-mail stored on their own computers, 2703(d) orders for e-mail comply with the Fourth Amendment.

1. The Fourth Amendment Sets a Reasonableness Standard for Compelled Disclosure.

By its terms, the Fourth Amendment protects people against unreasonable searches and seizures, but it imposes a probable cause requirement only on the issuance of warrants. *See* U.S. Const. amend. IV (“and no Warrants shall issue, but upon probable cause”). The Supreme Court has repeatedly affirmed for the past 100 years that compelled disclosure under the Fourth Amendment is based on a reasonableness standard. For example, in *Wilson v. United States*, 221 U.S. 361, 376 (1911), the Court held that “there is no unreasonable search and seizure when a [subpoena], suitably specific and properly limited in its scope, calls for the production of documents which, as against their lawful owner to whom the writ is

directed, the party procuring its issuance is entitled to have produced.” *See also Oklahoma Press Publishing Co. v. Walling*, 327 U.S. 186, 208 (1946) (“the Fourth [Amendment], if applicable [to a subpoena], at the most guards against abuse only by way of too much indefiniteness or breadth in the things required to be ‘particularly described,’ 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, expressed in terms, that the disclosure sought shall not be unreasonable.”); *Donovan v. Lone Steer, Inc.*, 464 U.S. 408, 413-15 (1984); *In re Subpoena Duces Tecum*, 228 F.3d 341, 346-49 (4th Cir. 2000) (discussing the Fourth Amendment’s reasonableness requirement for subpoenas).

The Supreme Court has explained the reason why the Fourth Amendment distinguishes the compulsion of subpoenas from other forms of forcible search and seizure:

‘The latter is abrupt, is effected with force or the threat of it and often in demeaning circumstances, and, in the case of arrest, results in a record involving social stigma. A subpoena is served in the same manner as other legal process; it involves no stigma whatever; if the time for appearance is inconvenient, this can generally be altered; and it remains at all times under the control and supervision of a court.’

United States v. Dionisio, 410 U.S. 1, 10 (1973) (quoting *United States v. Doe*, 457 F.2d 895, 898 (2d Cir. 1972) (Friendly, J.)). It follows from this reasoning that 2703(d) orders (which, unlike subpoenas, must be approved by a court prior to issuance) should be analyzed under the same constitutional standards as subpoenas.

A 2703(d) order is issued by a court on a finding that the government has offered “specific and articulable facts showing that there are reasonable grounds to believe that the [information sought is] relevant and material to an ongoing criminal investigation,” and it is otherwise served and executed in the same manner as a subpoena. Like a subpoena, a 2703(d) order is a form of compelled disclosure that is not effected by force or the threat of force. The SCA specifically allows the recipient of a 2703(d) order to seek relief from the court issuing the order: “A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.” 18 U.S.C. § 2703(d). Thus, as with subpoenas, 2703(d) orders remain at all times under the control and supervision of a court.

In *In re Administrative Subpoena John Doe, D.P.M.*, 253 F.3d 256, 265 (6th Cir. 2001), this Court analyzed the Supreme Court’s Fourth Amendment subpoena jurisprudence and held that there was no probable cause requirement for a subpoena used during a criminal investigation. This Court held that a subpoena should be enforced, provided that:

- 1) it satisfies the terms of its authorizing statute, 2) the documents requested were relevant to the DOJ’s investigation, 3) the information sought is not already in the DOJ’s possession, and 4) enforcing the subpoena will not constitute an abuse of the court’s process.

Id. Here, a court order issued pursuant to § 2703(d) will satisfy these requirements. Section 2703 is the authorizing statute. Section 2703(d) orders are sufficiently limited in scope, relevant in purpose, and not an abuse of process because they are issued only when a court finds that there are “reasonable grounds to believe that the [information sought is] relevant and material to an ongoing criminal investigation.” 18 U.S.C. § 2703(d). In addition, the service provider may move to quash if compliance would be unreasonably burdensome (as where the documents sought are already in the government’s possession). *See id.* Thus, 2703(d) orders comport with the Fourth Amendment.

Although Warshak characterizes his Fourth Amendment claim as an argument that 2703(d) orders are unconstitutional, in fact his claim is much more sweeping (and unprecedented) than that. In matters of compulsory process, the Supreme Court has often observed that the public “has a right to every man’s evidence.” *Branzburg v. Hayes*, 408 U.S. 665, 688 (1972) (citing cases)⁷; *see also* 8 J. Wigmore, *Evidence* § 2192 (McNaughton rev. 1961) (“For more than three centuries it has now been recognized as a fundamental maxim that the public . . . has a right to every man’s evidence.”). Providers of electronic communication

⁷ Although these cases deal with subpoenas rather than 2703(d) orders, the authority to seek 2703(d) orders is a form of agency investigative authority, and the Supreme Court has analogized agency investigative power to that of grand juries. *See United States v. Morton Salt Co.*, 338 U.S. 632, 642-43 (1950).

service are not immune from this rule; they must respond to compulsory process just like everyone else. Indeed, § 2703(b) allows the use of a subpoena to compel disclosure of the content of e-mail in exactly the same circumstances as a 2703(d) order.

Broad compelled disclosure authority is essential to the ability of courts to determine truth. In noting that the duty to give testimony extends to the production of documents, Wigmore's Evidence treatise explains "[t]his testimonial duty to attend and disclose all that is needed for the ascertainment of truth applies to *every form and material of evidence* whatever." 8 J. Wigmore, Evidence § 2193 (McNaughton rev. 1961) (emphasis in original). Moreover, imposing a probable cause standard on the government's use of compelled disclosure ignores a fundamental purpose for compelled disclosure: to determine whether probable cause exists. As the Supreme Court has explained in the context of subpoenas, "the Government cannot be required to justify the issuance of a grand jury subpoena by presenting evidence sufficient to establish probable cause because the very purpose of requesting the information is to ascertain whether probable cause exists." *United States v. R Enterprises, Inc.*, 498 U.S. 292, 297 (1991).

