RECOMMENDED FOR FULL-TEXT PUBLICATION
Pursuant to Sixth Circuit Rule 206

File Name: 07a0225p.06

UNITED STATES COURT OF APPEALS

FOR THE SIXTH CIRCUIT

STEVEN WARSHAK, *Plaintiff-Appellee,*	]	
v.	]	No. 06-4092
UNITED STATES OF AMERICA, *Defendant-Appellant.*	]	

Appeal from the United States District Court
for the Southern District of Ohio at Cincinnati.
No. 06-00357—Susan J. Dlott, District Judge.

Argued: April 18, 2007

Decided and Filed: June 18, 2007

Before: MARTIN and DAUGHTREY, Circuit Judges; SCHWARZER, District Judge.[*]

COUNSEL

ARGUED: Nathan P. Judish, UNITED STATES DEPARTMENT OF JUSTICE, Washington, D.C., for Appellant. Martin G. Weinberg, Boston, Massachusetts, for Appellee. **ON BRIEF:** Nathan P. Judish, John H. Zacharia, UNITED STATES DEPARTMENT OF JUSTICE, Washington, D.C., Benjamin C. Glassman, Donetta D. Wiethe, ASSISTANT UNITED STATES ATTORNEYS, Cincinnati, Ohio, for Appellant. Martin G. Weinberg, Boston, Massachusetts, Martin S. Pinales, SIRKIN, PINALES & SCHWARTZ, Cincinnati, Ohio, for Appellee. Kevin S. Bankston, ELECTRONIC FRONTIER FOUNDATION, San Francisco, California, Patricia L. Bellia, NOTRE DAME LAW SCHOOL, Notre Dame, Indiana, Susan A. Freiwald, UNIVERSITY OF SAN FRANCISCO SCHOOL OF LAW, San Francisco, California, for Amici Curiae.

OPINION

BOYCE F. MARTIN, JR., Circuit Judge. The government appeals the district court's entry of a preliminary injunction, prohibiting it from seizing "the contents of any personal e-mail account maintained by an Internet Service Provider in the name of any resident of the Southern District of Ohio without providing the relevant account holder or subscriber prior notice and an opportunity to be heard on any complaint, motion, or other pleading seeking issuance of such an order." D. Ct.

---

[*] The Honorable William W Schwarzer, United States District Judge for the Northern District of California, sitting by designation.

Op. at 19. For the reasons discussed below, we largely affirm the district court's decision, requiring only that the preliminary injunction be slightly modified on remand.

I.

In March 2005, the United States was engaged in a criminal investigation of Plaintiff Steven Warshak and the company he owned, Berkeley Premium Nutraceuticals, Inc. The investigation pertained to allegations of mail and wire fraud, money laundering, and related federal offenses. On May 6, 2005, the government obtained an order from a United States Magistrate Judge in the Southern District of Ohio directing internet service provider ("ISP") NuVox Communications to turn over to government agents information pertaining to Warshak's e-mail account with NuVox. The information to be disclosed included (1) customer account information, such as application information, "account identifiers," "[b]illing information to include bank account numbers," contact information, and "[any] other information pertaining to the customer, including set up, synchronization, etc."; (2) "[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 Warshak; and (3) "[a]ll Log files and backup tapes." Joint App'x at 49.

The order stated that it was issued under 18 U.S.C. § 2703, part of the Stored Communications Act ("SCA"), and that it was based on "specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation." The order was issued under seal, and prohibited NuVox from "disclos[ing] the existence of the Application or this Order of the Court, or the existence of this investigation, to the listed customer or to any person unless and until authorized to do so by the Court." The magistrate further ordered that "the notification by the government otherwise required under 18 U.S.C. § 2703(b)(1)(B) be delayed for ninety days." On September 12, 2005, the government obtained a nearly identical order pertaining to Yahoo, another ISP, that sought the same types of information from Warshak's Yahoo e-mail account and a Yahoo account identified with another individual named Ron Fricke.

On May 31, 2006, over a year after obtaining the NuVox order, the United States wrote to Warshak to notify him of both orders and their requirements.[1] The magistrate had unsealed both orders the previous day. Based on this disclosure, Warshak filed suit on June 12, 2006, seeking declaratory and injunctive relief, and alleging that the compelled disclosure of his e-mails without a warrant violated the Fourth Amendment and the SCA. After filing the complaint, Warshak's counsel sought the government's assurance that it would not seek additional orders under section 2703(d) directed at his e-mails, at least for some discrete period of time during the pendency of his civil suit. The government declined to provide any such assurance. In response, Warshak moved for a temporary restraining order and/or a preliminary injunction prohibiting such future searches. The district court held a telephonic hearing on the motions, and eventually granted part of the equitable relief sought by Warshak.

In considering the factors for a preliminary injunction, the district court reasoned that e-mails held by an ISP were roughly analogous to sealed letters, in which the sender maintains an expectation of privacy. This privacy interest requires that law enforcement officials obtain a warrant, based on a showing of probable cause, as a prerequisite to a search of the e-mails. Because it viewed Warshak's constitutional claim as meritorious, the district court deemed it unnecessary to examine his likelihood of success on the SCA claim. It also found that Warshak would suffer irreparable harm based on any additional constitutional violations, that such harm was imminent in

[1]The government has conceded that it violated the statute by waiting for over a year without providing notice of the e-mail seizures to Warshak or seeking extensions of the delayed notification period, and it appears to have violated the magistrate's decision for the same reason.

light of the government's past violations and its refusal to agree not to conduct similar seizures in the future, that Warshak lacked an adequate remedy at law to protect his Fourth Amendment rights, and that the public interest in preventing constitutional violations weighed in favor of the injunction. The district court also made clear that further factual development would be necessary for a final disposition, and that the injunction was tailored to protect Warshak from constitutional violations in the interim.

The district court rejected the full scope of Warshak's request to enjoin the government from seizing any of his e-mails in the future. It stated that it was not "presently prepared to hold that 18 U.S.C. § 2703(d) facially violates the Fourth Amendment by simple virtue of the fact that it authorizes the seizure of personal e-mails from commercial ISPs without a warrant and on less than a showing of probable cause." D. Ct. Op. at 16-17. The statute's authorization of this procedure based only on the government's *ex parte* representations struck the district court as more problematic, however, and it held that the "combination of a standard of proof less than probable cause and potentially broad *ex parte* authorization cannot stand." *Id*. at 17. As a result, it deemed the constitutional flaws of the statute "facial in nature," and agreed to preliminarily enjoin additional seizures of e-mails from an ISP account of any resident of the Southern District of Ohio without notice to the account holder and an opportunity for a hearing.

The gist of this remedy appears to be that when a hearing is required and the e-mail account holder is given an opportunity in court to resist the disclosure of information, any resulting order is more like a subpoena than a search warrant. Therefore the standard necessary to obtain an order under the SCA — that the government introduce "specific and articulable facts showing that there are reasonable grounds to believe that the contents" of the e-mail to be seized "are relevant and material to an ongoing criminal investigation" — is permissible as the functional equivalent of a subpoena given the subject's ability to contest the order in court. Because this standard is lower than the probable cause standard necessary to obtain a search warrant, it is sufficient to justify a warrantless search only in instances where notice is provided to the account holder.

The government appeals from the district court's ruling.

II.

The SCA, passed by Congress in 1986, is codified at 18 U.S.C. §§ 2701 to 2712, and contains a number of provisions pertaining to the accessibility of "stored wire and electronic communications and transactional records." Portions of the SCA that are not directly at stake here prohibit unauthorized access of electronic communications (§ 2701) and prohibit a service provider from divulging the contents of electronic communications that it is storing for a customer with certain exceptions pertaining to law enforcement needs (§ 2702). At issue in this case is § 2703, which provides procedures through which a governmental entity can access both user records and other subscriber information, and the content of electronic messages.

