RTF

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

File Name: 08a0252p.06

# UNITED STATES COURT OF APPEALS

FOR THE SIXTH CIRCUIT

---

STEVEN WARSHAK,

*Plaintiff-Appellee,*

*v.*

UNITED STATES OF AMERICA,

*Defendant-Appellant.*

No. 06-4092

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

Argued: December 5, 2007

Decided and Filed: July 11, 2008

Before: BOGGS, Chief Judge; MARTIN, BATCHELDER, DAUGHTREY, MOORE, COLE, CLAY, GILMAN, GIBBONS, ROGERS, SUTTON, COOK, McKEAGUE, and GRIFFIN, Circuit Judges.

---

## COUNSEL

**ARGUED:** Steven L. Lane, UNITED STATES DEPARTMENT OF JUSTICE, Washington, D.C., for Appellant. Martin G. Weinberg, LAW OFFICES, Boston, Massachusetts, for Appellee. **ON BRIEF:** Steven L. Lane, 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, LAW OFFICES, Boston, Massachusetts, Martin Stanley 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.

SUTTON, J., delivered the opinion of the court, in which BOGGS, C. J., BATCHELDER, GILMAN, GIBBONS, ROGERS, COOK, McKEAGUE, and GRIFFIN, JJ., joined. MARTIN, J. (pp. 12-15), delivered a separate dissenting opinion in which DAUGHTREY, MOORE, COLE, and CLAY, JJ., joined.

## OPINION

SUTTON, Circuit Judge. Since 1986, Title II of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 201, 100 Stat. 1848, *codified as amended at* 18 U.S.C. §§ 2701–2711, commonly referred to as the Stored Communications Act, has authorized the federal government to require internet service providers to disclose the contents of "electronic communication[s]" of their customers in certain circumstances, including by way of an *ex parte* court order. *Id.* § 2703(d). The government obtained two such orders in 2005 to search Steven Warshak's e-mails. When Warshak learned about the orders, roughly a year later, he filed a declaratory judgment action, seeking to invalidate § 2703(d) under the Fourth Amendment, and he moved for a preliminary injunction, seeking to enjoin the government from conducting further *ex parte* e-mail searches. The district court granted the motion and enjoined the government from using § 2703(d) to seize the contents of "any personal email account[]" belonging to Warshak or "any resident of the Southern District of Ohio" without "prior notice and an opportunity to be heard." JA 129. We vacate the preliminary injunction because Warshak's constitutional claim is not ripe for judicial resolution.

I.

A.

The Stored Communications Act prohibits unauthorized access to certain electronic communications, *see* 18 U.S.C. § 2701, and places restrictions on a service provider's disclosure of certain communications, *see id.* § 2702. It also permits a "governmental entity" to compel a service provider to disclose the contents of communications in certain circumstances. *See id.* § 2703.

Three relevant definitions bear on the meaning of the compelled-disclosure provisions of the Act. "[E]lectronic communication service[s]" permit "users . . . to send or receive wire or electronic communications," *id.* § 2510(15), a definition that covers basic e-mail services, *see* Patricia L. Bellia et al., *Cyberlaw: Problems of Policy and Jurisprudence in the Information Age* 584 (2d ed. 2004). "[E]lectronic storage" is "any temporary, intermediate storage of a wire or electronic communication . . . and . . . any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17). "[R]emote computing service[s]" provide "computer storage or processing services" to customers, *id.* § 2711(2), and are designed for longer-term storage, *see* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1216 (2004).

The compelled-disclosure provisions give different levels of privacy protection based on whether the e-mail is held with an electronic communication service or a remote computing service and based on how long the e-mail has been in electronic storage. The government may obtain the contents of e-mails that are "in electronic storage" with an electronic communication service for 180 days or less "only pursuant to a warrant." 18 U.S.C. § 2703(a). The government has three options for obtaining communications stored with a remote computing service and communications that have been in electronic storage with an electronic service provider for more than 180 days: (1) obtain a warrant; (2) use an administrative subpoena; or (3) obtain a court order under § 2703(d). *Id.* § 2703(a), (b).

Under § 2703(d), the provision at issue in this case, "a court of competent jurisdiction" may issue an order based on "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." *Id.* § 2703(d). Although the statute generally requires the government to give the user prior notice of the disclosure unless it obtains a warrant, it contains an exception, *id.* § 2703(b)(1)(B), which says the government may delay notice in 90-day increments, *id.* § 2705(a)(4), if notification would result in "(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," *id.* § 2705(a)(2); *see also id.* § 2705(b) (authorizing the government to seek a court order preventing the service provider from disclosing the subpoena if the same conditions are met).