In essence, Warshak is inviting the Court to invent an expansive new privilege against compelled disclosure of e-mail. According to Warshak, disclosure of e-mail cannot be compelled absent a judicial finding of probable

cause. (R.11, Motion for TRO at 5; JA ___). If this were true, however, records and other information could be shielded from grand juries or other investigations simply by storing the records as an e-mail. This Court should decline to create such a sweeping privilege. Indeed, the Supreme Court has refused to create new privileges against compelled discovery in situations much more limited than Warshak's proposed e-mail privilege. See *University of Pennsylvania v. EEOC*, 493 U.S. 182 (1990) (upholding compelled disclosure of confidential peer review materials relating to tenure); *Branzburg*, 408 U.S. at 679-80, 709 (holding that a grand jury could subpoena a newsman to appear and testify with respect to "confidential" sources). Because there is no probable cause requirement for compelled disclosure, the district court's injunction must be reversed.

2. The Fourth Amendment's Reasonableness Standard Governs Compelled Disclosure from a Third Party

The Fourth Amendment's reasonableness standard (rather than probable cause) applies when the government compels disclosure of information held by parties who are not themselves the subject of an investigation. For example, in *United States v. Phibbs*, 999 F.2d 1053, 1076-77 (6th Cir. 1993), a defendant challenged certain third-party subpoenas, arguing that "the district court erred in allowing the government to employ administrative subpoenas to uncover evidence without a finding of probable cause." *Id.* at 1076. This Court refused to apply a probable cause standard and reiterated the Fourth Amendment reasonableness

requirement, stating that a “subpoena has to be sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance [would] not be unreasonable.” *Id.* at 1077 (quotation marks omitted).

Courts have also rejected challenges to compelled disclosure of documents held by third parties. For example, in *Schwimmer v. United States*, 232 F.2d 855 (8th Cir. 1956), an attorney closed his office, placed his files in four cardboard boxes and four filing cabinet drawers, stored them with a storage company, and left the state. *See id.* at 858-59. The Eighth Circuit approved the use of a reasonably limited subpoena served on the storage facility for certain of Schwimmer’s documents. *See id.* at 861-63. Furthermore, the Fifth Circuit’s decision in *Newfield v. Ryan*, 91 F.2d 700 (5th Cir. 1937), is closely analogous to this case, as it also involves compelled disclosure of communications stored post-transmission by a communication service provider. In *Newfield*, the SEC subpoenaed a telegraph company for certain telegrams in its possession that had been sent or received by the targets of an investigation. The court held that Congress “was well within its constitutional powers” in granting subpoena authority to the SEC. *Id.* at 703. It held that the challenged subpoenas were issued “under the authority of a valid law, and for a public purpose,” and were lawful. *Id.* at 705. As a service provider is similar in function to a telegraph operator, *Newfield* directly supports the use of 2703(d) orders and subpoenas to compel disclosure of e-mail.

Critically, the constitutionality of a third-party subpoena turns on its reasonableness, not on whether the target has a reasonable expectation of privacy in the subpoenaed items. Thus, it would not even matter if Warshak's assertion that an e-mail is a closed container were correct. (See R.11, Motion for TRO at 5; JA ___). For example, in *United States v. Palmer*, 536 F.2d 1278, 1281-82 (9th Cir. 1976), Palmer was arrested for bank robbery and his car was impounded. Subsequently, at Palmer's direction, a third party picked up the car and delivered it to an attorney. Palmer may well have retained a reasonable expectation of privacy in the car, and the government could have violated Palmer's Fourth Amendment rights if it had seized items from the car without a warrant. Instead, however, the government served the attorney with a subpoena, and the attorney produced items from the car. The Ninth Circuit rejected Palmer's suppression motion because the subpoena was reasonable under the Fourth Amendment, and it therefore did not matter whether Palmer retained a reasonable expectation of privacy: "We do not explore the issue of a reasonable expectation of privacy, however, because the use of a properly limited subpoena does not constitute an unreasonable search and seizure under the Fourth Amendment." *Id.* at 1281-82.⁸

⁸ In the third-party compelled disclosure context, whether the target maintains a reasonable expectation of privacy in the targeted materials does have one consequence: a target of an investigation has standing to object to a third-party subpoena only if the target has a reasonable expectation of privacy in the subpoenaed items. For example, in *United States v. Miller*, 425 U.S. 435, 440-43

3. The Statutory Framework of the SCA and Industry Practice Support the Reasonableness of 2703(d) Orders

In evaluating the propriety of 2703(d) orders under the Fourth Amendment, this Court should also consider the statutory framework under which they were issued. Congress enacted the SCA in 1986, when e-mail and the Internet were still relatively new and used by few people. Through the SCA, Congress balanced the privacy interests of users of network communications, the rights of service providers to access and run their own computer networks, and the investigatory interests of the government. The SCA permits compelled disclosure of e-mail not in “electronic storage” (as that term is defined by 18 U.S.C. § 2510(17)) or e-mail in “electronic storage” for more than 180 days pursuant to a subpoena or 2703(d) order. *See* 18 U.S.C. § 2703(a), (b). In determining the scope of Fourth Amendment protections applicable to the rapidly developing contours of the online

(1976), the defendant had no standing to challenge an allegedly defective subpoena for bank records because he lacked a reasonable expectation of privacy in the challenged records. The Sixth Circuit applied this principle in *United States v. Phibbs*, 999 F.2d 1053, 1077 (6th Cir. 1993). The court rejected a Fourth Amendment challenge to a third-party subpoena and explained that “[h]ere, the administrative subpoenas were not directed at Rojas, but rather at third party businesses. As a consequence, he did not have standing to dispute their issuance on Fourth Amendment grounds, unless he could demonstrate that he had a legitimate expectation of privacy attaching to the records obtained.” *Id.* As a result of this principle, if an e-mail account owner retains a reasonable expectation of privacy in the contents of his e-mail, he has standing to challenge the reasonableness of the process used to compel its disclosure. However, the government is not required to show probable cause to compel the disclosure.

world, it is appropriate for courts to look to the legislative framework created by Congress.⁹ Internet and e-mail use has grown exponentially for the last twenty years under the SCA, and courts should be reluctant to upset at this late date the balance struck by Congress. *See Rostker v. Goldberg*, 453 U.S. 57, 64 (1981) (“Whenever called upon to judge the constitutionality of an Act of Congress – the gravest and most delicate duty this Court is called upon to perform – the Court accords great weight to the decisions of Congress.”).