Subsection (a) requires the use of a warrant to access messages that have been in storage for 180 days or less. Subsection (b) provides that to obtain messages that have been stored for over 180 days, the government generally must either (1) obtain a search warrant, (2) use an administrative subpoena, or (3) obtain a court order. The latter two require prior notice to the subscriber, allowing the subscriber an opportunity for judicial review before the disclosure:

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

> (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or
>
> (B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity--
>
> (i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or
>
> **(ii) obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2705 of this title.**

18 U.S.C. 2703(b) (emphasis added). The final subsection cited here contains the exception to the requirement that the government must either provide notice to the subscriber if seeking either an SCA order or an administrative subpoena, or must, in the absence of notice, obtain a search warrant. This exception, which allows for delayed notice under section 2705, is the root of the present controversy.

Subsection (d), which is referenced in subsection (b), sets forth the procedure and requirements for obtaining a court order (as opposed to a warrant):

> A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

18 U.S.C. 2703(d). The parties agree that the standard of proof for a court order — "specific and articulable facts showing that there are reasonable grounds to believe that the contents . . . or records . . . are relevant and material to an ongoing criminal investigation" — falls short of probable cause.

Section 2705, which provides for delayed notice of a 2703(d) court order, states in relevant part:

> (a) Delay of notification.
>
> (1) A governmental entity acting under section 2703(b) of this title may--
>
> (A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703(b) of this title for a period not to exceed ninety days, if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or
>
> (B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703(b) of this title for a period not to exceed ninety days upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.

> (2) An adverse result for the purposes of paragraph (1) of this subsection is--
> (A) endangering the life or physical safety of an individual;
> (B) flight from prosecution;
> (C) destruction of or tampering with evidence;
> (D) intimidation of potential witnesses; or
> (E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.
>
> * * * * *
>
> (4) Extensions of the delay of notification provided in section 2703 of up to ninety days each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subsection (b) of this section.
> (5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first-class mail to, the customer or subscriber a copy of the process or request together with notice that--
> (A) states with reasonable specificity the nature of the law enforcement inquiry; and
> (B) informs such customer or subscriber--
> (i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;
> (ii) that notification of such customer or subscriber was delayed;
> (iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and
> (iv) which provision of this chapter allowed such delay.

Subsection (b) of section 2705 similarly allows the government to obtain a court order prohibiting the ISP from notifying the account holder "of the existence of the warrant, subpoena, or court order," when the government is not required to provide him notice. These provisions of sections 2703 and 2705 largely govern the seizures of Warshak's e-mails.[2]

The injunctive relief imposed by the district court has a specific narrow application to portions of the SCA. It would still allow seizures of e-mails pursuant to a warrant or with prior notice to a subscriber. The portions that it enjoins are the exception provided in section 2703(b)(1)(B)(ii), which allows for a court order with delayed notice to the account holder, and the

---

[2] Although the remaining subsections of 2703 are not directly relevant to Warshak's present challenge, they are nevertheless informative. Subsection (c) provides a different and somewhat broader procedure by which the government may obtain records and other subscriber information, as opposed to the content of electronic messages. In addition to allowing a governmental entity to obtain such records with a warrant, a court order, or with the subscriber's consent, the statute provides for mandatory disclosure of particular subscriber records, such as name, address, telephone connection records, session times and durations, network identifying information, and means of payment for services. *See* 18 U.S.C. § 2703(c). Also noteworthy is subsection (f), which requires a provider to preserve evidence when requested by a governmental entity. This mechanism is designed to assist law enforcement in cases where they are required to provide notice to the subscriber but are concerned that he might destroy evidence prior to its seizure:

> (f) Requirement to preserve evidence.
> (1) In general. A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.
> (2) Period of retention. Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

procedures provided in section 2705, which are incorporated by reference into section 2703(b)(1)(B)(ii).

III.

The government focuses on four issues in challenging the preliminary injunction. First, it argues that Warshak's claims are not justiciable in the first instance, based on the doctrines of standing and ripeness. Second, it contends that the Fourth Amendment's probable cause standard is inapplicable in the context of SCA seizures, which it likens to compelled disclosures. This issue primarily covers Warhsak's likelihood of success on the merits, the first factor in the preliminary injunction analysis. Next, it argues that Warshak's claims are not the proper subject of a facial challenge to the provisions of the SCA in question. Finally, it challenges the district court's balancing of the remaining preliminary injunction factors.

We review a district court's decision regarding a preliminary injunction for an abuse of discretion. *Overstreet v. Lexington-Fayette Urban County Gov't*, 305 F.3d 566, 573 (6th Cir. 2002). Four factors must be considered and balanced by the district court in making its determination: "(1) whether the plaintiff has established a substantial likelihood or probability of success on the merits; (2) whether there is a threat of irreparable harm to the plaintiff; (3) whether issuance of the injunction would cause substantial harm to others; and (4) whether the public interest would be served by granting injunctive relief." *Nightclubs, Inc. v. City of Paducah*, 202 F.3d 884, 888 (6th Cir. 2000) (overruled on other grounds, *City of Littleton v. Z. J. Gifts D-4, L.L.C.*, 541 U.S. 774, 784 (2004)). "'The district court's determination will be disturbed only if the district court relied upon clearly erroneous findings of fact, improperly applied the governing law, or used an erroneous legal standard.'" *Id.* (quoting *Connection Distrib. Co. v. Reno*, 154 F.3d 281, 288 (6th Cir. 1998)).

We review de novo the legal questions of standing and ripeness. *See Prime Media v. City of Brentwood*, No. 05-6343, 2007 U.S. App. LEXIS 10862, at *9 (6th Cir. May 8, 2006).

A. Standing and Ripeness

1. Standing

The government first asserts that the district court lacked subject matter jurisdiction to entertain Warshak's claims, both because Warshak lacked standing to challenge future searches under the SCA, and because his claims were not ripe for review. To establish standing, a plaintiff must allege "(1) an injury that is (2) 'fairly traceable to the defendant's allegedly unlawful conduct' and that is (3) 'likely to be redressed by the requested relief.'" *Id.* at *11 (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992)). Where a plaintiff seeks injunctive relief, a natural outgrowth of these factors requires a showing of ongoing injury or an imminent threat of future injury. *See O'Shea v. Littleton*, 414 U.S. 488, 495-96 (1974) ("Past exposure to illegal conduct does not in itself show a present case or controversy regarding injunctive relief . . . if unaccompanied by any continuing, present adverse effects."); *but see Los Angeles v. Lyons*, 461 U.S. 95, 102 (1983) ("Past wrongs [are] evidence bearing on 'whether there is a real and immediate threat of repeated injury.'" (quoting *O'Shea*, 414 U.S. at 495-96)). Although past harm to a plaintiff seeking injunctive relief can serve as relevant evidence, he must also show a threat that is "sufficiently real and immediate" to establish the "prospect of future injury" as part of the standing requirement. *Lyons*, 461 U.S. at 102-103 (1983) (citing *O'Shea*, 414 U.S. at 496-97). The district court found that Warshak showed a sufficient threat of imminent harm, in light of the past seizures of his e-mails and the fact that the government "refused to pledge not to obtain or enforce future 2703(d) orders of this kind against other e-mail accounts of Warshak's." D. Ct. Op. at 12.

The government relies primarily upon *Lyons* to support its contention that Warshak's claims are largely hypothetical, and do not support a showing of imminent harm. In *Lyons*, the plaintiff

sought injunctive relief against the use of chokeholds by Los Angeles police after he had been put in a chokehold himself. 461 U.S. at 105. The Supreme Court determined that the plaintiff had failed to demonstrate any future harm upon which he would have standing to seek injunctive relief, because there was no imminent threat that he would be subjected to a chokehold again. *Id*. at 107. Among other things, the plaintiff could not show that the city had a policy authorizing the use of chokeholds or that all Los Angeles police always used chokeholds, and the Court was unwilling to assume that the plaintiff would voluntarily break the law again and be involved in a confrontation with police. *Id*. at 111 ("The speculative nature of Lyons' claim of future injury requires a finding that this prerequisite of equitable relief has not been fulfilled.").

