

No. 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 OF PLAINTIFF-APPELLEE STEVEN WARSHAK

MARTIN S. PINALES
SIRKIN, PINALES & SCHWARTZ LLP
105 West Fourth Street, Suite 920
Cincinnati, Ohio 45202
(513) 721-4876

MARTIN G. WEINBERG
20 Park Plaza, Suite 905
Boston, Massachusetts 02116
(617) 227-3700

TABLE OF CONTENTS

STATEMENT OF SUBJECT MATTER JURISDICTION	1
STATEMENT OF THE CASE/STATEMENT OF FACTS	1
SUMMARY OF ARGUMENT	6
I. THE DISTRICT COURT HAS SUBJECT MATTER JURISDICTION OF THIS ACTION	11
A. Warshak Has Standing To Seek Injunctive Relief	11
1. The applicable standard	11
2. Injury-in-fact	12
3. Redressability	21
B. Warshak's Claims Are Ripe For Adjudication	22
II. THE PRELIMINARY INJUNCTION CONSTITUTES A PROPER EXERCISE OF THE DISTRICT COURT'S DISCRETION	26
A. Standard of Review	26
B. The District Court Applied The Proper Legal Standards ...	27
1. Emails are "closed containers" which may not be searched without a warrant	29
2. The government's effort to substitute the standards applicable to subpoenas for the protections of the warrant clause should be rejected	31

3.	Generalities regarding the grand jury’s right to everyman’s evidence do not trump the requirements of the Fourth Amendment	37
4.	The cases regarding third-party subpoenas on which the government relies do not undermine the validity of the preliminary injunction	38
5.	The statutory framework and “industry practice” are irrelevant to the validity of the preliminary injunction	41
6.	The district court did not invalidate §2703 solely because of the absence of notice	43
C.	Judge Dlott Properly Concluded That The SCA Is Facially Unconstitutional To The Extent That It Permits Ex Parte Seizure of Email Content Without a Showing of Probable Cause	45
1.	The applicable standard	45
2.	The government has failed to demonstrate that there is any circumstance under which the use of §2703(d) orders to seize and search the content of ISP-stored emails, without a showing of probable cause and without notice to the account holder, would not violate the Fourth Amendment	46
D.	The District Court Properly Applied The Remaining Factors Governing Whether a Preliminary Injunction Should Enter	52
1.	Irreparable injury to Warshak	52
2.	Lack of substantial injury to the government	54
3.	The public interest	55

CONCLUSION	56
DESIGNATION OF JOINT APPENDIX CONTENTS	58
CERTIFICATE OF COMPLIANCE	59
CERTIFICATE OF SERVICE	60

TABLE OF AUTHORITIES

Cases

<i>Abbott Laboratories v. Gardner</i> , 387 U.S. 136 (1967)	22
<i>Abney v. Amgen, Inc.</i> , 443 F.3d 540 (6th Cir. 2006)	52
<i>Adarand Constructors, Inc. v. Slater</i> , 528 U.S. 216 (2000)	19
<i>Adult Video Ass'n v. Department of Justice</i> , 71 F.3d 563 (6th Cir. 1995).	24
<i>Almeida-Sanchez v. United States</i> , 413 U.S. 266 (1973)	54
<i>Babbitt v. United Farm Workers Nat'l Union</i> , 442 U.S. 289 (1979)	11, 14
<i>Baker v. Carr</i> , 369 U.S. 186 (1962)	17
<i>Baranski v. Fifteen Unknown Agents</i> , 452 F.3d 433 (6th Cir. 2006), petition for cert. filed, September 29, 2006 (No. 06-612)	37
<i>Bennett v. Spear</i> , 520 U.S. 154 (1997)	11, 12
<i>Blum v. Yaretsky</i> , 457 U.S. 991 (1982)	17, 18
<i>Branzburg v. Hayes</i> , 408 U.S. 665 (1972)	37
<i>Bristol-Myers Squibb Co. v. Shalala</i> , 91 F.3d 1493 (D.C.Cir. 1996)	11
<i>City of Chicago v. Morales</i> , 527 U.S. 41 (1999)	45
<i>City of Los Angeles v. Lyons</i> , 461 U.S. 95 (1983)	13, 15
<i>Cleveland Branch, NAACP v. City of Parma</i> , 263 F.3d 513 (6th Cir. 2001), cert. denied, 535 U.S. 971 (2002)	11

<i>Cleveland Nat. Air Show, Inc. v. Department of Transportation</i> , 430 F.3d 757 (6th Cir. 2005)	19
<i>Coleman v. DeWitt</i> , 282 F.3d 908 (6th Cir.), <i>cert. denied</i> , 536 U.S. 914 (2002)	45
<i>Dixie Fuel Co. v. Commissioner of Social Security</i> , 171 F.3d 1052 (6th Cir. 1999)	25
<i>Doe v. Broderick</i> , 225 F.3d 440 (4th Cir. 2000)	41
<i>Donovan v. Lone Steer, Inc.</i> , 464 U.S. 408 (1984)	33
<i>Ex Parte Jackson</i> , 96 U.S. 727 (1878)	29
<i>Freedman v. America Online, Inc.</i> , 325 F.Supp.2d 638 (E.D.Va. 2000) .	51
<i>Friends of the Earth, Inc. v. Laidlaw Environmental Services</i> , 528 U.S. 167, 189 (2000)	19, 21
<i>Groh v. Ramirez</i> , 540 U.S. 551 (2004)	37
<i>Guest v. Leis</i> , 255 F.3d 325 (6th Cir. 2001)	48
<i>Hays v. City of Urbana</i> , 104 F.3d 102 (7th Cir.), <i>cert. denied</i> , 520 U.S. 1265 (1997)	48
<i>Honig v. Doe</i> , 484 U.S. 305 (1988)	19
<i>Horton v. California</i> , 496 U.S. 128 (1990)	29
<i>In re Administrative Subpoena (Doe)</i> , 253 F.3d 256 (6th Cir. 2001) . . .	33, 34, 35
<i>In re Search of The Rayburn House Office Building Room</i> <i>Number 2113</i> , 432 F.Supp.2d 100 (D.D.C. 2006)	37
<i>In re Subpoena Duces Tecum</i> , 228 F.3d 341 (4th Cir. 2000)	34

<i>Kardules v. City of Columbus</i> , 95 F.3d 1335 (6th Cir. 1996)	23
<i>Katz v. United States</i> , 389 U.S. 347 (1967)	29
<i>Kelley v. Selin</i> , 42 F.3d 1501 (6th Cir.), cert. denied, 515 U.S. 1159 (1995)	11
<i>Lehn v. Holmes</i> , 364 F.3d 862 (7th Cir. 2004)	24
<i>Linton v. Commissioner of Health & Environment</i> , 30 F.3d 55 (6th Cir. 1994)	19
<i>LSO, Ltd. v. Stroh</i> , 205 F.3d 1146 (9th Cir. 2000)	13, 14
<i>Lujan v. Defenders of Wildlife</i> , 504 U.S. 555 (1992)	11, 14, 18
<i>Lynch v. Leis</i> , 382 F.3d 642 (6th Cir. 2004), cert. denied, 544 U.S. 949 (2005)	11
<i>Mascio v. Pub. Employees Ret. Sys. of Ohio</i> , 160 F.3d 310 (6th Cir.1998)	26
<i>Moltan Co. v. Eagle-Picher Indus., Inc.</i> , 55 F.3d 1171 (6th Cir.1995) ..	26
<i>Newfield v. Ryan</i> , 91 F.2d 700 (5th Cir.), cert. denied, 302 U.S. 729 (1937)	39, 40
<i>Ohio Forestry Ass'n v. Sierra Club</i> , 523 U.S. 726 (1998)	23, 25
<i>Oklahoma Press Publishing Co. v. Walling</i> , 327 U.S. 186 (1946)	33, 35
<i>O'Shea v. Littleton</i> , 414 U.S. 488 (1974)	13, 15
<i>Pennell v. City of San Jose</i> , 485 U.S. 1 (1988)	11
<i>People's Rights Org. v. City of Columbus</i> , 152 F.3d 522 (6th Cir. 1998)	22

<i>Pfizer, Inc. v. Shalala</i> , 182 F.3d 975 (D.C.Cir. 1999)	23
<i>Press-Enterprise Co. v. Superior Court</i> , 478 U.S. 1 (1986)	19
<i>Renne v. Geary</i> , 501 U.S. 312 (1991)	23
<i>Schwimmer v. United States</i> , 232 F.2d 855 (8th Cir.), cert. denied, 352 U.S. 833 (1956)	39
<i>SEC v. Jerry T. O'Brien, Inc.</i> , 467 U.S. 735 (1984)	43, 44
<i>Steel Co. v. Citizens for a Better Environment</i> , 523 U.S. 83 (1998)	21
<i>Sullivan v. Syracuse Housing Authority</i> , 962 F.2d 1101 (2d Cir. 1992) .	12
<i>Texas v. United States</i> , 523 U.S. 296 (1998)	24
<i>Theofel v. Farey-Jones</i> , 359 F.3d 1066 (9th Cir.), cert. denied, 543 U.S. 813 (2004)	2, 51
<i>Thomas v. Union Carbide Agricultural Products Co.</i> , 473 U.S. 568 (1985)	22
<i>United States v. Allen</i> , 106 F.3d 695 (6th Cir.), cert. denied, 520 U.S. 1281 (1997)	49
<i>United States v. Bach</i> , 310 F.3d 1063 (8th Cir. 2002), cert. denied, 538 U.S. 993 (2003)	52
<i>United States v. Barr</i> , 605 F.Supp. 114 (S.D.N.Y. 1985)	32
<i>United States v. Bautista</i> , 362 F.3d 584 (9th Cir. 2004)	50
<i>United States v. Caymen</i> , 404 F.3d 1196 (9th Cir. 2005)	49, 50
<i>United States v. Chadwick</i> , 433 U.S. 1 (1977)	30

<i>United States v. Colorado Supreme Court</i> , 87 F.3d 1161 (10th Cir. 1996)	11, 17
<i>United States v. Cunag</i> , 386 F.3d 888 (9th Cir. 2004)	50
<i>United States v. Dionisio</i> , 410 U.S. 1 (1973)	34, 35
<i>United States v. Edward Rose & Sons</i> , 384 F.3d 258 (6th Cir. 2004) ..	26
<i>United States v. Fell</i> , 360 F.3d 135 (2d Cir.), <i>cert. denied</i> , 543 U.S. 946 (2004)	24
<i>United States v. Frandsen</i> , 212 F.3d 1231 (11th Cir. 2000)	45
<i>United States v. Fultz</i> , 146 F.3d 1102 (9th Cir. 1998)	49
<i>United States v. Jacobsen</i> , 466 U.S. 109 (1982)	30
<i>United States v. Loy</i> , 237 F.3d 251(3d Cir. 2001)	24
<i>United States v. Miller</i> , 425 U.S. 435 (1976)	51
<i>United States v. Oswald</i> , 783 F.2d 663 (6th Cir. 1986)	49
<i>United States v. Palmer</i> , 536 F.2d 1278 (9th Cir. 1976)	40
<i>United States v. Phibbs</i> , 999 F.2d 1053 (6th Cir. 1993), <i>cert. denied</i> , 510 U.S. 1119 (1994)	38, 39
<i>United States v. Quinones</i> , 313 F.3d 49 (2d Cir. 2002), <i>cert. denied</i> , 540 U.S. 1051 (2003)	24, 45
<i>United States v. Robinson</i> , 390 F.3d 853 (6th Cir. 2004)	49
<i>United States v. Ross</i> , 456 U.S. 798 (1982)	29
<i>United States v. Salerno</i> , 481 U.S. 739 (1987)	45