The SCA also makes clear that service providers have the right to access all stored communications on their own computer systems. Section 2701 of the SCA provides civil and criminal penalties for unauthorized access to stored communications held by electronic communication service providers, such as ISPs. *See* 18 U.S.C. § 2701. However, § 2701 allows providers to access any stored communications on their own systems, as it includes a specific exception for “conduct authorized by the person or entity providing a wire or electronic communication service.” 18 U.S.C. § 2701(c)(1). Of course, the SCA is

⁹ Courts in other contexts have considered federal statutes and regulations in assessing Fourth Amendment claims. *See, e.g., Florida v. Riley*, 488 U.S. 445, 451 (1989) (plurality opinion) (looking to FAA regulations in determining defendant’s expectation of privacy regarding helicopter over his property); *United States v. Miller*, 425 U.S. 435, 442 (1976) (holding that there is no reasonable expectation of privacy in bank records and stating that a “lack of any legitimate expectation of privacy concerning the information kept in bank records was assumed by Congress in enacting the Bank Secrecy Act”); *Doe v. Brodderick*, 225 F.3d 440, 450-51 (4th Cir. 2000) (looking to federal statute to determine that plaintiff had reasonable expectation of privacy in his medical records).

concerned with preventing public service providers such as ISPs from violating the privacy of their customers. Yet it does so not by limiting providers' right to access to stored communications, but instead by limiting the providers' voluntary disclosure of the contents of communications except in specifically defined situations. *See* 18 U.S.C. § 2702(a), (b) (prohibiting voluntary disclosure of customer communications by public network service providers except in specified situations and specifically authorizing compelled disclosure pursuant to § 2703). Based on this statutory framework, service providers have unlimited access their own computers, and thus they may disclose information in response to compulsory process. Thus, through enactment of the SCA, Congress has shown that it regards the government's subpoenas and 2703(d) orders as reasonable under the Fourth Amendment.

Although Warshak asserts (without support) that service providers have at best a limited right to access e-mail stored on their servers, *see* (R.11, Motion for TRO at 9; JA ___), courts have rejected claims that service providers or computer system operators have limited rights to access to their own systems. For example, in *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114-15 (3rd Cir. 2003), the plaintiff sued his employer for violating § 2701 of the SCA after his employer (who provided e-mail service to him) went through its e-mail server and obtained copies of the plaintiff's previously opened and sent e-mail. The Third Circuit

rejected the employee's claim and held that "we read § 2701(c) literally to except from [the SCA's] protection all searches by communications service providers." *Id.* at 115; *see also Bohach v. City of Reno*, 932 F. Supp. 1232, 1236 (D. Nev. 1996) ("§ 2701(c)(1) allows service providers to do as they wish when it comes to accessing communications in electronic storage"); *Crowley v. Cybersource Corp.*, 166 F. Supp. 2d 1263, 1272 (N.D. Cal. 2001) ("Crowley's second argument in support of his unauthorized access claim, which is that Amazon had limited access to its own systems, strains credulity."). The law is thus clear that service providers may access e-mail stored on their own computer systems.

Moreover, in practice, service providers routinely screen the content of their users' e-mail. In particular, they check the content of stored e-mail for viruses, spam, and, increasingly, child pornography. For example, AOL, Yahoo, Microsoft, EarthLink and United Online are developing technology that will enable them to scan user images for child pornography; AOL "plans to check e-mail attachments that are already being scanned for viruses." Anick Jesdanun, *Internet Providers to Create Database to Combat Child Porn*, USA Today, June 27, 2006 (cited in R.16, Response in Opposition re Motion for TRO at 10; JA __) (available in Los Angeles Times on Westlaw at 2006 WLNR 11099699). *See also United States v. Zavakos*, No. 3:06-cr-03, 2006 WL 1697645 at *5 (S.D. Ohio June 19, 2006) (noting that child pornography investigation began when AOL provided a tip

that child pornography had been e-mailed by a particular subscriber). If Warshak's theory that service providers cannot access e-mail stored on their own servers were correct, then providers' attempts to limit child pornography, spam, fraud, and viruses would presumably be tortious or even criminal.

4. The Fourth Amendment Does Not Require Notice to the Target of an Investigation of Third-Party Compelled Disclosure.

The district court based its injunction in part on the fact that that SCA allows compelled production of e-mail without prior notice to the customer when such notice may have an adverse result, such as seriously jeopardizing an investigation. *See* (Order at 17-18; JA ___). However, the Supreme Court has explicitly held that the target of an investigation has no right to notice of third-party compelled disclosure. In *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984), the Supreme Court reversed a Ninth Circuit decision holding that targets of SEC investigations had a right to notice of third-party subpoenas. The Ninth Circuit had held that “[a]s a practical matter, unless the target of an SEC investigation receives notice of subpoenas served on third parties, no one will question compliance with the *Powell* standards [for administrative subpoenas] as to those questions.” *Jerry T. O'Brien, Inc. v. SEC*, 704 F.2d 1065, 1069 (9th Cir. 1983). The Supreme Court disagreed, holding that there was no basis, constitutional or otherwise, for requiring the target of an investigation to receive notice of subpoenas directed to

third parties. It explained that such a notice requirement “would substantially increase the ability of persons who have something to hide to impede legitimate investigations.” *Jerry T. O’Brien*, 467 U.S. at 750. The Court explicitly rejected the argument that the Fourth Amendment requires notice of a third-party subpoena to be given to the target of an investigation. *See id.* at 743.

Jerry T. O’Brien’s reasoning applies with equal or greater force to the 2703(d) orders in this case. The statutory rules of § 2703(b)(1)(B) and § 2705(a) require the government to provide an account holder with prior notice of a 2703(d) order unless the court determines that such notice would have an adverse effect, such as seriously jeopardizing an investigation. The SCA’s notice rules thus exceed the requirements of the Fourth Amendment, which under *Jerry T. O’Brien* does not require notice of third-party compelled disclosure. Therefore, there was no basis for the district court to order the government to provide investigatory targets with notice of 2703(d) orders.