Warshak's claims are distinguishable from those in *Lyons* for several reasons. First, unlike in *Lyons*, the government clearly has a policy of seizing e-mails — the very practice that Warshak alleges is unconstitutional. There is no dispute about the existence of this policy: not only have Warshak's e-mails been seized twice pursuant to the policy, and not only has the government refused to abstain from future seizures, but a statute explicitly authorizes the challenged government action. The presence of this policy and its applicability to Warshak are likely sufficient on their own to give Warshak standing to seek equitable relief. *See Lyons*, 461 U.S. at 105-06 ("In order to establish an actual controversy in this case, Lyons would have had not only to allege that he would have another encounter with the police but also to make the incredible assertion either (1) that all police officers in Los Angeles always choke any citizen with whom they happen to have an encounter, whether for the purpose of arrest, issuing a citation, or for questioning, **or (2) that the City ordered or authorized police officers to act in such manner**." (emphasis added)); *see also Baur v. Veneman*, 352 F.3d 625, 637 (2d Cir. 2003) (citing "alleged risk of harm aris[ing] from an established government policy" as a "critical factor that weigh[s] in favor of concluding that standing exists . . . ."); *31 Foster Children v. Bush*, 329 F.3d 1255, 1266 (11th Cir. 2003) ("[F]uture injury that depends on either the random or unauthorized acts of a third party is too speculative to satisfy standing requirements. However, when the threatened acts that will cause injury are authorized or part of a policy, it is significantly more likely that the injury will occur again.").

Further, although Warshak, like Lyons, finds himself in a confrontation with the government due to allegations of illegal conduct on his part, the nature of the confrontation is very different. Warshak has been subject to a lengthy, ongoing investigation, and even if it is prompted by suspicion of illegal conduct on his part, the ongoing nature of the investigation is clearly distinguishable from the brief encounter at issue in *Lyons*. Warshak's fear of the challenged government conduct need not be premised on a showing that he will resist arrest, attempt to escape from police custody, or otherwise engage in a physical confrontation with police, as the *Lyons* plaintiff would have had to show. Instead, the challenged conduct here involves an investigation during which the government might seek to seize additional e-mails at any time. Although Warshak has now been indicted, and the investigation is at a different and less secretive stage, the government would certainly want to search more of his e-mails if it had reason to believe that they might be incriminating. The brief and somewhat random nature of the confrontation in *Lyons* distinguishes it from the ongoing, targeted confrontation here. The government points out that there is no way to determine with any degree of certainty that it will seek such seizures in the future, but as Warshak argues, "[o]ne does not have to await consummation of threatened injury to obtain preventive relief." *Blum v. Yaretsky*, 457 U.S. 991, 1000 (1982).

In light of the past e-mail seizures, the ongoing nature of the investigation against Warshak, and the government policy of seizing e-mails without a warrant or notice to the account holder, we agree with the district court that Warhsak has shown a sufficiently imminent threat of future injury to meet the injury in fact element of standing under *Lyons*.

As Warshak has shown an imminent threat of injury, this threat would clearly be redressed by the injunctive relief issued by the district court, because the government would be prohibited

from repeating its allegedly unconstitutional conduct in the future. Although the government argues that the redressability requirement has not been met, its argument on this issue is subsumed by the imminent threat of injury inquiry, as it asserts that there is no redressability because there is no threatened future injury. The redressability requirement does not, therefore, present an independent basis for us to find a lack of standing.

2. Ripeness

The government also argues that Warshak's claims are not ripe, as they are too hypothetical without a pending order directed at his e-mails. The ripeness inquiry focuses on three factors: (1) the "likelihood that the harm alleged by [the] plaintiffs will ever come to pass"; (2) "whether the factual record is sufficiently developed to produce a fair adjudication of the merits of the parties' respective claims"; and (3) "the hardship to the parties if judicial relief is denied at [this] stage in the proceedings." *Adult Video Ass'n v. United States Dept. of Justice*, 71 F.3d 563, 568 (6th Cir. 1995) (internal citations omitted). As this Court has explained, "[t]he ripeness doctrine generally applies in cases . . . in which a party seeks a declaratory judgment based on pre-enforcement review of a statute or regulation . . . ." *Kardules v. City of Columbus*, 95 F.3d 1335, 1343 (6th Cir. 1996).

The government contends that because Warshak challenges future e-mail seizures that he cannot prove will occur again, his claims are too hypothetical to be ripe. Warshak's claim is distinguishable from the typical ripeness case, however, because he has suffered past alleged injuries from the exact conduct that he seeks to have enjoined, and because the ongoing nature of the investigation against him raises the likelihood of these harms occurring again. To a large extent, the first ripeness factor — the likelihood that alleged harm will ever come to pass — is quite similar to the standing requirement of an imminent threatened injury. *Adult Video Ass'n.*, 71 F.3d at 567 ("[T]he ripeness doctrine not only depends on the finding of a case and controversy and hence jurisdiction under Article III, but it also requires that the court exercise its discretion to determine if judicial resolution would be desirable under all of the circumstances.") (quoting *Brown v. Ferro Corp.*, 763 F.2d 798, 801 (6th Cir. 1985)). The past alleged injuries and our finding of a continued threat of injury would suggest that Warshak meets the first ripeness prong.

If the government's practice was to notify Warshak prior to seeking seizure of his e-mails, the second and third ripeness factors might support a determination that his claims are not ripe. In the context of administrative law, for example, a legal challenge is often unripe before a final agency decision, in part because a better developed legal challenge can be brought at that time. *See, e.g.*, *Ohio Forestry Ass'n v. Sierra Club*, 523 U.S. 726, 734 (1998) ("The Sierra Club thus will have ample opportunity later to bring its legal challenge at a time when harm is more imminent and more certain."). Here, however, the government's *ex parte* approach to obtaining Warshak's e-mails precludes the possibility of judicial review at a subsequent and more appropriate time. Thus, as Warshak points out, he will likely suffer the hardship of continuing to have his Fourth Amendment rights violated with limited legal recourse if his current claims are deemed unripe. Further, with respect to the second factor, the past seizures of his e-mails present an adequate factual basis on which to assess the government's conduct. Although future seizures, and not the past incidents, are those upon which Warshak's challenge is focused, the likely similarity renders them a sufficient backdrop for judicial review.

The government's elusive practices have themselves limited Warshak's abilities to seek redress for future constitutional violations in any other manner. Further, the past alleged Constitutional violations have demonstrated that the challenged conduct is at least not hypothetical. The government has not identified a single case where either standing or ripeness were found lacking where the plaintiff alleged multiple past constitutional violations, a statute explicitly condoned similar alleged violations in the near future, the threat of such violations continued in light of pending charges against the subject of the violation, and the government insisted on its

prerogative to continue the challenged conduct. Nor do we believe that any reading of the precedents of this Court or the Supreme Court can support such a result. For these reasons, we affirm the district court's determination that Warshak's claims are justiciable, and proceed to consider them on the merits.

B. Likelihood of Success on the Merits: Probable Cause versus Reasonableness and Fourth Amendment Implications of SCA Orders

1. Probable Cause versus Reasonableness

With respect to the merits of the preliminary injunction, the government argues that court orders issued under section 2703 are not searches but rather compelled disclosures, akin to subpoenas. As a result, according to the government, the more stringent showing of probable cause, a prerequisite to the issuance of a warrant under the Fourth Amendment, is inapplicable, and an order under section 2703 need only be supported by a showing of "reasonable relevance."