<i>United States v. Sturm, Ruger & Co., Inc.</i> , 84 F.3d 1 (1st Cir.), <i>cert. denied</i> , 519 U.S. 991 (1996)	33
<i>United States v. Triumph Capital Group</i> , 211 F.R.D. 31 (D.Conn.2002) .	32
<i>United States v. Upham</i> , 168 F.3d 532 (1st Cir.), <i>cert. denied</i> , 527 U.S. 1011 (1999)	36
<i>United States v. Van Leeuwen</i> , 397 U.S. 249 (1970)	30
<i>United States v. White</i> , 244 F.3d 1199 (10th Cir. 2001)	24
<i>Warth v. Seldin</i> , 422 U.S. 490 (1975)	11, 17, 21
<i>Whitmore v. Arkansas</i> , 495 U.S. 149 (1990)	14
<i>Wilson v. Moreau</i> , 440 F.Supp.2d 81 (D.R.I. 2006)	32

Constitutional Provisions

Article III, United States Constitution	14
Fourth Amendment, United States Constitution	<i>passim</i>

Statutory Provisisons

18 U.S.C. §2703	<i>passim</i>
18 U.S.C. §2703(b)	21
18 U.S.C. §2703(b)(1)(B)(ii)	6, 44
18 U.S.C. §2703(d)	<i>passim</i>
18 U.S.C. §2703(f)	16, 54
18 U.S.C. §2705	2, 6, 7, 44

18 U.S.C. §2705(a)(4) 2

STATEMENT REQUESTING ORAL ARGUMENT

Because this case presents complex issues of first impression regarding the constitutionality of the Stored Communications Act, appellee believes that oral argument will be of material aid to the Court in its decisional process. Appellee therefore requests oral argument.

STATEMENT OF SUBJECT MATTER JURISDICTION

The district court has subject matter jurisdiction of this case pursuant to 28 U.S.C. §1331. *See* Section I, *infra*.

STATEMENT OF THE CASE/ STATEMENT OF FACTS

This action arose from the government's secret utilization of 18 U.S.C. §2703(d) orders to seize and search thousands upon thousands of plaintiff Steven Warshak's private emails, without probable cause, without particularization as to subject matter or time frame, and without notice to him until long after the fact. In May, 2006, Warshak's counsel, having learned of the government's use of §2703(d) orders to seize the content of Warshak's emails, communicated to the government his contention that, under the Fourth Amendment, emails could not be seized and searched without probable cause; in response, the government declined to provide any assurance that it would not again secretly utilize §2703(d) to obtain access to the content of Warshak's emails. R1, Complaint, JA ___ - ___.

Following this exchange, on May 31, 2006, the government provided Warshak with the long-improperly-delayed statutory notice that the government had obtained a §2703(d) order directed to NuVox Communications on May 6, 2005, more than a year earlier, and a §2703(d) order directed to Yahoo! on September 12, 2005, more

than eight months earlier.¹ Those orders, which demanded compliance within three days, mandated the production of account information and “[t]he contents of wire or electronic communications (not in electronic storage unless greater than 181 days old) that were placed or stored in directories or files owned or controlled by the [identified] accounts . . . at any time during the hosting of the electronic communications and through the date of this Order.” R1, Complaint, JA _____. The attachment to the order – drafted by the government – told the ISPs that “[c]ommunications not in ‘electronic storage’ include any email communications received by the specified accounts that the owner or user of the account has already accessed, viewed, or downloaded.” *Id.*, JA _____.² NuVox followed that directive and

¹ Section 2703 subpoenas and orders may not be utilized without advance notice to the subscriber unless the government satisfies the requirements of §2705. Here, instead of complying with the requirement of §2705(a)(4) that it reapply every 90 days if it wished to delay notice beyond the initial 90-day period of delay authorized, the government obtained from the magistrate judge who issued the orders an open-ended sealing order. *See* R21, Order Granting in Part and Denying in Part Plaintiff Steven Warshak’s Motion for TRO and/or Preliminary Injunction and Entering Preliminary Injunction (“Order”), JA ____; *see also* R36, Memorandum in Opposition to Plaintiff’s Motion to Unseal Pertinent Case Files, JA _____.

² Contrary to the suggestion of the government, Proof Brief for Defendant-Appellant United States of America (“USB”) 6, opened emails, draft emails, and copies of sent emails less than 181 days old *do* fall within the scope of “electronic storage” and may, therefore, be obtained by the government only through the issuance and execution of a search warrant. *See Theofel v. Farey-Jones*, 359 F.3d 1066, 1077 (9th Cir. 2004). The proper construction of “electronic storage” is not, however,

turned over to the government many emails which were less than 181 days old. *Id.*, JA____. Yahoo!, however, recognizing that emails less than 181 days old were obtainable only with a search warrant, supplied the government only with emails more than 180 days old. *Id.*, JA____.

Warshak's Complaint was filed on June 12, 2006. Shortly thereafter, Warshak sought assurance from the government that it would not, at least for some discrete period of time pending litigation of Warshak's claims, seek any additional §2703(d) orders directed at Warshak's emails. In response, the government informed Warshak's counsel that it would not agree to forego seeking §2703(d) orders in relation to the investigation of Warshak. *See* R16, Warshak's Post-Argument Reply to Government Opposition to Motion for Issuance of a Temporary Restraining Order and/or Preliminary Injunction, JA____. In light of the government's position, Warshak filed on June 30, 2006, his Motion for Issuance of a Temporary Restraining Order and/or Preliminary Injunction ("Preliminary Injunction Motion"). R11, JA____. During the July 5, 2006, hearing on Warshak's motion, the government, in response to Judge Dlott's questioning, reiterated its refusal to agree that no new §2703(d) orders would be forthcoming. R23, 7/5/06 Transcript, JA____.³

before the Court in this appeal.

³

The government criticizes Warshak for not offering evidence at this hearing,

In ruling favorably on Warshak's request for a preliminary injunction, Judge Dlott first correctly stated the factors which courts are to consider in determining whether to issue a preliminary injunction, R21, Order, JA ___ - ___, and then proceeded to correctly apply them, turning first to Warshak's likelihood of success on the merits. She explained at some length Warshak's contention that ISP-stored emails are analogous to closed containers such as letters and packages which the Supreme Court has long held cannot be searched without a warrant issued upon a showing of probable cause, contrasting it with the government's contention that emails should be regarded as more in the nature of postcards because their contents can be accessed by the ISPs on which they are stored. *Id.*, JA ___ - ___. On the record before her, Judge Dlott said, it was not "reasonable to assume that once personal emails are stored on a commercial ISP's server, whatever expectation of privacy the account subscriber may have had in those emails has 'already been frustrated.'" *Id.*, JA ___. Judge Dlott, while recognizing that there were distinctions between emails and both sealed letters and postcards, found the letter analogy, based on the evidence then before her, "to be more apt." *Id.*, JA ___. Consequently, she concluded, Warshak had "shown a substantial likelihood of success on the merits of his Fourth

USB11, but neglects to mention that this was a *telephonic* hearing scheduled solely for the purpose of hearing the arguments of counsel.

Amendment claim.” *Id.*, JA ____.⁴

As to the second factor, Judge Dlott found that Warshak would be irreparably injured in the absence of a preliminary injunction. The government’s two prior warrantless §2703(d) seizures of Warshak’s emails and its “refus[al] to pledge not to obtain or enforce future 2703(d) orders . . . against other email accounts of Warshak’s” rendered “the prospective harm in this case . . . far from ‘speculative’ or ‘unsubstantiated’” *Id.*, JA ____.

As to the third factor, Judge Dlott rejected the government’s arguments that enjoining *ex parte* use of §2703(d) orders would impede its law enforcement efforts because “[s]uch considerations . . . cannot presumptively trump the grave constitutional concerns presented by Warshak’s complaint and motion.” *Id.*, JA ____.

The fourth factor also weighed in favor of injunctive relief, Judge Dlott concluded, because “it is always in the public interest to prevent violation of a party’s constitutional rights.” *Id.*, JA ____.

4

Because she rightly regarded the unconstitutionality of the SCA as a facial defect, Judge Dlott did not address Warshak’s as-applied challenge. The reason for this was not, however, as the government asserts, because Warshak presented insufficient evidence that he continued to maintain an email account. *See* USB30 n.4. An assertion that Warshak continued to maintain ISP email accounts is inherent in his claims for prospective injunctive relief, and it was not genuinely disputed below that Warshak continued to maintain email accounts potentially subject to future §2703 process, *see generally* R23, 7/5/06 Transcript, JA ____ - ____, as the government well knew that he did.

Based on the record before her, Judge Dlott was “provisionally persuaded that th[e] standard of proof less than probable cause and potentially broad *ex parte* authorization cannot stand.” *Id.*, JA _____. Accordingly, Judge Dlott preliminarily held that §§2703(b)(1)(B)(ii), 2703(d), and 2705 violate the Fourth Amendment “to the extent that they collectively authorize the *ex parte* issuance of search and seizure orders without a warrant and on less than a showing of probable cause.” *Id.*, JA _____.⁵ She therefore entered the preliminary injunction which is the subject of this appeal.

SUMMARY OF ARGUMENT

Utilizing *ex parte* orders issued under 18 U.S.C. §2703, the government obtained thousands upon thousands of Warshak’s personal and private email communications, which it proceeded over the next year and more to search at will, depriving Warshak of notice of its actions long beyond the period of delay permitted

5

That this was the first time any court had held the SCA unconstitutional, *see* USB3, 5, is not surprising in light of the fact that no reported decision has squarely addressed the Fourth Amendment implications of the Department of Justice’s policy of seizing the content of emails based on its own – rather than Congress’ – definition of “electronic storage.” In holding the SCA unconstitutional, Judge Dlott did not “ignor[e] the principle ‘that courts avoid reaching constitutional questions in advance of the necessity of deciding them.’” USB11. That principle is wholly inapplicable here: Judge Dlott was confronted with a constitutional challenge to the SCA, there were no nonconstitutional grounds on which the case could have been decided which would have afforded Warshak the relief requested, and decision of the constitutional issue was, therefore, essential to the determination of the issue before her.

under the procedures prescribed in §2705. This massive and secret invasion of personal privacy, against which Warshak was powerless to protect himself, was conducted without a warrant predicated upon a showing of probable cause and without the particularization of the communications to be seized required by the Fourth Amendment. Instead of the protections of the Fourth Amendment, the government contends that the applicable standards are those governing administrative and grand jury subpoenas. Contrary to the government's view, however, there *are* things which the government *cannot* obtain and search through the simple expedient of serving a subpoena. Closed containers, such as sealed letters and packages, are among them, and emails are the equivalent of closed containers, which the Supreme Court has long held cannot be searched without a warrant. The government's arguments largely beg the question whether the Fourth Amendment requires a warrant based on probable cause before the government may seize and search emails in electronic storage. Moreover, the administrative/grand jury subpoena context supplies protections which are lacking in the context of *ex parte* §2703 orders: an opportunity to contest production of the subpoenaed documents or materials *in advance* of their production to the government and the requirement that the subpoenaed material be relevant to the investigation. The §2703 order is far more closely akin to a warrant than it is to an administrative/grand jury subpoena, thus requiring such protections

as particularization and probable cause which were wholly lacking in the procedures enjoined by Judge Dlott.