D. The District Court Improperly Applied the Law in Balancing the Remaining Preliminary Injunction Factors.

1. Warshak Would Not Suffer Irreparable Harm Absent The Preliminary Injunction.

The United States respectfully submits that Warshak will not suffer immediate and irreparable harm if this Court vacates the preliminary injunction. Warshak claims that he faces an “irreparable violation” of his rights whenever the

Court grants a new 2703(d) order compelling disclosure of the content of his e-mail communications. (R.11, Memorandum in Support of Motion for TRO at 16; JA __). However, Warshak cannot carry his burden of showing that, absent immediate injunctive relief, he will suffer *immediate* irreparable harm for at least two reasons.

First, and as set forth in the Section I discussion regarding subject matter jurisdiction, Warshak has failed to establish that his e-mail communications currently are, or imminently will be, subject to disclosure pursuant to any 2703(d) orders. It is well-settled that an injunction “is unavailable absent a showing of irreparable injury, a requirement that cannot be met where there is no showing of any real or immediate threat that the plaintiff will be wronged again – a ‘likelihood of substantial and immediate irreparable injury.’” *Lyons*, 461 U.S. at 111 (citation omitted); *accord Abney v. Amgen, Inc.*, 443 F.3d 540 (6th Cir. 2006) (affirming denial of motion for preliminary injunction because plaintiffs could not show that irreparable harm would be “actual or imminent,” rather than “speculative or unsubstantiated”). Warshak speculates that the government could obtain such an order “in the future” simply because “the government has the *capability* of seeking additional orders pursuant to 18 U.S.C. § 2703(d).” (R.11, Memorandum in Support of Motion for TRO at 16; JA __ (emphasis added)). However, Warshak concedes that he is unaware of *any* pending 2703(d) orders that could allegedly

harm him, *see id.*, and the district court itself acknowledged that there is currently no “ripe, concrete context” in which to consider Warshak’s constitutional challenge. *See* (Order at 17; JA ___). Thus, “absent a sufficient likelihood that he will again be wronged in a similar way,” Warshak “is no more entitled to an injunction than any other citizen; and a federal court may not entertain a claim by any or all citizens who no more than assert that certain practices of law enforcement officers are unconstitutional.” *Lyons*, 461 U.S. at 111.

Second, Warshak has failed to establish, as he must, that there is no other adequate remedy at law to redress an unlawful 2703(d) order. To the extent Warshak can show that the government has willfully violated his rights under the SCA, the statute grants Warshak a right of action for monetary damages against the United States. 18 U.S.C. § 2712.

Furthermore, if the government were to seek to compel disclosure of Warshak’s e-mail pursuant to § 2703(b)(1)(B), it would be required to (1) obtain approval from a judicial officer before being permitted to serve a 2703(d) order and (2) give Warshak prior notice unless a court found that such notice may have an adverse result, such as seriously jeopardizing the investigation. *See* 18 U.S.C. § 2705(a). Now that the investigation of Warshak is public and he has been indicted on 107 counts of fraud, money laundering, and related charges, Warshak fails to

establish any reason to believe he would not be entitled to prior notice of any future 2703(d) orders compelling disclosure of the content of his e-mail.

Warshak will also likely have yet another opportunity to challenge the validity of the SCA in the parallel criminal action against him. Warshak has now been indicted on criminal counts arising out of a criminal investigation into the nationwide marketing, distribution, and sale of products by Berkeley. If the government intends to rely on the disclosures obtained by 2703(d) orders to convict Warshak, then he will have the opportunity to challenge the constitutionality of those orders before trial by filing a motion to suppress. Thus, Warshak has an adequate remedy to redress any alleged violation of his rights caused by a 2703(d) order. Accordingly, the United States respectfully submits that this Court vacate the preliminary injunction for the independent reason that Warshak will not suffer irreparable harm absent such relief.

2. The Preliminary Injunction Is Causing Substantial Harm to Others and Is Not Serving the Public Interest.

The preliminary injunction harms the criminal investigation process by requiring the government to give prior notice of 2703(d) orders, even in cases where such prior notice would jeopardize the investigation. Impairment of lawful criminal investigations harms the public interest. Moreover, the harm from this injunction is substantial: the district court did not limit the injunction to the parties before it. Instead, the injunction extends to any 2703(d) order for the content of e-

mail in the name of a resident of the Southern District of Ohio, regardless of the location of the criminal activity or the investigation.

Here, the government has an interest in the uniform and consistent application of the SCA, and the public interest lies in ensuring that law enforcement has the necessary tools created by the SCA to conduct criminal investigations. The preliminary injunction thwarts these interests by imposing a higher legal standard than Congress intended for compelled disclosure of e-mail. Congress authorized courts to compel disclosure of e-mail communications not in “electronic storage” or in “electronic storage” for greater than 180 days using a 2703(d) order or a subpoena. The SCA, a statute duly enacted by Congress, is entitled to deference and a presumption of validity. *See Rostker v. Goldberg*, 453 U.S. 57, 64 (1981). The preliminary injunction has upset the delicate balance Congress created between the public interests in privacy and in law enforcement.

Although Warshak may disagree with the choices Congress has made, that fact alone is insufficient to undermine the political process that led to the enactment of the SCA. Similarly, Warshak’s claim that he is vindicating his constitutional rights is belied by the fact that it is unlikely that any of his constitutional rights are implicated by the facts alleged in his complaint. *See Overstreet v. Lexington-Fayette Urban County Gov’t*, 305 F.3d 566, 579 (6th Cir. 2002) (affirming denial of motion for preliminary injunction where it is unlikely

that plaintiff can demonstrate that his constitutional rights are implicated); *cf. Steel Co.* 523 U.S. at 106 (stating that vindication of “the ‘undifferentiated public interest’ in faithful execution of [the law]” does not suffice to establish standing).