The government is correct that "whereas the Fourth Amendment mandates a showing of probable cause for the issuance of search warrants, subpoenas are analyzed only under the Fourth Amendment's general reasonableness standard." *Doe v. United States*, 253 F.3d 256, 263-64 (6th Cir. 2001). As this Court has explained, "[o]ne primary reason for this distinction 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 being enforced." *Id*. at 264 (quoting *In Re Subpoena Duces Tecum*, 228 F.3d 341, 347-49 (4th Cir. 2000)); *see also Donovan v. Lone Steer*, 464 U.S. 408, 415 (1984). The government is also correct that this principle extends to subpoenas to third-parties — that is, entities other than the subject of the investigation, like NuVox and Yahoo in this case. *See United States v. Phibbs*, 999 F.2d 1053, 1077 (6th Cir. 1993).

Phibbs makes explicit, however, a necessary Fourth Amendment caveat to the rule regarding third-party subpoenas: the party challenging the subpoena has "standing to dispute [its] issuance on Fourth Amendment grounds" if he can "demonstrate that he had a legitimate expectation of privacy attaching to the records obtained." *Id*.; *see also United States v. Miller*, 425 U.S. 435, 444 (1976) ("**Since no Fourth Amendment interests of the depositor are implicated here**, this case is governed by the general rule that the issuance of a subpoena to a third party to obtain the records of that party does not violate the rights of a defendant." (emphasis added)). This language reflects the rule that where the party challenging the disclosure has voluntarily disclosed his records to a third party, he maintains no expectation of privacy in the disclosure vis-a-vis that individual, and assumes the risk of that person disclosing (or being compelled to disclose) the shared information to the authorities. *See, e.g., United States v. Jacobsen*, 466 U.S. 109, 117 (1984) ("[W]hen an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information.").

Combining this disclosure to a third party with the government's ability to subpoena the third party alleviates any need for the third-party subpoena to meet the probable cause requirement, if the challenger has not maintained an expectation of privacy with respect to the individual being compelled to make the disclosure. For example, in *Phibbs*, the documents in question were credit card and phone records that were "readily accessible to employees during the normal course of business." 999 F.2d at 1078. A similar rationale was employed by the Supreme Court in *Miller*. 425 U.S. at 442 ("The checks are not confidential communications but negotiable instruments to be used in commercial transactions. All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."). *See also SEC v. Jerry T. O'Brien, Inc*., 467 U.S.

735, 743 (1984) ("When a person communicates information to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information or records thereof to law enforcement authorities."). The government's compelled disclosure argument, while relevant, therefore begs the critical question of whether an e-mail user maintains a reasonable expectation of privacy in his e-mails vis-a-vis the party who is subject to compelled disclosure — in this instance, the ISPs. If he does not, as in *Phibbs* or *Miller*, then the government must meet only the reasonableness standard applicable to compelled disclosures to obtain the material. If, on the other hand, the e-mail user does maintain a reasonable expectation of privacy in the content of the e-mails with respect to the ISP, then the Fourth Amendment's probable cause standard controls the e-mail seizure.

2. Reasonable expectation of privacy in e-mail content

Two amici curiae convincingly analogize the privacy interest that e-mail users hold in the content of their e-mails to the privacy interest in the content of telephone calls, recognized by the Supreme Court in its line of cases involving government eavesdropping on telephone conversations. *See Smith v. Maryland*, 442 U.S. 735 (1979); *Katz v. United States*, 389 U.S. 347 (1967); *Berger v. New York*, 388 U.S. 41 (1967). In *Berger* and *Katz*, telephone surveillance that intercepted the content of a conversation was held to constitute a search, because the caller "is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world," and therefore cannot be said to have forfeited his privacy right in the conversation. *Katz*, 389 U.S. at 352. This is so even though "[t]he telephone conversation itself must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment." *Smith*, 442 U.S. at 746 (Stewart, J., dissenting). On the other hand, in *Smith*, the Court ruled that the use of pen register, installed at the phone company's facility to record the numbers dialed by the telephone user, did not amount to a search. This distinction was due to the fact that "a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications." 442 U.S. at 741 (emphasis in original).

The distinction between *Katz* and *Miller* makes clear that the reasonable expectation of privacy inquiry in the context of shared communications must necessarily focus on two narrower questions than the general fact that the communication was shared with another. First, we must specifically identify the party with whom the communication is shared, as well as the parties from whom disclosure is shielded. Clearly, under *Katz*, the mere fact that a communication is shared with another person does not entirely erode all expectations of privacy, because otherwise eavesdropping would never amount to a search. It is true, however, that by sharing communications with someone else, the speaker or writer assumes the risk that it could be revealed to the government by that person, or obtained through a subpoena directed to that person. *See Miller*, 425 U.S. at 443 ("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities."). The same does not necessarily apply, however, to an intermediary that merely has the ability to access the information sought by the government. Otherwise phone conversations would never be protected, merely because the telephone company can access them; letters would never be protected, by virtue of the Postal Service's ability to access them; the contents of shared safe deposit boxes or storage lockers would never be protected, by virtue of the bank or storage company's ability to access them.

The second necessary inquiry pertains to the precise information actually conveyed to the party through whom disclosure is sought or obtained. This distinction provides the obvious crux for the different results in *Katz* and *Smith*, because although the conduct of the telephone user in *Smith* "may have been calculated to keep the *contents* of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed." 442 U.S. at 743. Like the depositor in *Miller*, the caller in *Smith* "assumed the risk" of the phone company disclosing the records that he conveyed to it. *Id*. Yet this assumption of the risk is limited to the specific

information conveyed to the service provider, which in the telephone context excludes the content of the conversation. It is apparent, therefore, that although the government can compel disclosure of a shared communication from the party with whom it was shared, it can only compel disclosure of the specific information to which the subject of its compulsion has been granted access. It cannot, on the other hand, bootstrap an intermediary's limited access to one part of the communication (e.g. the phone number) to allow it access to another part (the content of the conversation).

This focus on the specific information shared with the subject of compelled disclosure applies with equal force in the e-mail context. Compelled disclosure of subscriber information and related records through the ISP might not undermine the e-mail subscriber's Fourth Amendment interest under *Smith*, because like the information obtained through the pen register in *Smith* and like the bank records in *Miller*, subscriber information and related records are records of the service provider as well, and may likely be accessed by ISP employees in the normal course of their employment. Consequently, the user does not maintain the same expectation of privacy in them vis-a-vis the service provider, and a third party subpoena to the service provider to access information that is shared with it likely creates no Fourth Amendment problems.[3] The combined precedents of *Katz* and *Smith*, however, recognize a heightened protection for the **content** of the communications. Like telephone conversations, simply because the phone company or the ISP **could** access the content of e-mails and phone calls, the privacy expectation in the content of either is not diminished, because there is a societal expectation that the ISP or the phone company will not do so as a matter of course.[4]

Similarly, under both *Miller* and *Katz*, if the government in this case had received the content of Warshak's e-mails by subpoenaing the person with whom Warshak was e-mailing, a Fourth Amendment challenge brought by Warshak would fail, because he would not have maintained a reasonable expectation of privacy vis-a-vis his e-mailing partners. *See Phibbs*, 999 F.2d at 1077. But this rationale is inapplicable where the party subpoenaed is not expected to access the content of the documents, much like the phone company in *Katz*. Thus, as Warshak argues, the government could not get around the privacy interest attached to a private letter by simply subpoenaing the postal service with no showing of probable cause, because unlike in *Phibbs*, postal workers would not be expected to read the letter in the normal course of business. *See Ex Parte Jackson*, 96 U.S. 727, 733 (1878) ("No law of Congress can place in the hands of officials connected with the postal service any authority to invade the secrecy of letters and such sealed packages in the mail; and all regulations adopted as to mail matter of this kind must be in subordination to the great principle embodied in the fourth amendment of the Constitution."). Similarly, a bank customer maintains an expectation of privacy in a safe deposit box to which the bank lacks access[5] (as opposed to bank records, like checks or account statements) and the government could not compel disclosure of the contents of the safe deposit box only by subpoenaing the bank.