The government asks this Court to ignore the critically important constitutional issues at stake in this case by finding that Warshak lacks standing. Contrary to the government's argument, however, Warshak has alleged the necessary past, present, and threatened future injury to confer upon him standing to seek injunctive relief and to support the entry of the preliminary injunction, as Judge Dlott supportably found. Moreover, those injuries are certainly redressable by the courts, through declaratory and injunctive relief to prevent additional violations of Warshak's Fourth Amendment rights. Finally, Warshak's claims are clearly ripe for adjudication: they are neither abstract nor premature, no further extra-judicial factual developments are necessary to place the district court in a position to determine the facial constitutionality of §2703, and delaying consideration of Warshak's claims would visit substantial hardship on Warshak.

The "no constitutional application" standard on which the government relies in attacking Judge Dlott's facial invalidation of the SCA is not the standard applicable to Warshak's facial challenge to the validity of §2703. Furthermore, none of the examples offered by the government of circumstances under which it contends that warrantless *ex parte* seizures and searches of emails would not violate the Fourth

Amendment undermines the validity of the preliminary injunction. Judge Dlott properly concluded that an individual does not surrender his reasonable expectation of privacy in his personal emails by allowing them to be stored in his ISP subscriber account. The preliminary injunction creates a mechanism through which Fourth Amendment violations can be prevented in advance of their occurrence. Judge Dlott in no way abused her discretion in ruling that Warshak has a substantial likelihood of success on the merits.

Judge Dlott correctly assessed the remaining factors bearing on the issuance of a preliminary injunction as well. She rightly concluded, in light of the government's prior use of §2703 orders directed at Warshak's email accounts and the fact that it refused to agree that it would not again use §2703 process to seize Warshak's emails pending litigation of Warshak's claims, that Warshak would be irreparably injured in the absence of a preliminary injunction. Nor does Warshak have an adequate remedy at law against future violations of his Fourth Amendment rights. Even suppression would not remedy the vast intrusion on personal privacy resulting from the secret implementation of §2703(d) orders which contain no temporal or subject matter limitations on what the ISP is required to produce. The only remedy which is adequate is one which will *prevent* the government from unconstitutionally invading the privacy of private email correspondence.

The only “injury” that the government will suffer is its inability to continue its practice of seeking unconstitutional orders, in secret and at great expense to the legitimate privacy expectations of the residents of the Southern District of Ohio. If the preliminary injunction is impeding criminal investigations, as the government contends, then that is as it should be: if a law enforcement practice is unconstitutional – as the use of *ex parte* orders to seize and search the content of private email correspondence is – the government may not utilize it, no matter how much more efficiently it could investigate crime if the unlawful practice were available to it. The preliminary injunction properly prevents the government from investigating crime in a manner which violates the Fourth Amendment.

Finally, the public interest lies squarely on the side of preventing such incursions upon fundamental constitutional protections, yet these constitutional violations will continue unabated in the absence of the preliminary injunction. The public interest weighs heavily in favor of maintaining the preliminary injunction in full force and effect.

I. THE DISTRICT COURT HAS SUBJECT MATTER JURISDICTION OF THIS ACTION.

A. Warshak Has Standing To Seek Injunctive Relief.

1. The applicable standard.

Standing is to be determined as of the time the complaint was filed, *see, e.g., Lynch v. Leis*, 382 F.3d 642, 647 (6th Cir. 2004); *Cleveland Branch, NAACP v. City of Parma*, 263 F.3d 513, 524 (6th Cir. 2001). “At the pleading stage, a plaintiff can satisfy the injury-in-fact requirement by alleging facts that ‘demonstrate a realistic danger of [the plaintiff’s] sustaining a direct injury.’” *Bristol-Myers Squibb Co. v. Shalala*, 91 F.3d 1493, 1497 (D.C.Cir. 1996), *quoting Babbitt v. United Farm Workers Nat’l Union*, 442 U.S. 289, 298 (1979). When, as here, standing is challenged at the pleading stage, courts are to “accept as true all material allegations of the complaint and . . . construe the complaint in favor of the complaining party.” *Pennell v. City of San Jose*, 485 U.S. 1, 7 (1988), *quoting Warth v. Seldin*, 422 U.S. 490, 501 (1975). *See, e.g., United States v. Colorado Supreme Court*, 87 F.3d 1161, 1164 (10th Cir. 1996); *Kelley v. Selin*, 42 F.3d 1501, 1507-08 (6th Cir. 1995). “At the pleading stage, . . . we presume that general allegations embrace those specific facts that are necessary to support the claim.” *Bennett v. Spear*, 520 U.S. 154, 168 (1997), *quoting Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992).

2. Injury-in-fact.

The allegations of the Complaint suffice, at the pleading stage, to allege sufficient risk of injury to validate the invocation of the district court's subject matter jurisdiction and the entry of the preliminary injunction. The Complaint alleges that the government, without notice to Warshak, utilized §2703(d) orders to obtain access to the contents of his private email communications and that it refused to provide him with any assurance that it would not again utilize these unconstitutional procedures in the course of its investigation of him. R1, Complaint, JA ___, ___. From these allegations, "it is easy to presume specific facts under which [Warshak] will be injured." *Bennett*, 520 U.S. at 168. Warshak will be injured if the government again secretly obtains his emails through the use of §2703 orders, which the government has insisted upon maintaining as its prerogative. Indeed, it was only *after* Judge Dlott entered the preliminary injunction that the government began asserting that no use of §2703(d) orders against Warshak was "imminent." See R27, United States' Motion to Stay Pending Appeal, JA ___-___. These are additional facts which the Court can consider in determining Warshak's standing. See *Sullivan v. Syracuse Housing Authority*, 962 F.2d 1101, 1107 (2d Cir. 1992)(in determining standing, court can consider, "along with the allegations made in the complaint, . . . such other facts and circumstances as may be evident from the record").

Warshak's allegations are not, as the government characterizes them, solely allegations of past injury. *See* USB20-21. That argument rests on the faulty premise that the injury to Warshak ended as soon as the §2703 process was served upon, and complied with by, the ISPs. While past injury *alone* will not provide a basis for injunctive relief, *see O'Shea v. Littleton*, 414 U.S. 488, 495-96 (1974), it *does* provide such a basis if there are "continuing, present adverse effects." *Lujan*, 504 U.S. at 564, quoting *City of Los Angeles v. Lyons*, 461 U.S. 95, 102 (1983). Such effects are present in this case because the unlawfully seized emails remain in the government's possession. Warshak's feelings, thoughts, and expressions – many of them contained in private emails with no conceivable relevance to the government's investigation – remain captive on the case agent's computer, available to be read at will by federal agents. So long as those unlawfully seized emails remain in the government's possession, available for scrutiny and review by agents of the government, Warshak's injuries from the government's violations of his Fourth Amendment rights continue unabated.

Moreover, the Supreme Court has recognized that past wrongs are "evidence bearing on whether there is a real and immediate threat of repeated injury." *Lyons*, 461 U.S. at 102. Courts have also considered "the government's failure to disavow application of the challenged provision as a factor in finding standing," *LSO, Ltd. v.*

Stroh, 205 F.3d 1146, 1155 (9th Cir. 2000); such failure to disavow “is an attitudinal factor” which “impart[s] some substance to the fears of [plaintiffs]” *Id.* See, e.g., *United Farm Workers*, 442 U.S. at 302 (where state had not disavowed intention of invoking challenged provision against union, appellees were “not without some reason” in fearing prosecution). Here, the government has categorically refused, on several occasions, to disavow additional use of §2703(d) orders to obtain Warshak’s emails in the course of its investigation of him. That refusal speaks volumes as to the legitimacy and reality of Warshak’s reasonable belief that the government will again unconstitutionally invade his privacy and as to the likelihood that further injury will occur absent judicial intervention. See *Hays v. City of Urbana*, 104 F.3d 102, 103-04 (7th Cir. 1997)(standing not defeated where city had not declared challenged ordinance a “dead letter” but merely represented that it would not prosecute plaintiffs under the ordinance without evidence that they had violated the law).⁶ It is,

6

The government has cited no case in which Article III standing was denied which is remotely comparable to this one. In *Lujan*, the Court found unduly speculative assertions by plaintiffs that someday they intended to travel to places where they hoped to see animals that were allegedly endangered by the challenged agency action. Such “‘some day’ intentions,” the Court said, stretched the purpose of the “imminence” concept “beyond the breaking point” because the plaintiff alleged “only an injury at some indefinite future time, *and* the acts necessary to make the injury happen are at least partly within the plaintiff’s own control.” *Id.* at 564 & n.2 (emphasis added). In *Whitmore v. Arkansas*, 495 U.S. 149 (1990), the plaintiff’s injury depended upon a wholly speculative chain of future events, including that he

moreover, government policy and practice to utilize *ex parte* §2703 process to obtain the content of private email correspondence without a warrant and without a showing of probable cause.⁷ *See Lyons*, 461 U.S. at 105-06 (Court emphasized that there was no official policy authorizing the use of choke hold without provocation but suggested that plaintiff could establish the existence of a case or controversy if he were able to make such an assertion).

Even after the entry of the preliminary injunction, the government said only

obtain a new trial, that he then be again tried, convicted, and sentenced to death, and that the ultimate imposition of the death penalty might be affected by the inclusion of statistics relating to the defendant whose execution he was seeking to block in the state's comparative review data base. In *Lyons*, the Court found no standing where the plaintiff, who had been subjected to a choke hold by police in the past, failed to establish "a real and immediate threat that he would again be stopped for a traffic violation, or for any other offense, by an officer or officers who would illegally choke him into unconsciousness without any provocation or resistance on his part." 461 U.S. at 105. In *O'Shea*, the Court rejected claims by plaintiffs who would suffer injury only in the unlikely event that they violated the law, were charged with a crime, were subjected to proceedings before the respondent judicial officers, and were then the victims of the discriminatory practices of which they complained. 414 U.S. at 496-97. Unlike most of the cases on which the government relies, whether the government will secretly avail itself of §2703 to obtain additional emails of Warshak lies solely within its own control and is not contingent upon anything which Warshak or any third party might do in the future.