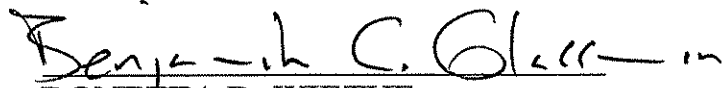
Accordingly, the government respectfully submits that vacating the preliminary injunction would not cause substantial harm to others and would serve the public interest.

CONCLUSION

For the foregoing reasons, the United States respectfully requests that the Court vacate the preliminary injunction in this case.

Respectfully submitted,

GREGORY G. LOCKHART
United States Attorney



DONETTA D. WIETHE
BENJAMIN C. GLASSMAN
Assistant United States Attorneys
221 East Fourth Street
Suite 400
Cincinnati, Ohio 45202
(513) 684-3711

JOHN H. ZACHARIA
NATHAN P. JUDISH
U.S. Department of Justice
1301 New York Ave., N.W.
Suite 600
Washington, D.C. 20005
(202) 305-2310

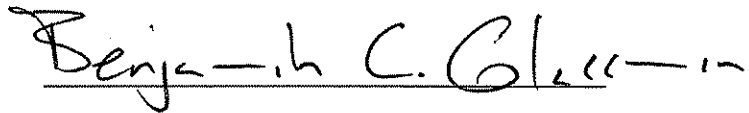
DESIGNATION OF JOINT APPENDIX CONTENTS

Pursuant to Rule 30(b) of the Rules of the Sixth Circuit, Defendant-Appellant United States of America hereby designates the following items for inclusion in the Joint Appendix:

<u>Item (date)</u>	<u>Record Number</u>
Docket Sheet	n/a
Complaint (6/12/2006)	1
Motion for Temporary Restraining Order (6/30/2006)	11
Response in Opposition re Motion for TRO (7/05/2006)	15
Order granting in part and denying in part Motion for TRO (7/21/06)	21
Transcript of Proceedings held on 7/05/06 (7/26/2006)	23
Plaintiffs' Opposition to Government's Motion to Stay Pending Appeal (8/21/2006)	30

CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing brief complies with the type-volume limitation provided in Rule 32(a)(7)(C)(i) of the Federal Rules of Appellate Procedure. The foregoing brief contains 13,017 words of Times New Roman (14 pt) proportional type. Microsoft Word is the word-processing software that I used to prepare this brief.

A handwritten signature in black ink that reads "Benjamin C. Glassman". The signature is written in a cursive style with a horizontal line underneath the name.

BENJAMIN C. GLASSMAN

CERTIFICATE OF SERVICE

I hereby certify that the foregoing Proof Brief for Defendant-Appellant United States of America was served this 11th day of October, 2006, by regular U.S. Mail upon the following attorneys for Plaintiff-Appellee Warshak:

Martin G. Weinberg, Esq.
20 Park Plaza, Suite 905
Boston, MA 02116

Martin S. Pinales, Esq.
105 W. 4th St., Suite 920
Cincinnati, OH 45202


BENJAMIN C. GLASSMAN

ADDENDUM OF UNPUBLISHED OPINION

Briefs and Other Related Documents

U.S. v. Zavakos S.D. Ohio, 2006. Only the Westlaw citation is currently available.

United States District Court, S.D. Ohio, Western Division.

UNITED STATES of America

v.

George ZAVAKOS.

No. 3:06-CR-003.

June 19, 2006.

Sheila Gay Lafferty, United States Attorney's Office, Dayton, OH, for United States of America.

**ENTRY AND ORDER OVERRULING
ZAVAKOS'S MOTION TO SUPPRESS (Doc. # 10)**

THOMAS M. ROSE, District Judge.

*1 Defendant George Zavakos ("Zavakos") is charged with one count of transportation of child pornography in violation of 18 U.S.C. § 2252(a)(1) and one count of possession of material constituting or containing child pornography in violation of 18 U.S.C. § 2252(a)(4)(B) and (b)(2). These charges stem, at least in part, from the search of a residence located at 5712 Marblehead Drive in Dayton, Ohio, and the search of a residence at 5133 Rosemont Boulevard in Dayton, Ohio.

Now before the Court is Zavakos's Motion To Suppress any evidence seized as a result of the search of the residence at 5712 Marblehead Drive. (Doc. # 10.) The residence at 5712 Marblehead Drive was searched using a warrant issued by Magistrate Judge Michael R. Merz on January 19, 2005. This Warrant was executed on January 24, 2005.

Based upon the search of the residence at 5712 Marblehead Drive and conversations there with Zavakos's mother, a warrant was obtained to search a residence at 1533 Rosemont Boulevard. The second Warrant was issued by Magistrate Judge Michael R. Merz on January 24, 2005, and was executed on that same day.

The Court conducted a hearing on Zavakos's Motion To Suppress on March 30, 2006, at which the Government presented the testimony of one witness,

FBI Special Agent Jeffrey L. Coburn ("SA Coburn"). Zavakos then attempted to file what appears to be a Memorandum In Support of his Motion To Suppress. However, this document was deleted by the Clerk's office. Zavakos's Counsel was instructed to resubmit the document, but he did not do so. Subsequently, the Government filed its response in opposition to Zavakos's Motion To Suppress. (Doc. # 14). The time has run and Zavakos has not filed a reply memorandum. Zavakos's Motion To Suppress is, therefore, ripe for decision. The law as it pertains to Zavakos's Motion To Suppress will first be set forth followed by an analysis of the Motion.

**THE RELEVANT LAW REGARDING
MOTIONS TO SUPPRESS**

The Fourth Amendment to the Constitution of the United States protects citizens from the unreasonable search of their property. The Fourth Amendment specifically provides that, "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." Groh v. Ramirez, 540 U.S. 551, 557 (2004). In addition, the officer executing the search warrant must ensure that the search is lawfully authorized and lawfully conducted. Id. at 563. Finally, the defendant has the burden of proving that a search is unconstitutional. United States v. Carter, Case No. 91-1509, 1992 WL 102506 at *2 (6th Cir. Apr. 29, 1992).