---

[3]Indeed, the SCA itself largely tracks this distinction by making it easier for the government to obtain records and subscriber information than to obtain the content of e-mails. *Compare* 18 U.S.C. § 2703(c)(2) (requiring disclosure by ISP to government of account holder's basic identifying information as a matter of course and without notice to account holder) *with* 18 U.S.C. § 2703(b) (requiring warrant, subpoena, or court order to obtain "contents of any wire or electronic communication").

[4]As the Supreme Court explained in *Smith*, the reasonable expectation of privacy inquiry "embraces two discrete questions. The first is whether the individual, by his conduct, has exhibited an actual (subjective) expectation of privacy,— whether, in the words of the *Katz* majority, the individual has shown that he seeks to preserve [something] as private. The second question is whether the individual's subjective expectation of privacy is one that society is prepared to recognize as reasonable, — whether, in the words of the *Katz* majority, the individual's expectation, viewed objectively, is justifiable under the circumstances." 442 U.S. at 740 (internal citations and quotation marks omitted).

[5]*See United States v. Thomas*, No. 88-6341, 1989 U.S. App. LEXIS 9628, at *6 (6th Cir. July 5, 1989) ("Citizens have legitimate expectations of privacy in the contents of their safe deposit boxes.").

This analysis is consistent with other decisions that have addressed an individual's expectation of privacy in particular electronic communications. In *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2007), we concluded that users of electronic bulletin boards lacked an expectation of privacy in material posted on the bulletin board, as such materials were "intended for publication or public posting." Of course the public disclosure of material to an untold number of readers distinguishes bulletin board postings from e-mails, which typically have a limited, select number of recipients. *See also Jackson*, 96 U.S. at 733 ("[A] distinction is to be made between different kinds of mail matter, — between what is intended to be kept free from inspection, such as letters, and sealed packages subject to letter postage; and what is open to inspection, such as newspapers, magazines, pamphlets, and other printed matter, purposely left in a condition to be examined."). Although we stated that an e-mail sender would "lose a legitimate expectation of privacy in an e-mail that had already reached its recipient," analogizing such an e-mailer to "a letter-writer," this diminished privacy is only relevant with respect to the recipient, as the sender has assumed the risk of disclosure by or through the recipient. *Id*. at 333 (citing *United States v. King*, 55 F.3d 1193, 1196 (6th Cir. 1995)).[6] *Guest* did not hold that the mere use of an intermediary such as an ISP to send and receive e-mails amounted to a waiver of a legitimate expectation of privacy.

Other courts have addressed analogous situations where electronic communications were obtained based on the sender's use of a computer network. In *United States v. Simons*, the Fourth Circuit held that a government employee lacked a reasonable expectation of privacy in electronic files on his office computer, in light of the employer's policy that explicitly notified the employee of its intention to "audit, inspect, and monitor," his computer files. 206 F.3d 392, 398 (4th Cir. 2000). In light of this explicit policy, the employee's belief that his files were private was not objectively reasonable. *Id*. On the other hand, in *United States v. Heckenkamp*, the Ninth Circuit held that a university student did have a reasonable expectation of privacy in his computer files even though he "attached [his computer] to the university network," because the "university policies do not eliminate Heckenkamp's expectation of privacy in his computer." Nos. 05-10322, 10323, 2007 U.S. App. LEXIS 7806, at *12-13 (9th Cir. Apr. 5, 2007). Although the university did "establish limited instances in which university administrators may access his computer in order to protect the university's systems," this exception fell far short of a blanket monitoring or auditing policy, and the Ninth Circuit deemed it insufficient to waive the user's expectation of privacy.

Heckenkamp and *Simons* provide useful bookends for the question before us, regarding when the use of some intermediary provider of computer and e-mail services — be it a commercial ISP, a university, an employer, or another type of entity — amounts to a waiver of the user's reasonable expectation of privacy in the content of the e-mails with respect to that intermediary. In instances where a user agreement explicitly provides that e-mails and other files will be monitored or audited as in *Simons*, the user's knowledge of this fact may well extinguish his reasonable expectation of privacy. Without such a statement, however, the service provider's control over the files and ability to access them under certain limited circumstances will not be enough to overcome an expectation of privacy, as in *Heckenkamp*.

Turning to the instant case, we have little difficulty agreeing with the district court that individuals maintain a reasonable expectation of privacy in e-mails that are stored with, or sent or received through, a commercial ISP. The content of e-mail is something that the user "seeks to preserve as private," and therefore "may be constitutionally protected." *Katz*, 389 U.S. at 351. It goes without saying that like the telephone earlier in our history, e-mail is an ever-increasing mode

[6]Although the *Guest* panel did not explain the contours of this rule, the rule is apparent from *King*, the case it relied upon, in which the defendant's wife, the recipient of his letters, gave them to another individual who subsequently turned them over to the government. 55 F.3d at 1195. Because the letters were obtained through the recipient, against whom the defendant had maintained no privacy interest, we held that he could not raise a Fourth Amendment challenge to the disclosure. *Id*. at 1196.

of private communication, and protecting shared communications through this medium is as important to Fourth Amendment principles today as protecting telephone conversations has been in the past. *See Katz*, 389 U.S. at 352 ("To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.")

The government asserts that ISPs have the contractual right to access users' e-mails. The district court's ruling was based on its willingness to credit Warshak's contrary factual argument that "employees of commercial ISPs [do not] open and read — [nor do] their subscribers reasonably expect them to open and read — individual subscriber e-mails as a matter of course." D. Ct. Op. at 10-11. This factual determination tracks the language from *Miller* and *Phibbs* that suggests a privacy interest in records held by a third party is only undermined where the documents are accessed by the third party or its employees "in the ordinary course of business." *Miller*, 425 U.S. at 442. Moreover, as explained in the Ninth Circuit's decision in *Heckenkamp*, mere accessibility is not enough to waive an expectation of privacy. *See Heckenkamp*, 2007 U.S. App. LEXIS 7806 at *13 (holding that university policies establishing "limited instances in which university administrators may access [the user's] computer in order to protect the university's systems" was insufficient to eliminate an expectation of privacy); *see also Katz*, 389 U.S. at 351 ("[W]hat [a pay phone user] seeks to preserve as private, **even in an area accessible to the public**, may be constitutionally protected." (emphasis added)). Where a user agreement calls for regular auditing, inspection, or monitoring of e-mails, the expectation may well be different, as the potential for an administrator to read the content of e-mails in the account should be apparent to the user. *See Simons*, 206 F.3d at 398. Where there is such an arrangement, compelled disclosure by means of an SCA order directed at the ISP would be akin to the third party subpoena directed at a bank, as in *Miller* and *Jerry T. O'Brien*. In contrast, the terms of service in question here, which the government has cited to in both the district court and this Court, clearly provide for access only in limited circumstances, rather than wholesale inspection, auditing, or monitoring of e-mails.[7] Because the ISPs right to access e-mails under these user agreements is reserved for extraordinary circumstances, much like the university policy in *Heckenkamp*, it is similarly insufficient to undermine a user's expectation of privacy. For now, the government has made no showing that e-mail content is regularly accessed by ISPs, or that users are aware of such access of content.