⁷
The Department of Justice has played a major role in the litigation of this case and has made it clear that the Department has followed this policy for 20 years and intends to continue to do so in the absence of an injunction. *See* R23, 7/5/06 Transcript, JA ____.

that no further use of secret §2703 orders to obtain Warshak's emails was "imminent," a term which may reflect the language of the Supreme Court's standing cases – and was no doubt chosen for that very reason – but which provides Warshak with no objective protection against further Fourth Amendment violations.⁸ Under the government's theory, a person aggrieved by the unlawful seizure of his emails through *ex parte* §2703 process would *never* be able to prevent another such violation of his Fourth Amendment rights through recourse to the courts, unless the government announced that it intended imminently to seek another secret order, a vanishingly unlikely scenario. Since the *ex parte* process would *always* have been

8

It is *not* "undisputed that Warshak will not be 'imminently' subject to such legal process in the future." USB21. That is merely the position adopted by the government *after* the preliminary injunction entered; Warshak has never acquiesced in it. Moreover, under §2703(f), the government can require an ISP to maintain email on its system for up to 180 days, which means that its representation that no use of §2703 process is "imminent" does not reduce its ability to acquire the content of Warshak's emails if they are currently being preserved against the day when the government can, absent the upholding of the preliminary injunction, again secretly obtain them, even if that day comes during the litigation of the constitutionality of the SCA.

Warshak has never conceded that he "can only guess whether such process will occur in the next week, or month, or ever." USB22. Instead, Warshak was commenting on the government's failure to provide any temporal frame of reference for its assertion that no new orders were "imminent," concluding that "[o]ne thing appears certain: that it means something less than not during the pendency of the litigation of Warshak's complaint." R30, Plaintiffs' Opposition to Government's Motion to Stay Pending Appeal, JA___ (emphasis added).

executed before the victim of an unconstitutional §2703 seizure learned of it, the government would remain free to continue to violate his Fourth Amendment rights with impunity. However, “[o]ne does not have to await consummation of threatened injury to obtain preventive relief.” *Blum v. Yaretsky*, 457 U.S. 991, 1000 (1982). *See, e.g., Colorado Supreme Court*, 87 F.3d at 1166 (“once the gun has been cocked and aimed and the finger is on the trigger, it is not necessary to wait until the bullet strikes before invoking the Declaratory Judgment Act”).⁹ The only reasonable conclusion that can be drawn from the government’s conduct is that, at the time the complaint was filed, there was a real threat of additional *ex parte* subpoenas or orders hanging over Warshak’s head, a threat which has not been eliminated by the government’s self-serving assertion that no such process is “imminent.” Thus, Warshak has the requisite “personal stake in the outcome of the controversy as to assure that concrete adverseness which sharpens the presentation of issues upon which the court so largely depends for the illumination of difficult constitutional questions.” *Baker v. Carr*, 369 U.S. 186, 204 (1962). *See Warth*, 422 U.S. at 498-99. Contrary to the government’s assertion, USB23, this dispute did *not* end before the complaint was filed.

9

The government makes much of the fact that no §2703 process was pending when the complaint was filed, USB19, 21, 22, but it was the government’s own actions in proceeding without notice to Warshak which made it impossible for Warshak to commence litigation while process was pending.

“Imminent” does not have the crabbed meaning which the government attributes to it. It is not a temporal concept requiring injury which is on the verge of occurring but is instead a legal term of art, an “elastic concept” intended to “ensure that the alleged injury is not too speculative for Article III purposes.” *Lujan*, 504 U.S. at 564 n.2. That Warshak cannot pinpoint the hour or the day when the government will again violate his Fourth Amendment rights does not defeat the justiciability of his claims. The government’s refusal to agree that it would not seek new §2703(d) orders during the litigation of this action suffices to remove the injury to Warshak from the realm of speculation and hypothesis. That refusal plainly leaves a real, nonspeculative threat of constitutional injury hanging over Warshak’s head. Thus, in seeking injunctive relief, Warshak relied on real, present injuries and real, threatened future injuries. *See, e.g., Blum*, 457 U.S. at 1000-01 (because nursing homes in which plaintiffs resided were free to transfer patients to lower level of care based on findings of physicians that their continued stay was not medically necessary, possibility that nursing homes would do so was not “imaginary or speculative”).

Because standing existed at the time the complaint was filed, the government cannot defeat that standing by now saying, after the Complaint was filed, that no new use of §2703 is “imminent.”

It is well settled that a defendant’s voluntary cessation of a challenged

practice does not deprive a federal court of its power to determine the legality of the practice. . . . If it did, the courts would be compelled to leave the defendant free to return to his old ways.

Friends of the Earth, Inc. v. Laidlaw Environmental Services, 528 U.S. 167, 189 (2000). See, e.g., *Linton v. Commissioner of Health & Environment*, 30 F.3d 55, 57 (6th Cir. 1994). The government is essentially contending that its assertion that no use of §2703 orders or subpoenas is “imminent” moots the case. However, “a defendant claiming that its voluntary compliance moots a case bears the formidable burden of showing that it is absolutely clear that the allegedly wrongful behavior could not be expected to recur.” *Friends of the Earth*, 528 U.S. at 190. See, e.g., *Adarand Constructors, Inc. v. Slater*, 528 U.S. 216, 222 (2000). The government has not even purported to meet this “formidable burden.”¹⁰

¹⁰

In this sense, this case is analogous to the “capable of repetition, yet evading review” mootness cases, in which courts have held that cases do not become moot simply because the specific dispute which prompted the filing of the action has ended, where there is a reasonable likelihood of recurrence and the duration of the controversy is too short to permit meaningful judicial intervention. See, e.g., *Honig v. Doe*, 484 U.S. 305, 318-19 (1988); *Press-Enterprise Co. v. Superior Court*, 478 U.S. 1, 6 (1986); *Cleveland Nat. Air Show, Inc. v. Department of Transportation*, 430 F.3d 757, 761-62 (6th Cir. 2005). The government maintains its right to employ §2703 process to obtain Warshak’s emails, creating sufficient potential for recurrence, and the duration of the controversy is not just short – Warshak would not even know he had been injured until it was too late to take any action whatsoever to prevent the invasion.

On the record before her, Judge Dlott correctly concluded, based on the government's prior use of §2703(d) orders to seize Warshak's emails and its refusal to agree to refrain from directing such orders to other email accounts of Warshak, "that the prospective harm in this case is far from 'speculative' or 'unsubstantiated.'" R21, Order, JA ___ - ___. She further noted the incongruity inherent in denying a preliminary injunction on the ground that Warshak could not pinpoint exactly when the government would seek another §2703(d) order, when the very *ex parte* nature of the process would prevent his ever having such knowledge. *Id.*, JA ___. The preliminary injunction rightly ensures that when the government again seeks to utilize §2703 to obtain the content of Warshak's emails, Warshak will have the advance notice essential to his ability to assert his constitutional and statutory objections in advance of disclosure to the government. Judge Dlott acted in the only way possible to ensure that Warshak would not be repeatedly subject to violations of his Fourth Amendment rights which he, because of his lack of knowledge that such violations were occurring, would be powerless to prevent, requiring that "[t]o the extent that the United States wishes to avoid making a showing of probable cause and obtaining a warrant before undertaking future email seizures, it must at least notify Warshak of

its intent to circumvent those standard constitutional protections.” *Id.*, JA ____.¹¹

3. Redressability.

The government’s redressability argument is nothing more than a variant of its argument that Warshak has not satisfied the injury-in-fact requirement. *See* USB25-26. There can be no real question that if Warshak has satisfied the injury-in-fact component of standing – as he has – the threat of injury is one redressable by the federal courts. Redressability is a question of whether a plaintiff “personally would benefit in a tangible way from the court’s intervention.” *Steel Co. v. Citizens for a Better Environment*, 523 U.S. 83, 104 n.5 (1998), *quoting* *Warth*, 422 U.S. at 508. Here, Warshak has demonstrated the existence of a real, nonspeculative threat that the government will again use *ex parte* §2703 process to obtain his emails in violation of the Fourth Amendment. Injunctive relief would perfectly redress that threatened injury by preventing its occurrence. *See* R21, Order, JA ____ (“there is no apparent dispute that the requested injunction, if granted, would avert the prospective harm Warshak describes”); *see also* *Friends of the Earth*, 528 U.S. at 185-86. This is not,

11

After Judge Dlott issued the preliminary injunction order, the government disclosed that it had also utilized secret §2703(b) subpoenas to obtain the content of Warshak’s emails in addition to the §2703(d) orders which were the subject of Warshak’s Complaint. This revelation led to the filing of Warshak’s First Amended Complaint on August 28, 2006. R33.

reasons addressed in Section I(A)(2), *supra*, the constitutional ripeness requirement is satisfied in this case.

“Ripeness entails a functional, not a formal inquiry.” *Pfizer, Inc. v. Shalala*, 182 F.3d 975, 980 (D.C.Cir. 1999). Here, the practical, functional reality is that under the government’s ripeness theory, Warshak would *never* be able to mount an advance challenge to further secret use of §2703 to seize his emails because, by depriving him of notice, the government can ensure that Warshak’s emails will have already been disclosed to it before he could possibly seek judicial intervention to challenge the constitutionality of the procedure utilized to obtain disclosure. *See Kardules v. City of Columbus*, 95 F.3d 1335, 1345 (6th Cir. 1996)(“Appellant’s claims could be found ripe if they could show that, at the time they filed the complaint, the merger proposal was likely to be presented to the voters in the upcoming election, *and that they could not have obtained timely injunctive relief had they waited until the merger proposal was actually placed on the ballot to file suit*”(emphasis added)); *see also Ohio Forestry Ass’n v. Sierra Club*, 523 U.S. 726, 734 (1998)(finding case not ripe because Sierra Club would have “ample opportunity” to bring suit later when the threatened harm became more concrete); *Renne v. Geary*, 501 U.S. 312, 322-23 (1991)(similar).

government will again use secret §2703 process directed at Warshak’s emails defeats neither Warshak’s standing nor the ripeness of his claims.

Prudential ripeness considerations are satisfied in this case as well. Warshak's facial challenge is not, contrary to the government's argument, "completely contingent upon a court authorizing a 2703(d) order sometime in the future." USB27. See, e.g., *Lehn v. Holmes*, 364 F.3d 862, 868 (7th Cir. 2004); *United States v. Fell*, 360 F.3d 135, 139-40 (2d Cir. 2004); *United States v. Quinones*, 313 F.3d 49, 59-60 (2d Cir. 2002); *United States v. Loy*, 237 F.3d 251, 256-58 (3d Cir. 2001); *United States v. White*, 244 F.3d 1199, 1202-1204 (10th Cir. 2001). Warshak's facial challenge to the constitutionality of §2703 is a legal one: Does the government's secretly obtaining the content of private emails without a warrant and on less than a showing of probable cause violate the Fourth Amendment? Whatever facts are necessary to the determination of that issue can be presented to the district court in the course of this litigation. The issues are *now* "fit[] . . . for judicial decision," *Texas v. United States*, 523 U.S. 296, 301 (1998),¹³ and the Court would not "benefit from

13

In *Texas v. United States*, USB28, the challenged procedure had *never* been implemented and required the occurrence of several contingencies before it ever would be; Texas described no circumstances under which imposition of the procedure was likely, and the specific circumstances under which the provision was applied, were it ever to be applied, would be important to the determination of the issues before the courts. See 523 U.S. at 300-01. Such circumstances are not present here. In the only other case relied on by the government, *Adult Video Ass'n v. Department of Justice*, 71 F.3d 563 (6th Cir. 1995), plaintiffs did not challenge the facial validity of federal anti-obscenity laws but instead sought a declaration that they could not be prosecuted under those statutes were they to disseminate a particular film. *Id.* at 566-

further factual development of the issues presented.” *Ohio Forestry Ass’n*, 523 U.S. at 733. “A case may be considered ripe when there is no compelling judicial interest in deferring review.” *Dixie Fuel Co. v. Commissioner of Social Security*, 171 F.3d 1052, 1058 (6th Cir. 1999). No such compelling judicial interest is present here.