Probable Cause

Probable cause is defined as "reasonable grounds for belief, supported by less than prima facie proof but more than mere suspicion." United States v. Smith, 182 F.3d 473, 477 (6th Cir. 1999)(citing United States v. Bennett, 905 F.2d 931, 934 (6th Cir. 1990)). Probable cause exists "when there is a 'fair probability,' given the totality of the circumstances, that contraband or evidence of a crime will be found in a particular place." United States v. Helton, 314 F.3d 812, 819 (6th Cir. 2003)(quoting United States v. Davidson, 936 F.2d 856, 859 (6th Cir. 1991)).

*2 The Fourth Amendment requires only that the magistrate had a "substantial basis for ... concluding"

that a search warrant would uncover evidence of wrongdoing. United States v. Allen, 211 F.3d 970, 973 (6th Cir.2000), cert. denied, 531 U.S. 907 (2000). Therefore, a magistrate's findings regarding probable cause should not be set aside unless arbitrarily exercised. United States v. Weaver, 99 F.3d 1372, 1376 (6th Cir.1996)(citing United States v. Pelham, 801 F.2d 875, 877 (6th Cir.1986), cert. denied, 479 U.S. 1092 (1987)).

Affidavit Supporting Search Warrant

For a judge to be able to perform his or her official function regarding search warrants, the affidavit submitted as part of the request for the search warrant must contain adequate supporting facts about the underlying circumstances to show that probable cause exists for the issuance of the warrant. Smith, 182 F.3d at 477. Said another way, the affidavit must provide the magistrate with a substantial basis for determining the existence of probable cause. Helton, 314 F.3d at 819 (quoting Illinois v. Gates, 462 U.S. 213 (1983)).

A court may construe a warrant with reference to a supporting application or affidavit if the warrant uses appropriate words of incorporation and if the supporting document accompanies the warrant. Groh, 540 U.S. at 557-58. Zavakos does not challenge the fact that the Applications and Affidavits in this case are incorporated into the Warrants.

When reviewing the sufficiency of a supporting affidavit, a "totality of the circumstances" approach is used. Allen, 211 F.3d at 972 (citing Gates, 462 U.S. 213). Also, the review is limited to the "four corners" of the affidavit. United States v. Coffee, 434 F.3d 887, 892 (6th Cir.2006), cert. denied, 2006 WL 1079063 (2006).

The affidavit is to be interpreted in a commonsense and realistic manner without placing technical requirements of elaborate specificity on it. United States v. Hatfield, 599 F.2d 759, 761 (6th Cir.1979). Also, when reviewing the sufficiency of an affidavit, courts are to accord the judge's determination "great deference" and not engage in a de novo review. Allen, 211 F.3d at 972-73.

Finally, for probable cause considerations, "it is imperative that affidavits accurately reflect the facts of the particular situation at hand." Weaver, 99 F.3d at 1378. For example, statements by an affiant that are intentionally false or made with reckless

disregard for the truth must be stricken before the probable cause consideration. United States v. Cummins, 912 F.2d 98, 100 (6th Cir.1990).

Staleness

In addition to the accuracy requirement, the affidavit must present facts regarding a presently existing situation. Since probable cause to search is concerned with facts relating to a presently existing situation, a problem arises when probable cause which once existed has grown stale. United States v. Spikes, 158 F.3d 913, 923 (6th Cir.1998), cert. denied, 525 U.S. 1086 (1999). Said another way, probable cause "cannot be based upon stale information that no longer suggests that the item sought will be found in the place to be searched." United States v. Shomo, 786 F.2d 981, 983 (10th Cir.1986)(citing United States v. Haimowitz, 706 F.2d 1549, 1554-55 (11th Cir.1983), cert. denied, 464 U.S. 1069 (1984)).

*3 The standard of review for a determination of staleness is the same as the standard of review for determining the sufficiency of the affidavit. United States v. Greene, 250 F.3d 471, 480 (6th Cir.2001). Further, whether information contained in a affidavit is stale is determined on a case-by-case basis. Spikes, 158 F.3d at 923.

The question of staleness depends upon the nature of the crime and is not measured solely by counting the days between the events listed in the affidavit and the application for the warrant. *Id.* As a result, a number of factors may be considered to determine if the information contained in an affidavit is too stale to support a finding of probable cause. The factors are: (1) the character of the crime (chance encounter or regenerating conspiracy); (2) the criminal (nomadic or entrenched); (3) the thing to be seized (perishable and easily transferrable or of enduring utility to its holder); and (4) the place to be searched (criminal forum of convenience or secure operational base). Greene, 250 F.3d at 480-81. "As these variables demonstrate, even if a significant period has elapsed since a defendant's last reported criminal activity, it is still possible that, depending upon the nature of the crime, a magistrate may properly infer that evidence of wrongdoing is still to be found on the premises." Spikes, 157 F.3d at 923 (referring to United States v. Greany, 929 F.2d 523, 525 (9th Cir.1991)).

Evidence of ongoing criminal activity will generally defeat a claim of staleness. *Id.* at 481.

Further, “where the criminal activity occurred in a secure operational base, the passage of time becomes less significant.” Greene, 250 F.3d at 480-81. (citing Spikes, 158 F.3d at 923). For example, in the case of drug dealers, evidence is likely to be found in the place where the dealers live. United States v. Jones, 159 F.3d 969, 975 (6th Cir.1998), cert. denied, 126 S.Ct. 148 (2005). Also for example, images of pornography are “often stored on the user's hard drive for periods as long as eight or nine months.” United States v. Roby, 27 Fed.Appx. 779, 2001 WL 1381093 (9th Cir. Nov. 6, 2001). Finally, probable cause may be found where recent information corroborates otherwise stale information. Spikes, 158 F.3d at 924.

The Good-Faith Rule

The exclusionary rule which suppresses illegally obtained evidence does not apply where the evidence was discovered pursuant to a search warrant that was issued in good faith. Helton, 314 F.3d at 823. Accordingly, evidence should be suppressed based upon a lack of probable cause “only if the supporting affidavit was ‘so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable.’” United States v. Savoca, 761 F.2d 292, 296 (6th Cir.1985), cert. denied, 474 U.S. 852 (1985)(quoting United States v. Leon, 468 U.S. 897, 923 (1984)). This is termed the Good-Faith Rule and was first set forth in the case of United States v. Leon.