The government also insists that ISPs regularly screen users' e-mails for viruses, spam, and child pornography. Even assuming that this is true, however, such a process does not waive an expectation of privacy in the content of e-mails sent through the ISP, for the same reasons that the terms of service are insufficient to waive privacy expectations. The government states that ISPs "are developing technology that will enable them to scan user images" for child pornography and viruses. The government's statement that this process involves "technology," rather than manual, human review, suggests that it involves a computer searching for particular terms, types of images, or similar indicia of wrongdoing that would not disclose the content of the e-mail to any person at the ISP or elsewhere, aside from the recipient. But the reasonable expectation of privacy of an e-mail user goes to the **content** of the e-mail message. The fact that a computer scans millions of e-mails for signs of pornography or a virus does not invade an individual's content-based privacy interest in the e-mails and has little bearing on his expectation of privacy in the content. In fact, these screening processes are analogous to the post office screening packages for evidence of drugs or explosives, which does not expose the content of written documents enclosed in the packages. The

[7]*See* Gov't Br. at 34 (citing Yahoo terms of service which allow access where "reasonably necessary to: (a) comply with legal process; (b) enforce the [Terms of Service]; (c) respond to claims that any Content violates the rights of third parties; (d) respond to your requests for customer service; or (e) protect the rights, property or personal safety of Yahoo!, its users and the public."). As amicus Electronic Frontier Foundation points out, each instance involves outside prompting for an ISP to review content, and does not occur in the normal course of business. This type of accessibility by the service provider was rejected as diminishing the expectation of privacy in *Katz*, as well as in *Heckenkamp*.

fact that such screening occurs as a general matter does not diminish the well-established reasonable expectation of privacy that users of the mail maintain in the packages they send.

It is also worth noting that other portions of the SCA itself strongly support an e-mail user's reasonable expectation of privacy in the content of his e-mails. Section 2701 prohibits unauthorized users from accessing e-mails. Section 2702 generally prohibits an ISP from disclosing e-mail content without the permission of the user. Further, section 2703 makes it easier for the government to get an order requiring the disclosure of records and subscriber information, in which the user does not maintain a privacy interest vis-a-vis the ISP, than to obtain an order requiring the disclosure of content. The statute also requires a warrant to search the content of e-mails that have been stored for 180 days or less. 18 U.S.C. 1703(a). Thus, even though the contested exception in section 2703(b) creates tension with the Fourth Amendment's requirements for a warrant, independent provisions support the proposition that a user maintains a reasonable expectation of privacy in the content of his e-mails.

The government's compelled disclosure argument is initially on point, but fails to address adequately the caveat relating to a party's maintenance of a reasonable expectation of privacy in documents in the custody of a third party. A warrant based on probable cause would not have been necessary had the government subpoenaed Warshak or given him prior notice of its intent to seek an SCA order, because the need for this higher showing would be offset by his ability to obtain judicial review before producing any e-mails. *See Phibbs*, 999 F.2d at 1077 ("The subpoena has to be 'sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance [would] not be unreasonable.' If it is a subpoena duces tecum, the government does not have to secure a judicial warrant before service is effectuated. Nonetheless, 'the subpoenaed party [must be able to] obtain judicial review of the reasonableness of the demand prior to suffering penalties for refusing to comply.'" (citing *See v. City of Seattle*, 387 U.S. 541, 544 (1967)). The same rationale would apply if the government subpoenaed a third party that had access to the content of the e-mails, and against whom Warshak had no claim of privacy, such as the recipient of one of his e-mails. By the same token, an SCA order that provided notice to the ISP alone, and not to the user, would be appropriate in the limited instances where the user had waived his expectation of privacy with respect to the ISP, such as where the government can show that auditing, monitoring, or inspection are expressly provided for in the terms of service, or where the user has e-mailed content directly to the ISP. Where the third party is not expected to access the e-mails in the normal course of business, however, the party maintains a reasonable expectation of privacy, and subpoenaing the entity with mere custody over the documents is insufficient to trump the Fourth Amendment warrant requirement.

The district court enjoined the United States "from seizing, pursuant to court order under 18 U.S.C. § 2703(d), the contents of any personal e-mail account maintained by an Internet Service Provider in the name of any resident of the Southern District of Ohio without providing the relevant account holder or subscriber prior notice and an opportunity to be heard . . . ." D. Ct. Op. at 19. Our discussion above necessitates one modification to this injunction, which counsel for Warshak agreed at oral argument would be appropriate. If the government can show, based on specific facts, that an e-mail account holder has waived his expectation of privacy vis-a-vis the ISP, compelled disclosure of e-mails through notice to the ISP alone would be appropriate. This is a narrow modification, however, as a right to access e-mails in an account only in certain limited circumstances would not be sufficient. Rather, the government must show that the ISP or other intermediary clearly established and utilized the right to inspect, monitor, or audit the content of e-mails, or otherwise had content revealed to it. In such cases the SCA order will operate as the functional equivalent of a third party subpoena, allowing disclosure through a party that has total access to the documents in question. On remand, therefore, the preliminary injunction shall allow seizures of e-mail in three situations: (1) if the government obtains a search warrant under the Fourth Amendment, based on probable cause and in compliance with the particularity requirement;

(2) if the government provides notice to the account holder in seeking an SCA order, according him the same judicial review he would be allowed were he to be subpoenaed; or (3) if the government can show specific, articulable facts, demonstrating that an ISP or other entity has complete access to the e-mails in question and that it actually relies on and utilizes this access in the normal course of business, sufficient to establish that the user has waived his expectation of privacy with respect to that entity, in which case compelled disclosure may occur if that entity is afforded notice and an opportunity to be heard.[8]

C. Was Warshak's claim appropriately upheld as a facial challenge?

The government argues that under *United States v. Salerno*, Warshak must prove that the challenged portion of the statute can never be constitutionally applied in order for the facial challenge to be upheld. 481 U.S. 739, 745-46 (1987) ("A facial challenge to a legislative Act is, of course, the most difficult challenge to mount successfully, since the challenger must establish that no set of circumstances exists under which the Act would be valid."). It specifically contends that, assuming some ISP e-mail account holders maintain a reasonable expectation of privacy in the content of their e-mails, there still are likely to be others who do not. Because the statute would be constitutional with respect to these account holders, the government argues that it should not be facially invalidated. It also identifies several hypothetical scenarios in which it contends the account holder's reasonable expectation of privacy could be maintained.

Warshak and amici initially counter that the statement from *Salerno* relied upon by the government in fact overstates the requirement for facially enjoining a statute. In a separately written concurrence in a denial of a petition of certiorari, Justice Stevens has pointed out that the "rigid and unwise dictum" from *Salerno* upon which the government now relies was neither an accurate statement of the law nor, more importantly, an accurate description of the Supreme Court's practice with respect to facial challenges. *Janklow v. Planned Parenthood, Sioux Falls Clinic*, 517 U.S. 1174 n.1 (1996) (Stevens, J., concurring in dissent from denial of certiorari). Justice Stevens catalogued several opinions that he claimed demonstrated the Court has effectively, if not explicitly, rejected the *Salerno* dictum.

There are a few well-known exceptions to the "no circumstances" test for facial validity. For example, in the First Amendment context, an overbreadth challenge allows a plaintiff to facially challenge a statute that can be constitutionally applied to his own conduct so as to protect the speech of others from any chilling effect the statute might have. *See, e.g.*, *Prime Media*, 2007 U.S. App. LEXIS 10862, at *10-11. In the abortion context, the "undue burden" test has a similar effect, as an abortion statute can be facially invalid even if, in some instances, its prohibition of certain abortions would be constitutional. *See Casey*, 505 U.S. at 895. We have noted that "[a]lthough

---

[8]Because our opinion speaks to the appropriate remedy in this case, we note one other important principle that applies both to e-mail seizures pursuant to a warrant supported by probable cause, and to compelled disclosure through a process akin to that involved with subpoenas. In neither instance is the government necessarily entitled to every e-mail stored with the ISP, many of which are likely to be entirely unrelated to its specific investigation. If the e-mails are seized pursuant to a warrant, the Fourth Amendment's particularity requirement would necessitate that the scope of the search somehow be designed to target e-mails that could reasonably be believed to have some connection to the alleged crime being investigated. *See United States v. Logan*, 250 F.3d 350, 364-65 (6th Cir. 2001) ("The purpose of this particularity requirement is to prevent the use of general warrants authorizing wide-ranging rummaging searches in violation of the Constitution's proscription against unreasonable searches and seizures."). Similarly, where a subpoena or an SCA order compels the disclosure of e-mails, the demand must be reasonable in scope and relevance. *Doe v. United States (In re Admin. Subpoena)*, 253 F.3d 256, 263 (6th Cir. 2001). Both of these requirements are fact specific. *See Logan*, 250 F.3d at 365 ("A description contained in a warrant is sufficiently particular if it is as specific as the circumstances and the nature of the alleged crime permit."). In either instance, a district court should consider whether the search could be narrowed by parameters such as the sender, recipient, date, relevant attachments, or keywords. We need not address these requirements in depth here, as the district courts are well suited to incorporate them on a case-by-case basis. We only reiterate them lest our opinion be read to somehow circumvent them.