Contrary to the government’s argument, USB28-29, withholding judicial consideration of the constitutionality of §2703 would impose substantial hardship on Warshak – it would effectively deny him the ability to *ever* obtain relief to prevent further violations of his Fourth Amendment rights. There is nothing “prudential” about leaving the government free to violate the Fourth Amendment with impunity simply because Warshak cannot identify an exact moment in time when the government will again violate his Fourth Amendment rights. In entering the preliminary injunction, Judge Dlott acted in the only way possible, given her preliminary conclusions regarding the unconstitutionality of *ex parte* §2703(d) orders, to protect the Fourth Amendment rights of the residents of the Southern District of

67. The claim was not ripe, this Court concluded, because the government had not indicated that it intended to take action with respect to that particular film and because it was could not be accurately determined whether or not the film was obscene without the background of how the film was promoted and disseminated, facts which did not yet exist. *Id.* at 568. Here, by contrast, Warshak *has* challenged the facial validity of §2703, the government has insisted on maintaining its power to seek additional §2703(d) orders, and no further extrajudicial developments are needed for the court to be able to determine the facial validity of §2703.

Ohio pending full litigation of the merits of Warshak's Fourth Amendment claim *and* to ensure that when the government again sought to utilize §2703 to obtain Warshak's emails, Warshak would have the opportunity to present an as-applied challenge *before* the government seized and searched his emails. Warshak's claims are fully ripe for adjudication.

II. THE PRELIMINARY INJUNCTION CONSTITUTES A PROPER EXERCISE OF THE DISTRICT COURT'S DISCRETION.

A. Standard of Review.

A trial court's decision to grant a preliminary injunction is accorded great deference. *See, e.g., United States v. Edward Rose & Sons*, 384 F.3d 258, 261 (6th Cir. 2004). "The injunction will seldom be disturbed unless the district court relied upon clearly erroneous findings of fact, improperly applied the governing law, or used an erroneous legal standard." *Mascio v. Public Employees Ret. Sys.*, 160 F.3d 310, 312 (6th Cir.1998). Moreover, "[t]his Court 'will reverse a district court's weighing and balancing of the equities only in the rarest of circumstances.'" *Id.*, quoting *Moltan Co. v. Eagle-Picher Indus., Inc.*, 55 F.3d 1171, 1175 (6th Cir.1995). Judge Dlott did not abuse her discretion in entering the preliminary injunction in this case.

B. The District Court Applied The Proper Legal Standards.

In recent years, email has become the preferred medium of written communication for millions of Americans, revolutionizing the form in which individuals communicate to each other their thoughts, ideas, beliefs, hopes, dreams, and fears and becoming the backbone of the country's communication system. This new embodiment of private communication is no less deserving of the protections of the warrant clause of the Fourth Amendment, with its attendant protections of probable cause and particularity and its prohibition of overbroad searches than were sealed letters and packages formerly conveyed by horseback, then by mail carrier's truck and common carriers, which the Supreme Court has long held may not be opened and searched by the government without a warrant. Instead of the protections of the warrant clause of the Fourth Amendment, the government contends that the applicable standards are those governing administrative and grand jury subpoenas and that, under that standard, it may pursue a policy and practice under which agents of the executive branch secretly and without the protections which would be supplied by a warrant, seize and read private communications. The government's arguments rest upon the fallacious assumption that there are no limitations on that which the government may obtain and search by means of a subpoena. Moreover, protections are available in the administrative/grand jury subpoena context which are lacking in

the context of *ex parte* §2703(d) orders: an opportunity to contest production of the subpoenaed documents or materials *in advance* of their production to the government and the requirement that the subpoenaed material be relevant to the investigation. Here, the government seized and searched *every* ISP-stored email in the accounts at which the orders were directed, without limitation as to time frame, parties to the communication, or the subject matter of the communication, the very antithesis of a “reasonable” search.

At the outset, it is important to note that the government is incorrect in stating that Judge Dlott required the application of a probable cause standard to §2703(d) orders. *See* USB36. She did not. While finding Warshak’s analogy between ISP-stored emails and sealed containers, including letters, “more apt” than the government’s position, Judge Dlott did not incorporate a requirement of probable cause into her ruling. On the contrary, she expressly stated that she was *not* “presently prepared to hold that . . . §2703(d) facially violates the Fourth Amendment by simple virtue of the fact that it authorizes the seizure of personal emails from commercial ISPs without a warrant and on less than a showing of probable cause.” R21, Order, JA ___ - ___. All that the preliminary injunction does is ensure that, where the government does not have probable cause to obtain a warrant, the account holder will have an opportunity to be heard *before* the government invades the privacy of his

emails.

In any event, the government's position is not well-taken. The government's insistence that "compelled disclosure" is subject only to a "reasonableness" requirement simply assumes the conclusion that an individual's ISP-stored emails may, consistently with the Fourth Amendment, be obtained through the issuance of an order/subpoena commanding their production and then be subjected to warrantless search. That conclusion is inconsistent with the Supreme Court's well-established case law regarding closed containers, such as letters and packages, which is equally applicable in the context of seizures and searches of ISP-stored emails.

1. Emails are "closed containers" which may not be searched without a warrant.

Warrantless searches and seizures are presumptively unreasonable under the Fourth Amendment, *Horton v. California*, 496 U.S. 128, 133 n.4 (1990); *Katz v. United States*, 389 U.S. 347, 357 (1967), as are searches and seizures of closed containers based on less than probable cause. *United States v. Ross*, 456 U.S. 798, 809-12 (1982). As early as 1878, the Supreme Court recognized that the contents of "[l]etters and sealed packages . . . in the mail are as fully guarded from examination and inspection . . . as if they were retained by the parties forwarding them in their own domicile." *Ex Parte Jackson*, 96 U.S. 727, 733 (1878). So long as a package is

“closed against inspection,” the Fourth Amendment protects its contents, “wherever they may be,” and the police must obtain a warrant to search it just “as is required when papers are subjected to search in one’s own household.” *Id. Accord United States v. Van Leeuwen*, 397 U.S. 249 (1970). Indeed, the Supreme Court has long recognized that individuals do not surrender their expectations of privacy in closed containers when they send them by mail or common carrier and that “[l]etters and sealed packages are in the general class of effects in which the public at large has a reasonable expectation of privacy; warrantless searches of such effects are presumptively unreasonable.” *United States v. Jacobsen*, 466 U.S. 109, 114 (1984). See *United States v. Chadwick*, 433 U.S. 1, 10 (1977).

Emails stored on an ISP’s server are a form of closed container. The contents of an email are not visible to the naked eye; instead, several intrusive searches must occur before the contents may be read. One seeking to view the contents of an ISP-stored email must first gain access to that portion of the ISP’s server that houses the subscriber’s email; this is a search in and of itself. Even after one gains access to the a subscriber’s virtual mailbox, the content of those emails remain shielded from public view, much like the content of letters sitting in a “real” mailbox. To view the contents of an email, another physically intrusive act is necessary: the email must be unsealed through the operation of a computer function such as clicking on the email

using a mouse or using the computer's "open" function, an act doctrinally indistinguishable from the act of opening a sealed letter or package or unlocking a closed footlocker. *See* R1, Complaint, JA ___ - ___; R11, Preliminary Injunction Motion, JA ___ - ___. ISP-stored emails are entitled to protection of the Fourth Amendment commensurate with those accorded other closed containers such as letters and packages.

2. The government's effort to substitute the standards applicable to subpoenas for the protections of the warrant clause should be rejected.

In essence, the government argues that because §2703(d) orders are more like subpoenas than they are warrants, they should be subject to the same constitutional standards as subpoenas. USB39-40. This argument entirely begs the question whether the Fourth Amendment requires that the government obtain a warrant before it may seize and search ISP-stored email content. Contrary to the government's assumption, there *are* limits to what the government may accomplish through the mechanism of grand jury and administrative subpoenas. No one, for example, would contend that the government could effect a search of an individual's rented storage compartment by issuing a subpoena to the management company to produce its contents before the grand jury. Nor could it be contended that the government could search a suitcase in the custody of an airline or a footlocker shipped via a third party carrier simply

because it obtained possession of it through a subpoena. Nor could the government permissibly seize and search a briefcase by issuing a subpoena to the restaurant where it had been checked while its owner dined or subpoena a first-class letter on its way to its intended recipient and then open and read it.

Even if the government can acquire possession of a closed container through service of a subpoena, that container cannot be searched without a warrant. For example, the government cannot search a computer's files simply because it obtained possession of the computer pursuant to a subpoena, *see United States v. Triumph Capital Group*, 211 F.R.D. 31 (D.Conn.2002)(government obtained laptop through grand jury subpoena but obtained warrant before searching it), nor can the government search unopened mail without a warrant, even if it obtained the mail pursuant to a subpoena. *See United States v. Barr*, 605 F.Supp. 114 (S.D.N.Y. 1985)(government obtained unopened mail through grand jury subpoena but obtained search warrant before opening it). *See also Wilson v. Moreau*, 440 F.Supp.2d 81, 108 (D.R.I. 2006)(police could not search library patron's private email account which he accessed through public library computers without either a warrant or valid consent). Under the government's expansive and untenable proposition, the government could extinguish the protections of the Fourth Amendment warrant clause through the simple expedient of serving a grand jury or administrative subpoena requiring the

production of the closed container which it wishes to search. This is not, has never been, and certainly should not be, the law.