B.

Warshak is the president and sole owner of Berkeley Premium Nutraceuticals, Inc., which became the target of an investigation into "mail and wire fraud, money laundering, and other federal offenses" based on its "nationwide marketing, distribution, and sale of products." JA 47, 50. The government sought permission from a magistrate judge to require Warshak's internet service providers—NuVox Communications and Yahoo!—to turn over Warshak's account information, "[a]ll [l]og files and backup tapes" and the contents of e-mails that had been "accessed, viewed, or downloaded" or that were more than 181 days old. JA 49, 52.

On May 6, 2005, and again on September 12, 2005, the magistrate judge granted the applications under § 2703(d) of the Act. As required, the orders were based on "specific and articulable facts showing that there [were] reasonable grounds to believe that the records or other information sought [were] relevant and material to an ongoing criminal investigation." JA 48, 51; *see* 18 U.S.C. § 2703(d). As permitted, the orders did not give Warshak immediate notice of the disclosures. 18 U.S.C. § 2703(b)(1)(B). Concluding that notice to Warshak "would seriously jeopardize the investigation," the magistrate judge ordered the government to delay notice for 90 days and mandated that the "[o]rder[s] [be] sealed until otherwise ordered by the Court." JA 48, 51; *see* 18 U.S.C. §§ 2703(b)(1)(B), 2705(a).

On May 31, 2006, roughly a year after the court issued the first § 2703(d) order, the government gave Warshak notice of the orders. In response, he sued the government on June 12, seeking declaratory and injunctive relief. Among other complaints, Warshak alleged that § 2703(d) violated the Fourth Amendment on its face and as applied because the searches were based on a showing of less than probable cause and were not supported by a warrant.

On June 30, Warshak filed a motion for a preliminary injunction. The court granted the motion and enjoined the government from using § 2703(d) to search "the contents of any personal email account maintained by an [ISP] in the name of any resident of the Southern District of Ohio" without providing the user "prior notice and an opportunity to be heard." JA 130. The court reasoned that Warshak likely would succeed on his Fourth Amendment claim because internet users have a reasonable expectation of privacy in e-mails, and because the orders authorized warrantless searches on less than probable cause. The court also concluded that Warshak faced imminent harm based on the two prior orders and the government's refusal to pledge not to seek additional orders in the future. The court enjoined the government from enforcing § 2703(d) or related sections of the Act (sections 2703(b)(1)(B)(ii) and 2705) to the extent that they "authorize the *ex parte* issuance of search and seizure orders without a warrant and on less than a showing of probable cause." JA 129. While the court relied "in part" on the "threat of irreparable injury" to Warshak, it explained that "the constitutional flaws . . . are facial in nature." *Id.*

On September 20, 2006, a federal grand jury indicted Warshak for bank fraud, mail fraud and money laundering, among other federal crimes. *See* Indictment, *United States v. Warshak*, No. 1:06-

cr-00111 (S.D. Ohio Sept. 20, 2006). On February 22, 2008, a jury convicted him on 93 counts. *See* Jury Verdict as to Steven E. Warshak, *Warshak*, No. 1:06-cr-00111 (S.D. Ohio Feb. 22, 2008).

II.

The Constitution does not extend the "judicial Power" to any legal question, wherever and however presented, but only to those legal questions presented in "Cases" and "Controversies." U.S. Const. art. III, § 2. A claim is not "amenable to . . . the judicial process," *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 102 (1998), when it is filed too early (making it unripe), when it is filed too late (making it moot) or when the claimant lacks a sufficiently concrete and redressable interest in the dispute (depriving the plaintiff of standing). This case implicates at least two of these doctrines today, ripeness and standing, both of which "unquestionably . . . overlap," *Airline Prof'ls Ass'n of the Int'l Bhd. of Teamsters v. Airborne, Inc.*, 332 F.3d 983, 988 (6th Cir. 2003), and at some point could well implicate the third (mootness) in view of the motion to suppress that Warshak filed in his criminal case. As there is no obligation to favor one of these justiciability doctrines over the other and as none of these questions goes to the merits of the case, we may address them in any sequence we wish. *See Arizonans for Official English v. Arizona*, 520 U.S. 43, 66–67 (1997). We start—and end—with ripeness.