Casey does not expressly purport to overrule *Salerno* [in the abortion context], in effect it does." *Women's Medical Professional Corp. v. Voinovich*, 130 F.3d 187, 194 (6th Cir. 1997). Although these exceptions pertain to specific subject matters that are not applicable here, they do demonstrate that the "no circumstances" standard is less sacrosanct than the government suggests.

The fact that there are exceptions to *Salerno* and that members of the Supreme Court have quibbled in the public record about its ongoing validity does not demonstrate its invalidity as a general principle pertaining to facial challenges. A more convincing argument about why *Salerno* does not apply in the Fourth Amendment context is the Supreme Court's decision in *Berger*, a case that is particularly analogous to this one. In *Berger*, the Court facially invalidated a New York statute that provided for court ordered wiretaps of telephone conversations on a showing of less than probable cause. 388 U.S. at 54. The Court explicitly stated that by allowing such a procedure, the statute violated the Warrant Clause by endorsing searches without a showing of probable cause. "The purpose of the probable-cause requirement of the Fourth Amendment, to keep the state out of constitutionally protected areas until it has reason to believe that a specific crime has been or is being committed, is thereby wholly aborted." *Id*. at 59. The Court acknowledged that it had "in the past, under specific conditions and circumstances, sustained the use of eavesdropping devices." *Id*. at 63. Under the government's present *Salerno* argument, this fact would have precluded facial invalidation of the statute in *Berger* as well. Yet the prospect of a constitutional application of the statute, either where a court order was supported by probable cause, or where the participants in the conversation lacked a reasonable expectation of privacy, did not prevent facial invalidation in *Berger*.

Under *Berger*, facial invalidation is justified where the statute, on its face, endorses procedures to authorize a search that clearly do not comport with the Fourth Amendment. A seizure of e-mails from an ISP, without either a warrant supported by probable cause, notice to the account holder to render the intrusion the functional equivalent of a subpoena, or a showing that the user maintained no expectation of privacy in the e-mail, amounts to exactly this. Therefore the district court's injunction was appropriate under *Berger*, regardless of the ongoing validity of the statement from *Salerno* on which the government relies.

Even if the stringent *Salerno* standard did govern the claim here, the government has not shown that the challenged application of the statute can be constitutionally applied. The government attempts to argue that under several scenarios, an e-mail user will not maintain a reasonable expectation of privacy in his e-mail account and, therefore a court order under section 2703 would not raise any Constitutional problems. First, the government points to certain user-provider relationships that could diminish the subscriber's expectation of privacy. These include an employer that issues e-mail accounts to its employees and requires them to waive any expectation of privacy in the account, and ISPs with similar requirements in their terms of service. As discussed above, we reject the argument that the user agreements in this case have such an effect. In some situations, like that in *Simons*, the user agreement might indicate that the user lacks a privacy interest vis-a-vis the employer or other relevant e-mail provider. This possibility does not diminish a privacy right with respect to the entire outside world, however. It would be proper in this situation for the government to seek disclosure with notice to an employer or provider who has access to the content of the e-mail, but this is an exception that our modification of the injunction adequately accounts for and does not defeat the validity of a facial challenge altogether.

The government also argues that by reserving the right to screen e-mails, the ISPs diminish any expectation of privacy their subscribers might have. Again, it is entirely possible, if not likely, that this process occurs without ever having a human being read the content of subscribers' e-mails. Where total access is the norm, we hold that the government may show as much and then may compel disclosure through the ISP. Less in-depth screening, however, is insufficient to diminish the privacy interest in an e-mail account.

As another example, the government contends that when an e-mail account is abandoned, as could occur with ISPs that require payment which the user fails to remit, the account holder maintains no reasonable expectation of privacy. The government analogizes this situation to a hotel room, in which the guest has an expectation of privacy, but abandons it when he leaves the room or is evicted by management. *See, e.g.*, *United States v. Allen*, 106 F.3d 695, 699 (6th Cir. 1997). This analogy lacks any connection to the actual practices of commercial ISPs. When a hotel guest checks out of his room, another person will occupy it, access every part of it in which he might have maintained any privacy interest, put his underwear in the same drawer, and otherwise extinguish any privacy interest to the fullest extent. Dominion and control over the hotel room is entirely surrendered to the hotel management, which in turn passes it on to the next guest who occupies the room. On the other hand, when an e-mail user stops using an e-mail address that is tied to his personal identity, he would certainly not expect that somebody else could come along, sign up for the same account, and not only send e-mails in his name, but read every past e-mail that he had failed to delete from the account or sent to someone else. There is no reason to believe that dominion or control over the contents of the account is yielded to the ISP or another user. This analogy is entirely inapposite.

Finally, the government points to "e-mail accounts that are procured through fraudulent means" as situations where an account holder has no reasonable expectation of privacy. This argument is another red herring, primarily because it cannot account for the majority of commercial e-mail services that offer their services for free. This obviously begs the question of why someone would have to commit fraud to get an account. Yet even if a hypothetical user wanted to conceal his identity or address from the ISP, the provision of misinformation would not bear in any way upon the privacy of the content of the user's e-mails. Further, the government suggests that a "hacker" who obtains "Internet services and e-mail accounts using stolen credit cards" would lack an expectation of privacy in the account he purchases, citing to a case where the thief of a stolen laptop did not have an expectation of privacy in material on the computer's hard drive. *See United States v. Caymen*, 404 F.3d 1196, 1201 (9th Cir. 2005). Where a thief steals someone else's property, it is true that he lacks an expectation of privacy in that property, such as the laptop computer at issue in *Caymen*. The government's hypothetical thief in this case would clearly not have an expectation of privacy in the victim's credit card account, which he illegally accessed. Why this person would lack a reasonable expectation of privacy in the contents of an e-mail account, however, is far from clear.[9] Because the government's hypothetical "hackers" cannot be said to "steal" the contents of the e-mails in the account, or an entire ISP server for that matter, this example is also unhelpful.

In light of our minor modification of the district court's injunction, we hold that narrow, facial invalidation of the statute is justified. *See Ayotte v. Planned Parenthood*, 546 U.S. 320, 328-329 (2006) ("Generally speaking, when confronting a constitutional flaw in a statute, we try to limit the solution to the problem. We prefer, for example, to enjoin only the unconstitutional applications of a statute while leaving other applications in force, or to sever its problematic portions while leaving the remainder intact." (citing *United States v. Raines*, 362 U.S. 17, 20-22 (1960) and *United States v. Booker*, 543 U.S. 220, 227-229 (2005))).[10] The government has not accounted in any way

---

[9]Of course if there were reason to suspect this individual of identity theft or credit card fraud, and some nexus to the use of the e-mail account, the government may well have reason to search it. This possibility has no bearing, however, on the entirely separate question of whether the user maintains a reasonable expectation of privacy that would require a warrant to authorize the search.