The government's effort to analogize §2703(d) orders to subpoenas must fail. Administrative subpoenas are not self-executing, *see United States v. Sturm, Ruger & Co., Inc.*, 84 F.3d 1, 3 (1st Cir. 1996), but may be enforced only by judicial order *after* the affected parties have had the opportunity to be heard and to raise their constitutional claims. *See, e.g., Oklahoma Press Publishing Co. v. Walling*, 327 U.S. 186, 195 (1946)(distinguishing administrative subpoena from search on ground that “[n]o officer or other person has sought to enter petitioner’s premises against their will, to search them, or to seize or examine their books, records or papers without their assent, otherwise than pursuant to orders of court authorized by law *and made after adequate opportunity to present objections . . .*”(emphasis added)); *Donovan v. Lone Steer, Inc.*, 464 U.S. 408, 414-15 (1984) (same); *In re Administrative Subpoena (Doe)*, 253 F.3d 256, 264 (6th Cir. 2001)(“[o]ne primary reason” for the distinction between the reasonableness standard applicable to administrative subpoenas and the probable cause standard applicable to searches and seizures pursuant to a warrant is that “unlike ‘the immediacy and intrusiveness of a search and seizure conducted pursuant to a warrant,’” the reasonableness of an administrative subpoena’s command can be contested in federal court before yielding the

information).¹⁴

As the Fourth Circuit has explained:

A warrant is a judicial authorization to a law enforcement officer to search or seize persons or things. To preserve the advantage of speed and surprise, the order is issued without prior notice and is executed, often by force, with an unannounced and unanticipated physical intrusion. . . . Because this invasion is both an immediate and substantial invasion of privacy, a warrant may be issued only by a judicial officer upon a demonstration of probable cause – the safeguard required by the Fourth Amendment.

A subpoena, on the other hand, commences an adversary process during which the person served with the subpoena may challenge it in court before complying with its demands. . . . As judicial process is afforded before any intrusion occurs, the proposed intrusion is regulated by, and its justification derives from, that process.

In re Subpoena Duces Tecum, 228 F.3d 341, 348 (4th Cir. 2000). See also *United States v. Dionisio*, 410 U.S. 1, 10 (1973). The *ex parte* §2703(d) order is far more closely akin to a warrant than to an administrative subpoena: it is swift, sudden,

14

The government relies on the four-part standard for enforcement of subpoenas articulated by this Court in *Doe*. See USB40-41. In *Doe*, which largely turned on the language and intent of the statute authorizing the use of administrative subpoenas in health care investigations, the subpoena listed nine particularly described categories of documents, 253 F.3d at 260-61, in sharp contrast to the unlimited production commands of the §2703(d) orders here. The unlimited §2703(d) orders here – which there is no reason to believe differ from those generally employed by the government – do not even satisfy the *Doe* standard. Use of §2703 orders to conduct wholesale fishing expeditions among a subscriber's email communications is an abuse of the court's processes.

extremely invasive of personal privacy, commands a physical intrusion into a protected area of the account holder, and, as to the account holder, is entirely veiled in secrecy. The prior ability to contest the subpoena, including the ability to raise all available Fourth Amendment claims, in *advance* of production to the government is a key safeguard embodied in the administrative subpoena context,¹⁵ which is entirely lacking in the context of *ex parte* §2703(d) orders, which give the government, through invocation of §2705, the power to prevent notice to the email account holder, leaving him powerless to prevent the government's trampling upon his Fourth Amendment rights and invasion into an intensely private area.¹⁶

15

In *Oklahoma Press* and *Doe*, on which the government relies, the administrative subpoenas were served on the targets of the agency investigation, providing them with full notice of the government's action and full opportunity to challenge it before the documents were produced. The government also relies on *Dionisio*, a case involving a grand jury subpoena for voice exemplars. See USB39. *Dionisio* is, however, of dubious relevance to the government's argument. The Court predicated its holding upon two conclusions: one, that a grand jury subpoena is not a seizure within the meaning of the Fourth Amendment, 410 U.S. at 9, and two, that the defendant had no reasonable expectation of privacy in the sound of his voice, which was routinely exposed to the public. 410 U.S. at 14-15. Here, by contrast, there was both a seizure and "a governmental intrusion on privacy against which the Fourth Amendment affords protection." 410 U.S. at 10. Moreover, Warshak, in contrast to *Dionisio*, had no opportunity to challenge the compulsion through pre-disclosure adversarial litigation.

16

Section 2703 allows the ISP to seek relief from the order, but only based on unusual voluminosity or other undue burden. The government's argument that §2703(d) orders "remain at all times under the control and supervision of a court,"

The *ex parte* §2703(d) order differs from an administrative subpoena in another crucial aspect as well: the complete and utter absence of the particularity required to prevent the exploratory rummaging through a citizen's private papers and effects which were such anathema to the Framers that they erected in the Fourth Amendment a prohibition against general warrants. See *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999). As the administrative subpoena cases on which the government relies demonstrate, an administrative subpoena is necessarily limited to the subject matter of the specific investigation which the agency is authorized by law to undertake, and the items sought must be relevant to that investigation; an administrative subpoena will be accompanied by a specific list of responsive documents, which may be challenged as irrelevant or overbroad. Here, in exceedingly sharp contrast, the *ex parte* §2703(d) orders compelled the production of *all* of Warshak's emails – regardless of how far removed their content was from the subject

USB40, is not consistent with reality. The court issues the order, but if the ISP complies with the order and turns over to the government the entirety of the target's emails, the court's involvement is at an end. Once the government obtains the emails, it is free to rummage at will through private correspondence without limitation, having successfully prevented the target from having the notice which would permit him to invoke the protection of the courts to challenge the overbreadth and lack of particularity of the order or to otherwise seek a judicial order limiting the scope of the government's search of his emails to those likely to be relevant to the investigation. While notice to the target of a traditional subpoena may not be *required* by the Fourth Amendment, see USB50-51, this is far different from a procedure which affirmatively *prevents* notice to the target. See Section II(B)(6), *infra*,

matter of the government's investigation – and left the government in unchallenged possession of that content, free to read every word Warshak had written and every word that had been written to him – regardless of how intensely private and personal the content and how utterly unrelated to the government's investigation. Contrary to the government's argument, unlimited *ex parte* §2703 orders such as those used here *would* fail any reasonableness test, even were that the applicable standard, which it is not. *See Groh v. Ramirez*, 540 U.S. 551 (2004)(lack of particularity in warrant rendered search unreasonable under Fourth Amendment). The Fourth Amendment reasonableness clause imposes requirements *in addition to* those imposed by the warrant clause. *See Baranski v. Fifteen Unknown Agents*, 452 F.3d 433 (6th Cir. 2006); *In re Search of The Rayburn House Office Building Room Number 2113*, 432 F.Supp.2d 100, 107 (D.D.C. 2006).

3. Generalities regarding the grand jury's right to everyman's evidence do not trump the requirements of the Fourth Amendment.

The constitutional inquiry central to this appeal is not advanced by recitations of oft-repeated generalities regarding the grand jury's "right to everyman's evidence," USB41, *quoting Branzburg v. Hayes*, 408 U.S. 665, 688 (1972). Nothing in the arguments advanced by Warshak would make ISPs "immune" from the general rules

regarding grand jury or administrative subpoenas *where what the government seeks is permissibly obtainable by it through the issuance of a subpoena*. See USB42. The resolution of the constitutional issue in this case turns not upon generalities regarding the powers of grand juries and administrative agencies to investigate violations of the law but instead upon an examination of the nature of ISP-stored emails in relation to the scope of the warrant clause of the Fourth Amendment.

Nor is Warshak asking the Court to create a “sweeping” privilege for emails. See USB42-43. If, as it does, the Fourth Amendment requires that the government obtain a warrant based on probable cause before it seizes and searches ISP-stored emails, then the grand jury or investigative agency is not entitled to obtain those emails through the issuance of a subpoena.

4. The cases regarding third-party subpoenas on which the government relies do not undermine the validity of the preliminary injunction.

The government also relies on a number of cases concerning subpoenas to third parties, reiterating its argument that the applicable standard is one of reasonableness. At issue in *United States v. Phibbs*, 999 F.2d 1053 (6th Cir. 1993), USB43-44, were garden-variety subpoenas issued to third parties for telephone and credit card records, as to which Phibbs had no reasonable expectation of privacy and, hence, no Fourth

Amendment claim. Nothing in *Phibbs* undercuts the validity of the preliminary injunction, which was predicated upon a supportable finding that email account holders maintain a reasonable expectation of privacy in their ISP-stored emails and upon the conjunction of the seizure of email content without probable cause *and* without notice.

In *Schwimmer v. United States*, 232 F.2d 855 (8th Cir. 1956), USB44, the defendant did not contend that a warrant based on probable cause was required before the government could seize and search his closed containers, arguing only that the subpoena was unreasonable under the Fourth Amendment. *Schwimmer* predated the Supreme Court's "closed container" case law, and, to the extent that it authorized the government to search, without a warrant, closed containers belonging to another produced pursuant to a grand jury subpoena addressed to the third party in whose custody they temporarily reposed for safekeeping, it is no longer good law. Notably, in *Schwimmer*, the Court invalidated the first subpoena issued by the government, which sought unlimited access to *all* of Schwimmer's documents in the possession of the third party, because it "constitute[d] a general fishing expedition" amounting to an unreasonable search and seizure against Schwimmer. *Id.* at 862.

The telegram copies in the possession of the telegraph companies which were the subject of the subpoenas in *Newfield v. Ryan*, 91 F.2d 700 (5th Cir. 1937), are,

contrary to the government's argument, not remotely comparable to private emails stored in an ISP account in the name of the subscriber. *See* USB44. Moreover, the subpoenas to the telegraph companies were limited to telegrams which were sent or received during a finite period of time, and which dealt only with the subject matter under investigation. *See id.* at 701, 703. They could not, therefore, the Court said, "be regarded as dragnets for fishing expeditions." *Id.* at 703. The same cannot be said in this case.

The government's reliance on *United States v. Palmer*, 536 F.2d 1278 (9th Cir. 1976), *see* USB45, is also misplaced. In *Palmer*, the government obtained, via subpoena to defendant's attorney, two suitcases which had been removed from defendant's car by a third party and delivered to the attorney on the defendant's behalf. The Court found it unnecessary to address the defendant's expectation of privacy in the subpoenaed items based on its conclusion that the use of a properly limited subpoena was not an unreasonable search under the Fourth Amendment. *Id.* at 1281-82. However, the suitcases were apparently sought not for their contents but because they were thought to have been purchased with proceeds from the robbery for which the defendant was arrested. *See id.* at 1281. Had it been the contents of the suitcases that were sought, the suitcases could not have been searched without a warrant. Even if a third party may be compelled via subpoena to *produce* a closed

container, the government may gain access to its contents only through a warrant issued upon a showing of probable cause.

5. The statutory framework and “industry practice” are irrelevant to the validity of the preliminary injunction.

That the SCA authorizes the use of subpoenas and orders to obtain emails in electronic storage for more than 180 days is not in dispute; it plainly does. *See* USB46. That fact does not, however, control the inquiry. The question is not what the *statute* authorizes, but what the *Constitution* requires. As to the latter inquiry, Congress is not the final arbiter.¹⁷ Ultimately, it is the province of the courts to determine whether ISP-stored emails should be regarded, for purposes of the Fourth Amendment, as closed containers which cannot be searched absent a warrant issued upon probable cause. Moreover, the “balance” struck by Congress “when email and the Internet were still relatively new and used by few people,” USB46, is not automatically the “balance” which should be drawn when, as now, email has evolved

17

The Fourth Amendment issue presented here is thus very different from that in cases which have looked, in part, to federal statutory and regulatory authority in determining whether an individual had an objectively reasonable expectation of privacy. *See* USB47 n.9. In *Doe v. Broderick*, 225 F.3d 440, 451 (4th Cir. 2000), on which the government relies, the Court concluded that the plaintiff had a legitimate expectation of privacy in his medical treatment records because they “contain intimate and private details that people do not wish to have disclosed [and] expect will remain private.” The same can be said of many email communications.

into the communication method of choice for millions of Americans.¹⁸ And, ultimately, it is not a question of “balance” at all, but of what the Fourth Amendment requires in the context of seizure and search of private ISP-stored emails.