*4 There are four exceptions to the Good-Faith Rule. They are: (1) where the supporting affidavit contains information the affiant knew or should have known is false; (2) where the issuing magistrate lacked neutrality and detachment; (3) where the affidavit is devoid of information that would support a probable cause determination making any belief that probable cause exists completely unreasonable; or (4) where the warrant is facially deficient. Helton, 314 F.3d at 824.

For example, an affidavit that states suspicions, beliefs or conclusions to justify issuance of a search warrant without providing underlying factual circumstances regarding veracity, reliability and basis of knowledge is not entitled to the good-faith exception because a reasonably prudent officer would have sought greater corroboration. Weaver, 99 F.3d at 1378. Another example is a search warrant that contains sufficient recitation of facts so that it can be executed with an objectively reasonable good faith reliance on the probable cause determination is not invalid for being facially defective. United States v.

Smith, 63 F.3d 766, 769 (8th Cir.1995), cert. denied, 516 U.S. 1063 (1996). Having set forth the relevant law, Zavakos's Motion To Suppress is next analyzed.

ANALYSIS

Zavakos argues that any and all evidence seized during the execution of the two search warrants should be suppressed. He specifically argues that the facts used to support issuance of both warrants were stale and the information provided in support of the second Warrant was not specific enough to support a probable cause finding. Zavakos also argues that, based upon the alleged illegality of the searches, any statements that he might have made should also be suppressed.

Both Warrants were issued pursuant to Applications and Affidavits for Search Warrants presented to Magistrate Judge Merz by SA Coburn. Attached to and in support of each of the Applications was an Affidavit by SA Coburn.

The Affidavit submitted by SA Coburn for the search of 5712 Marblehead Drive, the first search, sets forth, and the supporting testimony confirms, the following information: On December 22, 2004, the Northeast Ohio Internet Crimes Against Children (NOICAC) Task Force sent a letter to the Dayton office of the Federal Bureau of Investigation (“FBI”). (1/19/05 Aff. ¶ 4.) The letter advised the FBI that America Online (“AOL”), an Internet service provider, had provided a tip that child pornography had been e-mailed via AOL from an individual in the Dayton area. (*Id.* ¶¶ 14, 17.) AOL reported that, on October 23, 2004, user Gzavakos@aol.com had e-mailed a file containing known child pornography. (*Id.* ¶¶ 16, 17.)

Pursuant to a subpoena, AOL revealed the subscriber information of “Gzavakos.” (*Id.* ¶ 16.) The results of the subpoena were compared to public records which revealed that G. Nicholas Zavakos currently lived at 5712 Marblehead Drive. (*Id.* ¶¶ 17, 19.) Also revealed was that G. Nicholas Zavakos uses the screen name “gzavakos,” among others. (*Id.*) On January 11, 2005, Task Force Officer Steven O. Maynard confirmed that Zavakos was receiving mail at 5712 Marblehead Drive. (*Id.* ¶ 20.)

*5 The Affidavit describes the characteristics of individuals who buy, produce, trade or sell child pornography. (*Id.* ¶ 4.) These individuals collect child pornography in the form of photographs,

magazines, motion pictures, videotapes, books and slides and they rarely, if ever, dispose of this material. (*Id.*) Also, these individuals often collect, read, copy or maintain names, addresses, phone numbers or lists of others who have similar interests regarding child pornography. (*Id.*)

The Affidavit further indicates that an individual interested in child pornography and familiar with a computer will use the computer in some private location to interact with other individuals to traffic in, trade or collect child pornography. (*Id.*) Also, a suspect may try to conceal child pornography in various ways on computer storage devices. (*Id.*)

The Affidavit presenting these facts to Magistrate Judge Merz is dated January 19, 2005. The first Warrant was issued on that same day and was executed on January 24, 2005.

The information provided to the Magistrate Judge to obtain the Warrant to search 1533 Rosemont Boulevard, the second search, was in the Affidavit of SA Coburn that was part of the application for the second Warrant. The Affidavit that was part of the application for the second Warrant included all of the information that was in the Affidavit that was part of the application for the first Warrant plus additional information obtained as a result of the execution of the first Warrant.

As a result of executing the first Warrant, SA Coburn wanted to search the residence at 1533 Rosemont Boulevard. Following is a summary of the additional information contained in the Affidavit presented to obtain the Warrant to search 1533 Rosemont Boulevard, the second Warrant. This second Affidavit indicates that the Warrant to search the 5712 Marblehead Drive residence was executed on January 24, 2005. (1/24/05 Aff. ¶ 19.) During this search, Linda Gray was present and stated that Zavakos is her son and that he uses her personal computer located at 5712 Marblehead Drive. (*Id.*) She also stated that Zavakos currently resides at 1533 Rosemont Boulevard and that he owns and uses a personal computer located at that address. (*Id.* ¶ 20.)

The Affidavit presenting these facts to Magistrate Judge Merz is dated January 24, 2005. The second Warrant was issued and executed on that same day.

Staleness of First Search Warrant

Zavakos argues that facts used to support the first

Warrant to search the premises at 5712 Marblehead Drive were stale. Each of the factors used to determine if the information used in the Affidavit supporting issuance of the first Warrant was stale will next be addressed.

Character of the Crime

The key consideration regarding the character of the crime is whether it was a chance encounter or an ongoing activity. In this case, the character of the crime is child pornography. The Affidavit indicates that a computer file containing child pornography was emailed by a user suspected to be Zavakos. The Affidavit also indicates that those who engage in child pornography collect it and rarely ever dispose of it. Therefore, there was reason to expect ongoing activity regarding child pornography.

Criminal Nomadic or Entrenched

*6 The key consideration regarding the criminal is whether he or she is moving about or can be expected to return to the same location. In this case, public records showed that Zavakos lived at 5712 Marblehead Drive and further investigation revealed that, as of a few days before the warrant was issued, Zavakos was receiving mail at 5712 Marblehead Drive. Therefore, there was reason to believe that Zavakos was not moving about and could be expected to return to 5712 Marblehead Drive.