[10]*Ayotte* seems to counsel against the extreme reading of *Salerno* that the government advances here. The case involved a New Hampshire statute that prohibited minors from receiving an abortion until 48 hours after their parents or guardians had received written notice of the planned procedure. The Court accepted the fact that in a "small percentage" of cases, the statute would present a serious health risk to the pregnant minor, but otherwise deemed it to

for the privacy of shared communications, which since *Katz* have been protected from disclosure without either a warrant, the consent of one of the parties to the conversation, or compelled disclosure accompanied by an opportunity for judicial review. Our order sufficiently narrows the facial attack on the statute so that only its unconstitutional applications are enjoined, thereby obviating any problems under *Salerno*.

D. Balancing of Preliminary Injunction Factors

In addition to its argument pertaining to Warshak's likelihood of success on the merits, the government contends that other preliminary injunction factors — irreparable harm and balancing of the interests of the public and the parties — do not support the injunction here. The district court determined that Warshak would be irreparably harmed by future intrusions into his private e-mails, and that money damages cannot compensate him for this harm. With regard to the balancing of interests, the district court noted that "it is always in the public interest to prevent violation of a party's constitutional rights." D. Ct. Op. at 15 (citing *Deja Vu of Nashville, Inc. v. Metro. Gov't of Nashville & Davidson County*, 274 F.3d 377, 400 (6th Cir. 2001)). The district court also stated that its order would not unduly inhibit law enforcement, as the preliminary injunction would still permit e-mail seizures pursuant to a warrant or after the provision of notice to the account holder, and that law enforcement interests cannot trump the Fourth Amendment concerns raised by the government's conduct. It therefore concluded that "all four factors weigh in favor of granting preliminary injunctive relief to Warshak." *Id*. at 15-16. This balancing determination is reviewed for an abuse of discretion, under which this Court "accords great deference to the decision of the district court. The district court's determination will be disturbed only if the district court relied upon clearly erroneous findings of fact, improperly applied the governing law, or used an erroneous legal standard." *Blue Cross & Blue Shield Mut. v. Blue Cross & Blue Shield Ass'n*, 110 F.3d 318, 322 (6th Cir. 1997).

On appeal, the government contends that Warshak will not suffer irreparable harm, relying again on its argument that Warshak cannot show an imminent threat of future seizures, and also contending that he can recover money damages for any future violations of the SCA, that he would receive notice of future seizures of his e-mails now that he has been indicted and there would be no reason to hide the investigation, and that a motion to suppress in his criminal trial represents another adequate remedy for Warshak's fear of future seizures.

Initially, for similar reasons to our determination that Warshak has standing to bring suit, we conclude that Warshak has shown imminent threat of harm in the form of continued invasions of his Fourth Amendment rights. This determination is based on the past e-mail seizures,[11] which violated the SCA itself as well as the Fourth Amendment, the government's ongoing investigation of Warshak, and the government's clear policy of seizing e-mails without a warrant or notice to the account holder. Further, the government's contention that it would have no reason to seek future

---

be a valid regulation. 546 U.S. at 327. The Court indicated that partial invalidation of the statute was the preferred remedy, in light of the prospect of mixed constitutional and unconstitutional applications. *Id*. at 329. ("[T]he 'normal rule' is that 'partial, rather than facial, invalidation is the required course,' such that a 'statute may . . . be declared invalid to the extent that it reaches too far, but otherwise left intact.'"(citing *Brockett v. Spokane Arcades, Inc.*, 472 U.S. 491, 504 (1985)). Although the Court distinguished between partial and facial **invalidation**, it certainly did not state that existence of valid, constitutional applications in some situations precluded the use of a facial **challenge** altogether, calling instead for the case to continue after remand for reconsideration of the appropriate remedy. *Ayotte* suggests that the narrow injunctive relief we endorse today avoids any potential *Salerno* problems. Nor, unlike *Casey*, can we read this portion of *Ayotte* to be limited to the abortion context, as it describes a general approach to remedies without focusing on the underlying subject matter, and relies on cases that have nothing to do with abortion.

[11]*See, e.g., Lyons*, 461 U.S. at 102 ("Past wrongs [are] evidence bearing on 'whether there is a real and immediate threat of repeated injury.'").

disclosures without providing notice to Warshak seems at odds with its refusal to give him any assurance that this would be the case. Although it appears that Warshak made a general request that the government stop seeking court ordered seizures of his e-mails, rather than requesting notice pursuant to the statute, the government could have simply offered to provide notification under the statute, rather than replying with a blanket rejection. It also seems that the government would have reason not to provide Warshak with advance notice of any future searches of his e-mails. Although he has been indicted, and is obviously now aware of the investigation against him, it does not appear that Warshak is in custody, and thus he could have as much opportunity and incentive to destroy evidence now as he would have at any other time. Ultimately, the government's prior conduct renders it difficult for us to believe that Warshak's privacy interests can simply be trusted to the government's alleged "lack of interest" in future searches without prior notice.

The government's remaining arguments regarding alternative remedies would not protect the privacy interest that Warshak is seeking to uphold. His privacy interest in his e-mail conversations goes beyond not wanting to be incriminated by his e-mails, which is the only potential remedy from a suppression motion in his criminal case. Further, although money damages might be available to Warshak for the violations,[12] they similarly would not necessarily provide an adequate remedy. Warshak is seeking to protect the privacy of his communications, guaranteed to him by the Fourth Amendment, rather than merely seeking not to be incriminated by the content of his e-mails or to be compensated for the privacy violations he has suffered. We cannot conclude that the district court abused its discretion in finding that irreparable harm to Warshak supported the issuance of the preliminary injunction.

The district court's decision also appears to be supported by the balancing of the interests of Warshak, the government, and the public. Although the government claims that its investigative abilities will be unduly hampered by the injunction, it still can search e-mails stored with ISPs either through obtaining a warrant, by notifying the account holder, or, in light of our modification to the injunction, by making a fact specific showing that the account holder has waived his expectation of privacy with respect to the ISP. Further, under section 2703(f), it can require an ISP to preserve evidence "pending the issuance of a court order or other process," ameliorating any concerns about the destruction of evidence. This provision would seemingly address the government's concerns about destruction of evidence, as it could order the ISP to preserve evidence at the same time it provides Warshak notice of its intent to compel disclosure. To the extent that the government seeks to search e-mails covertly without a warrant, this interest is simply incompatible with the Fourth Amendment, and provides no basis for overturning the injunction. *See Almeida-Sanchez v. United States*, 413 U.S. 266, 273 (1973) ("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."). Further, because "it is always in the public interest to prevent violation of a party's constitutional rights," this desire to conduct ex parte e-mail searches without notice to the account holder indicates that the public interest counsels in favor of the preliminary injunction. It goes without saying that Warshak's constitutional privacy interest is also advanced by the injunction.

For these reasons, we agree with the district court that the other preliminary injunction factors support the injunctive relief it issued. At a minimum, we would be hard-pressed to believe that they show in any way that the district court abused its discretion, particularly in light of the narrowed scope of the preliminary injunction that our added modification has imposed.

---

[12] 18 U.S.C. § 2712 provides for monetary relief against the United States for violations of the SCA. Warshak's constitutional claims go beyond violations of the statute, however. Even so, he would still potentially have a cause of action under 42 U.S.C. § 1983, although one would have to imagine that he would face viable defenses of qualified immunity were he inclined to seek money damages.

IV.

The district court correctly determined that e-mail users maintain a reasonable expectation of privacy in the content of their e-mails, and we agree that the injunctive relief it crafted was largely appropriate, although we find necessary one modification. On remand, the preliminary injunction should be modified to prohibit the United States from seizing the contents of a personal e-mail account maintained by an ISP in the name of any resident of the Southern District of Ohio, pursuant to a court order issued under 18 U.S.C. § 2703(d), without either (1) providing the relevant account holder or subscriber prior notice and an opportunity to be heard, or (2) making a fact-specific showing that the account holder maintained no expectation of privacy with respect to the ISP, in which case only the ISP need be provided prior notice and an opportunity to be heard.