Similarly, it is irrelevant to the validity of the preliminary injunction that the SCA permits ISPs to access communications stored on their systems and to respond to compulsory process. *See* USB47-49. That the ISP may access stored email does not make it reasonable for the *government* to obtain and read the contents of private emails without a warrant or to dispense with any pretense of particularization or of confining the scope of the search to the subject of the investigation. The SCA itself expressly differentiates between what the ISP may do and what the government may do. Moreover, the government has provided no reasons to believe that ISPs routinely *read* the contents of their customers’ emails, as opposed to screening via computer

18

In addition, the “balance” struck by Congress, *see* USB47, makes no sense. Congress extended the full protection of the warrant clause of the Fourth Amendment to emails in electronic storage for 180 days or less, but permitted the government to obtain emails in electronic storage for 181 days or more through subpoena or court order. Why Congress drew such an arbitrary demarcation is not revealed. A year-old email is no less worthy of Fourth Amendment protection than is a day-old one, and permitting the seizure of a 181-day old email via §2703 orders or subpoenas but requiring a warrant based on probable cause for a 179-day old one is a distinction without constitutional foundation or principle.

programs without human intervention or actual comprehension of the content.¹⁹ In any event, the mere fact that a third party has a theoretical right of access to the closed containers of another in their possession for specific and limited purposes does not give *the government* the right to obtain the contents of the container without either a warrant or an exception to the warrant requirement. The government's proposed substitution of a "reasonableness" standard for the Fourth Amendment probable cause requirement threatens to eviscerate the protections of the Fourth Amendment where closed containers, including letters and emails, are concerned and to upset the valid privacy expectations of the millions of citizens who regularly entrust their belongings, including their most intimate and personal possessions, to third parties, believing them to be safe and secure from unwarranted intrusion, including intrusion by the government.

6. The district court did not invalidate §2703 solely because of the absence of notice.

The government also criticizes the requirement of the preliminary injunction that notice be given to the account holder, relying on *SEC v. Jerry T. O'Brien, Inc.*,

19

Contrary to the government's suggestion, nothing in the preliminary injunction, or in Warshak's arguments, has the slightest potential to impact the ability of ISPs to protect the integrity of their systems by screening for viruses, pornography, spam, or the like. *See* USB49-50.

467 U.S. 735 (1984). USB50-51. The district court did not invalidate the SCA solely because of the lack of notice, but instead based upon the unconstitutional synergy of §§2703(b)(1)(B)(ii), 2703(d), and 2705, which, in conjunction, allow the government to secretly seize and search the entirety of an individuals' private email correspondence and to affirmatively *prevent* the individual from learning of the intrusion at a point at which he could lodge a judicial challenge in advance of the seizure. In the administrative/grand jury subpoena context, while notice to the target of the subpoena may not be required by the Fourth Amendment, the fact remains that, where, as is often the case, the target learns of the subpoena, he has the ability to move to quash it. In the §2703 context, however, notice to the account holder is *prohibited*, thus affirmatively denying him any chance to protect his rights in advance of disclosure.²⁰ Judge Dlott was quite correct in recognizing the "grave" constitutional concerns presented by the combination of unparticularized wholesale warrantless seizures of the content of personal emails and the prohibition of prior notice to the account holder which precludes the raising of constitutional or statutory challenges to the seizure and subsequent search of personal correspondence.

20

Moreover, in the §2703 context, unlike the statutory framework at issue in *O'Brien*, Congress expressed a preference for advance notice unless the government satisfies the exceptions to the notice requirement enumerated in §2705.

C. Judge Dlott Properly Concluded That The SCA Is Facially Unconstitutional To The Extent That It Permits *Ex Parte* Seizure of Email Content Without a Showing of Probable Cause.

1. The applicable standard.

The “no constitutional application” standard articulated in *United States v. Salerno*, 481 U.S. 739, 745-46 (1987), on which the government relies, USB30, is not the standard applicable to Warshak’s facial challenge to the constitutionality of §2703. More recently, in *City of Chicago v. Morales*, 527 U.S. 41 (1999), a plurality of the Supreme Court “indicated that the standard for mounting a facial challenge is not as severe as *Salerno* had suggested.” *United States v. Quinones*, 313 F.3d 49, 60 n.8 (2d Cir. 2002). See *United States v. Frandsen*, 212 F.3d 1231, 1235 n.3 (11th Cir. 2000) (noting that “the *Salerno* rule’ has been subject to heated debate in the Supreme Court, where it has not been consistently followed”). The *Morales* plurality stated: “To the extent we have consistently articulated a clear standard for facial challenges, it is not the *Salerno* formulation, which has never been the decisive factor in any decision of this Court, including *Salerno* itself.” 527 U.S. at 55 n.22.

Unlike *Salerno* and *Coleman v. Dewitt*, USB30,²¹ Warshak’s facial challenge

21

This Court applied the *Salerno* rule to the defendant’s overbreadth challenge in *Coleman v. DeWitt*, 282 F.3d 908 (6th Cir. 2002), but the applicable standard would not have affected the result, as this Court concluded that not only did the

to the SCA is not an overbreadth challenge. Instead, it is a straightforward legal challenge: because ISP-stored emails are the equivalent of closed containers which the Supreme Court has long said may not be searched absent a warrant issued upon probable cause, it follows that to the extent that the SCA authorizes the government to seize and search email content without a warrant issued upon a showing of probable cause, it falls afoul of the requirements of the Fourth Amendment.²²

2. **The government has failed to demonstrate that there is any circumstance under which the use of §2703(d) orders to seize and search the content of ISP-stored emails, without a showing of probable cause and without notice to the account holder, would not violate the Fourth Amendment.**

The government offers three examples of circumstances under which it contends that email senders or recipients have no reasonable expectation of privacy in the content of their emails such that *ex parte* warrantless seizure and search of their emails would not violate the Fourth Amendment. None of these examples withstand

challenged statute apply to the defendant's conduct, it did not appear to be potentially unconstitutional in *any* application. *Id.* at 914-15.

22

For example, the possibility that exceptions to the Fourth Amendment warrant requirement could be hypothesized – such as the need to enter a home in a medical emergency – would not prevent a court from striking down as facially unconstitutional a statute permitting warrantless searches of homes, which would be the untenable result of the application of the “no constitutional application” to facial challenges based not on overbreadth but on the substantive requirements of the Fourth Amendment.

scrutiny. Judge Dlott properly concluded that an individual does not “surrender[] 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.” R21, Order, JA ___.²³

What the preliminary injunction accomplishes – and properly so – is to prevent Fourth Amendment violations in advance of their occurrence, a crucial intervention where the content of private email correspondence is concerned, as no after-the-fact remedy can undo the government’s invasion into the private thoughts, hopes, dreams, fears, and aspirations of the citizen whose emails have been read by government agents. The privacy rights and expectations of account holders in their ISP-stored emails correctly recognized by Judge Dlott cannot be excluded from injunctive relief simply because the government can imagine circumstances under which a hypothetical subscriber might not have a reasonable expectation of privacy.

23

In creating a relationship with an ISP, the subscriber does not relinquish a reasonable expectation of privacy in his emails stored on the ISP’s server. Like an individual who rents a storage space at a local storage facility, an ISP subscriber secures a section of the ISP’s server, which is “locked” by being password-protected and hence inaccessible to the public at large. *See* R1, Complaint, JA ___ - ___; R11, Preliminary Injunction Motion, JA ___ - ___. Indeed, the previously-issued orders in this case demanded the production of emails “that were placed or stored in directories *owned or controlled by the accounts identified in Part A*” JA ___, ___ (emphasis added).

The government first points to the potential that employees may not have a reasonable expectation of privacy in their work email. USB32-33. That employees' reasonable expectations of privacy in emails on their employer-provided service may in certain circumstances be eliminated by express employer disclaimers does not render Judge Dlott's ruling infirm.²⁴ Judge Dlott held the SCA facially unconstitutional *only* to the extent that it permits warrantless seizures of email content without advance notice to *the account holder*. Thus, a §2703(d) order directed at the employer-provided email service would, under Judge Dlott's ruling, violate the Fourth Amendment only if the government failed to give advance notice to *the employer*. Whatever expectations of privacy individual employees may or may not have is irrelevant to the validity of the preliminary injunction.

Second, the government suggests that an email account is abandoned when the subscriber stops paying for the service and that the subscriber thereafter maintains no legitimate expectation of privacy in the account. USB33. Property is not, however, abandoned if the person claiming the protection of the Fourth Amendment continues

24

The government's reliance on *Guest v. Leis*, 255 F.3d 325 (6th Cir. 2001), USB32, is misplaced. *Guest* involved an internet bulletin board run by a teenager from his home, not a private email account maintained with an ISP. The bulletin board expressly warned that no messages posted should be considered private and that they could be read by the system operator. *See id.* at 331, 333.

to have a legitimate expectation of privacy in it, *see, e.g., United States v. Robinson*, 390 F.3d 853, 873 (6th Cir. 2004); *United States v. Oswald*, 783 F.2d 663, 666 (6th Cir. 1986), and the government offers nothing to negate a continuing, reasonable expectation that emails already on the service would remain private after termination of the account except its bald say-so.²⁵ Yahoo!, for example, informs its users that the consequence of termination may be *deletion* of the user's content from the service, thus assuring its users that their private communications will not be revealed if they cease to use Yahoo!'s service. *See* R30, Plaintiff's Opposition to Government's Motion to Stay Pending Appeal, JA ____.

Third, the government suggests that persons who obtain email services by fraud, such as through the use of stolen credit cards, have no reasonable expectation of privacy in their emails. The case cited by the government, *United States v.*

²⁵ Property is not "abandoned" in the legal sense if it is left in the hands of a third party who the owner reasonably believes will safeguard it from the prying eyes of the government; the individual retains a reasonable expectation of privacy in such property. *See, e.g., United States v. Fultz*, 146 F.3d 1102 (9th Cir. 1998). The government's attempted analogy to hotel rooms after the expiration of the rental period is misplaced. In the hotel room context, once the rental period has expired or been lawfully terminated, the physical space within which the guest's possessions are located reverts to the hotel, to which then passes the power to consent to a search of the room. *See United States v. Allen*, 106 F.3d 695, 699 (6th Cir.1997). The government has presented nothing to suggest that, absent the force of warrant, subpoena, or order, any ISP would consent as a normal practice to the disclosure of its prior customers' emails.