The Thing To Be Seized

Key considerations regarding the thing to be seized are whether it is perishable and easily transferable or of enduring utility to its holder. In this case, the things to be seized were computers and computer storage devices containing child pornography and allegedly used by Zavakos. A computer and information stored on a computer is generally of enduring utility to its holder. Also, the Affidavit indicates that, in cases where individuals trade in child pornography, they generally collect and store it and they, many times, use computers to do so. Therefore, Zavakos could reasonably have been collecting and storing child pornography on his computer and his computer could reasonably have enduring utility to him for purposes of collecting and/or trading child pornography.

The Place To Be Searched

The key issue regarding the place to be searched is whether it is a mere criminal forum of convenience or a secure operational base. In this case, the place to be searched was the residence at 5712 Marblehead Drive. Public records indicated that Zavakos was known to reside there and he was receiving mail there. As a result, Zavakos could reasonably have been using 5712 Marblehead Drive as a secure operational base.

Conclusion

Under the totality of the circumstances presented in the first Affidavit, the Magistrate Judge could reasonably conclude that the information in the first Affidavit was not stale. Even though the child pornography was e-mailed on October 23, 2004, and the first Warrant was not issued until January 19, 2005, the Affidavit indicates that criminal activity most probably occurred in a secure operational base, making the passage of time less significant. Also, the nature of the alleged crime is such that evidence of it could be expected to be stored for some period of time at the secure operational base.

Probable Cause for Second Search Warrant

Zavakos argues that the information provided to search 1533 Rosemont Boulevard was not specific enough to support a probable cause finding. The information provided to the Magistrate Judge was that Zavakos had transmitted known child pornography in an e-mail, that the public records indicated that Zavakos resided at 5712 Marblehead Drive, that Zavakos was receiving personal mail at 5712 Marblehead Drive, that 5712 Marblehead Drive had been searched, that Zavakos's mother had informed the agents that Zavakos may have used her computer at 5712 Marblehead Drive, that Zavakos now resided at 1533 Rosemont Boulevard and that Zavakos owns and uses a personal computer located at that address.

*7 Zavakos does not challenge any of the specific facts presented in the second Affidavit. Given the totality of the circumstances presented in the second Affidavit, including detail provided about child pornographers and the use of computers, the Magistrate Judge had a substantial basis for concluding that there was probable cause to search the residence at 1533 Rosemont Boulevard.

Staleness of Second Search Warrant

Zavakos argues that the facts used to support the second Warrant to search the premises at 1533 Rosemont Boulevard were stale. Therefore, each of the factors used to determine if the information used in the affidavit supporting issuance of the second Warrant was stale will next be addressed.

Character of the Crime

As with the first Affidavit to obtain the warrant to search 5712 Marblehead Drive, the character of the crime in the second Affidavit to search 1533 Rosemont Boulevard is child pornography. The second Affidavit indicates that a computer file containing child pornography was e-mailed by a user suspected to be Zavakos. The second Affidavit also indicates that those who engage in child pornography collect it and rarely ever dispose of it. Finally, the second Affidavit indicates that Zavakos now resides at 1533 Rosemont Boulevard. Therefore, there was reason to expect ongoing activity regarding child pornography at Rosemont Boulevard.

Criminal Nomadic or Entrenched

The second Affidavit indicates that Zavakos's mother said that he now resides at 1533 Rosemont Boulevard and this statement was made on the same day that the second Warrant was issued. Therefore, there was reason to believe that Zavakos was not moving about and could be expected to return to 1533 Marblehead Drive.

The Thing To Be Seized

As with the first Affidavit, the second Affidavit indicates that the things to be seized were computers and computer storage devices containing child pornography and used by Zavakos. A computer and information stored on a computer is generally of enduring utility to its holder. Also, the second Affidavit indicates that, in cases where individuals trade in child pornography, they generally collect and store it and they, many times, use computers to do so. Finally, Zavakos's mother indicated that he owned and used a personal computer located at 1533 Rosemont Boulevard. Therefore, Zavakos could reasonably have been collecting and storing child

pornography on his computer at 1533 Rosemont Boulevard and his computer could reasonably have enduring utility to him for purposes of collecting and/or trading child pornography.

The Place To Be Searched

In the case of the second Warrant, the place to be searched was 1533 Rosemont Boulevard. This was the location where Zavakos's mother said he was residing and where he owned and used a personal computer. As a result, Zavakos could reasonably have been using 1533 Rosemont Boulevard as a secure operational base.

Conclusion

Under the totality of the circumstances, the Magistrate Judge could reasonably conclude that the information in the second Affidavit presented to obtain the second Warrant was not stale. Even though the alleged child pornography was e-mailed on October 23, 2004, and the second Warrant was not issued until January 24, 2005, the second Affidavit indicates that criminal activity most probably occurred in a secure operational base, making the passage of time less significant. Also, the nature of the alleged crime is that evidence of it could be expected to be stored at the secure operational base at 1533 Rosemont Boulevard.

SUMMARY

*8 The information contained in the Affidavit presented to obtain the first Warrant was not stale. Also, the information contained in the Affidavit presented to obtain the second Warrant was not stale and the Magistrate Judge had probable cause to issue the second Warrant. Therefore, the first Branch of Zavakos's Motion To Suppress is OVERRULED.

SA Coburn testified that no statements were given by Zavakos at the time of the searches. Therefore, the second, and final, Branch of Zavakos's Motion To Suppress is not well founded and is also OVERRULED.

Finally, the Government argues that, even if either or both of the Warrants were somehow deficient, it is entitled to the good-faith exception. However, since neither of the Warrants was defective, the Court need not address this argument.

DONE and ORDERED in Dayton, Ohio on this Nineteenth day of June, 2006.

S.D. Ohio, 2006.
U.S. v. Zavakos
Slip Copy, 2006 WL 1697645 (S.D. Ohio)

Briefs and Other Related Documents ([Back to top](#))

• [3:06cr00003](#) (Docket) (Jan. 10, 2006)

END OF DOCUMENT