Caymen, 404 F.3d 1196 (9th Cir. 2005), USB33, does not, however, bear out its assertion. In *Caymen*, the stolen laptop had lawfully come into the possession of the police through the execution of a valid search warrant before it was searched. In concluding that the defendant had no reasonable expectation of privacy in the stolen laptop, the Court distinguished two cases involving hotel rooms still being used by the persons who had obtained them through fraud, which held that so long as the hotel had not taken affirmative steps to reclaim possession of the room, the occupant maintained a reasonable expectation of privacy in the room. *United States v. Cunag*, 386 F.3d 888, 894-95 (9th Cir. 2004); *United States v. Bautista*, 362 F.3d 584, 590-91 (9th Cir. 2004). Thus, just because the government may believe that something has been procured by fraud does not mean that the person using it or in possession of it automatically loses any expectation of privacy.

Lastly, the government refers generally to ISP service agreements, relying specifically upon a portion of the Yahoo! terms of service. That Yahoo! informs its account holders that it may access and disclose "Content" for certain limited purposes, including to comply with legal process, is not controlling for purposes of determining the requirements of the Fourth Amendment with respect to ISP-stored email. The terms of service are, at most, contractual agreements between private parties which cannot and do not confer any rights on the government or render

constitutional conduct by the government which would otherwise be unconstitutional. Whatever the provisions of the terms of service, the government must still conduct itself in accordance with the law. If the Fourth Amendment requires a warrant, the fact that Yahoo! has announced to its subscribers that it will access "Content" to comply with legal process other than a warrant is irrelevant.²⁶

United States v. Miller, 425 U.S. 435 (1976), USB35, does not support the government's position. In *Miller*, the checks obtained via subpoena to the banks were "not confidential communications but negotiable instruments to be used in commercial transactions." *Id.* at 442. The other documents obtained "contain[ed] only information voluntarily conveyed to the banks and exposed to their employees *in the ordinary course of business.*" *Id.* (emphasis added). Nothing in the Yahoo! terms of service indicates that the content of subscriber emails is routinely exposed to Yahoo! employees. Indeed, to the extent that ISPs "access" their customers' email, such "access" is generally accomplished through computerized processes, *without* human

26

Implicit in the terms of service is that the process be lawful. For example, Yahoo! declined to comply with the §2703 order in this case because the SCA, as construed in *Theofel*, see note 2, *supra*, requires a warrant for emails in electronic storage for less than 181 days which had been opened by the subscriber. See *Freedman v. America Online, Inc.*, 325 F.Supp.2d 638, 644 (E.D.Va. 2000)(AOL conceded that it violated the law when it disclosed subscriber information in response to an unsigned warrant application):

scrutiny of the content of private emails. There is, for example, no reason to believe – and the government has suggested none – that any human being at Yahoo! ever read the content of Warshak’s emails in the process of retrieving them for delivery to the government. *See United States v. Bach*, 310 F.3d 1063, 1065 (8th Cir. 2002)(noting that when executing §2703 warrants, Yahoo! technicians do not review the contents of the account).

D. The District Court Properly Applied The Remaining Factors Governing Whether a Preliminary Injunction Should Enter.

1. Irreparable injury to Warshak.

In arguing that Warshak will not be irreparably injured in the absence of a preliminary injunction, the government relies in large measure on the same arguments it advanced in support of its contention that Warshak lacked standing to seek a preliminary injunction; those arguments should be rejected for all the reasons addressed in Section I(A)(2), *supra*. Judge Dlott correctly concluded that “the prospective harm in this case is far from ‘speculative’ or ‘unsubstantiated’ under [*Abney v. Amgen, Inc.*, 443 F.3d 540 (6th Cir. 2006)].” R21, Order, JA ___-___. Certainly, on the record before her, it was not an abuse of discretion to so conclude.

Contrary to the government’s argument, USB53-54, Warshak has no adequate

remedy at law against future violations of his Fourth Amendment rights. The *only* remedy which is adequate is one which will *prevent* the government from unconstitutionally invading the privacy of private email correspondence. After-the-fact awards of damages or suppression of evidence may penalize the government for its unlawful conduct, but such remedies can never restore the privacy of the communications read by government agents.

The government's argument that it cannot again secretly seize the contents of Warshak's emails unless a court authorizes a §2703(d) order and also authorizes deprivation of notice, USB53, "simply begs the constitutional question: 2703's existing safeguards are legally adequate only to the extent they pass muster under the Fourth Amendment, and the [district court] . . . found a substantial likelihood that they do not." R21, Order, JA ___. Absent the preliminary injunction, there is no guarantee that Warshak would receive prior notice of future applications for §2703(d) orders. *See* USB53-54. Just as the government has remained unwilling to provide any assurance that it would not again seek to obtain Warshak's emails through the use of secret §2703 process, it is even now unwilling to state that it would provide Warshak with advance notice when it does so. The district court did not abuse its discretion in concluding that the preliminary injunction was necessary to prevent irreparable injury to Warshak.

2. Lack of substantial injury to the government.

The only "injury" that the government will suffer is its inability to continue its practice of seeking unconstitutional orders, in secret and at great expense to the legitimate privacy expectations of the residents of the Southern District of Ohio. If the preliminary injunction is impeding criminal investigations, as the government contends, USB54-55, then that is as it should be: if a law enforcement practice is unconstitutional – as the use of *ex parte* §2703(d) orders to seize and search the content of private email correspondence is – the government may not utilize it, no matter how much more efficiently it could investigate crime if the unlawful practice were available to it.

The needs of law enforcement stand in constant tension with the Constitution's protections of the individual against certain exercises of official power. It is precisely the predictability of these pressures that counsels a resolute loyalty to constitutional safeguards.

Almeida-Sanchez v. United States, 413 U.S. 266, 273 (1973). The preliminary injunction properly prevents the government from investigating crime in a manner which violates the Fourth Amendment.

The government's irreparable injury argument ignores the fact that it remains free to gain *ex parte* access to the content of emails under §2703 if it has probable cause to believe that the emails would provide evidence of a crime and obtains the

emails under a duly issued search warrant. In addition, the government has at its disposal §2703(f), which allows it to require an ISP to preserve emails pending a court order or other process – an intermediate remedy that all but extinguishes any potential for substantial injury. While the government of course prefers that it be able to execute §2703 process in secret, the balance struck by the preliminary injunction ensures that residents of the Southern District of Ohio will not have the privacy of their email correspondence invaded by the government without a warrant issued upon a showing of probable cause unless they have the prior opportunity to assert in advance their Fourth Amendment rights, thus ensuring, in the only way possible, that the government will be able to search the content of private emails only insofar as such a search is consistent with the commands of the Fourth Amendment. Being unable to violate the Fourth Amendment is not a cognizable injury to the government.

3. The public interest.

As Judge Dlott correctly concluded, “it is always in the public interest to prevent violation of a party’s constitutional rights.” R21, Order, JA ____. The right to be free from unlawful government seizures and searches, which is perhaps at its zenith where governmental searches of private correspondence are concerned, lies at the heart of the protections guaranteed by the Fourth Amendment. While the public certainly has an interest in the investigation of potential criminality by *lawful* means,

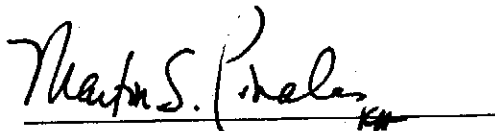
that interest does not extend to the use by the government of investigative methods which violate the Fourth Amendment. The unsuspecting public would be shocked and appalled at the power which the government claims to invade their private email without notice and without probable cause to believe that the individual is involved in wrongdoing or that his email would provide evidence of a crime. The public interest lies squarely on the side of preventing such incursions upon fundamental constitutional protections, yet these constitutional violations will continue unabated in the absence of the preliminary injunction. The public interest weighs heavily indeed in favor of maintaining the preliminary injunction in full force and effect.

CONCLUSION

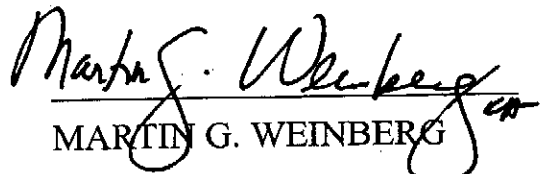
For all the foregoing reasons, this Court should uphold the preliminary injunction.

Respectfully submitted,

By his attorneys,



MARTIN S. PINALES
SIRKIN, PINALES & SCHWARTZ LLP
105 West Fourth Street, Suite 920
Cincinnati, Ohio 45202
(513) 721-4876



MARTIN G. WEINBERG
20 Park Plaza, Suite 905
Boston, Massachusetts 02116
(617) 227-3700

ON BRIEF:

KIMBERLY HOMAN

20 Park Plaza, Suite 905

Boston, Massachusetts 02116

(617) 227-8616

DESIGNATION OF JOINT APPENDIX CONTENTS

Pursuant to Rule 30(b) of the Rules of the Sixth Circuit, Plaintiff-Appellee Steven Warshak hereby designates the following items for inclusion in the Joint Appendix, in addition to those already designated by the Defendant-Appellant:

<u>Document</u>	<u>Record Number</u>
Warshak's Post-Argument Reply to Government Opposition to Motion for Issuance of a Temporary Restraining Order and/or Preliminary Injunction, July 5, 2006	16
United States' Motion to Stay Pending Appeal, August 16, 2006	27
Memorandum in Opposition to Plaintiff's Motion to Unseal Pertinent Case Files, August 29, 2006	36

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

No. 06-4092

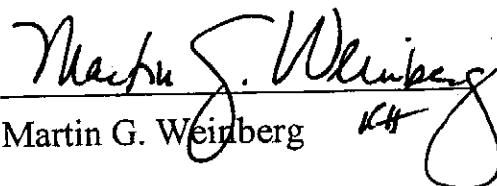
STEVEN WARSHAK,
Plaintiff-Appellee

v.

UNITED STATES OF AMERICA,
Defendant-Appellant

CERTIFICATE OF COMPLIANCE WITH TYPEFACE AND LENGTH
LIMITATIONS

This Brief complies with the type-volume requirements of Fed. R. App. P.
32(a)(7)(C)(i). This Brief has was prepared using WordPerfect 12.0, 14-point Times
New Roman and contains 13, 993 words.

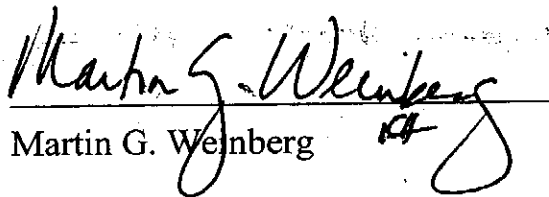

Martin G. Weinberg *KG*

CERTIFICATE OF SERVICE

I, Martin G. Weinberg, hereby certify that the foregoing Proof Brief of Plaintiff-Appellee Steven Warshak was served this 13th day of November, 2006, by first-class mail, postage prepaid, upon the following attorneys for the United States:

Donetta D. Wiethe
Benjamin C. Glassman
Assistant United States Attorneys
221 E. 4th Street, Suite 400
Cincinnati, Ohio 45202

John H. Zacharia
Nathan P. Judish
U.S. Department of Justice
1301 New York Ave., N.W., Suite 600
Washington, D.C. 20005


Martin G. Weinberg