Like standing, ripeness "is drawn both from Article III limitations on judicial power and from prudential reasons for refusing to exercise jurisdiction." *Nat'l Park Hospitality Ass'n v. Dep't of Interior*, 538 U.S. 803, 808 (2003) (internal quotation marks omitted). The ripeness doctrine serves to "avoid[] . . . premature adjudication" of legal questions and to prevent courts from "entangling themselves in abstract" debates that may turn out differently in different settings. *Id.* at 807. In ascertaining whether a claim is ripe for judicial resolution, we ask two basic questions: (1) is the claim "fit[] . . . for judicial decision" in the sense that it arises in a concrete factual context and concerns a dispute that is likely to come to pass? and (2) what is "the hardship to the parties of withholding court consideration"? *Abbott Labs. v. Gardner*, 387 U.S. 136, 149 (1967); *see also Ammex, Inc. v. Cox*, 351 F.3d 697, 706 (6th Cir. 2003); *Adult Video Ass'n v. U.S. Dept. of Justice*, 71 F.3d 563, 568 (6th Cir. 1995).

A.

There are several reasons why this claim is not "fit" for judicial review. To start, we have no idea whether the government will conduct an *ex parte* search of Warshak's e-mail account in the future and plenty of reason to doubt that it will, making this a claim that depends on "contingent future events that may not occur as anticipated, or indeed may not occur at all." *Texas v. United States*, 523 U.S. 296, 300 (1998) (internal quotation marks omitted). Answering difficult legal questions before they arise and before the courts know how they will arise is not the way we typically handle constitutional litigation. *See Lujan v. Nat'l Wildlife Fed'n*, 497 U.S. 871, 894 (1990).

Past is precedent, Warshak responds: Government agents have conducted two *ex parte* searches of his e-mails before, so it is fair to assume they will do so again. Making that prospect more likely, he adds, is the government's reluctance to promise not to search Warshak's e-mail accounts in the future. But this position overlooks a central feature of the statute. Searches under the statute generally require what Warshak demands: "prior notice." 18 U.S.C. § 2703(b)(1)(B). In conducting its previous searches of Warshak's e-mails, the government obtained judicial permission to delay notice to Warshak on the ground that disclosure would "seriously jeopardiz[e] [the] investigation." *Id.* § 2705(a)(2)(E). That possibility no longer exists. Warshak has ample notice of the investigation—indeed notice of the worst sort: He has been indicted (and now convicted). The question, as framed by the complaint, is not whether the government will conduct another search of Warshak's e-mails; it is whether the government will conduct another *ex parte*

search of his e-mails, a possibility that is exceedingly remote given that the reason the government kept these searches confidential—that they would jeopardize the ongoing investigation—no longer exists. It is within the realm of possibility, we suppose, that a new investigation could commence or that some other reason for delaying notice could arise, such as the need to avoid "endangering the life or physical safety of an individual; . . . flight from prosecution; . . . destruction of or tampering with evidence; . . . intimidation of potential witnesses; or . . . unduly delaying a trial." *Id.* § 2705(a)(2)(A)–(E). But these possibilities are just that—possibilities (and remote possibilities at that)—making it eminently unpredictable whether, when or why the government would seek judicial permission to conduct another *ex parte* search of Warshak's e-mails.

Not only do "we have no idea whether or when" such a search will occur but we also "have no idea" what e-mail accounts, or what types of e-mail accounts, the government might investigate. *Toilet Goods Ass'n, Inc. v. Gardner*, 387 U.S. 158, 163 (1967). That uncertainty looms large in a debate about the expectations of privacy in e-mail accounts. The underlying merits issue in the case is this: In permitting the government to search e-mails based on "reasonable grounds," is § 2703(d) consistent with the Fourth Amendment, which generally requires "probable cause" and a warrant in the context of searches of individuals, homes and, perhaps most analogously, posted mail? The answer to that question will turn in part on the expectations of privacy that computer users have in their e-mails—an inquiry that may well shift over time, that assuredly shifts from internet-service agreement to internet-service agreement and that requires considerable knowledge about ever-evolving technologies. Because "[t]he task of generating balanced and nuanced rules" in this area "requires a comprehensive understanding of technological facts," Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801, 875 (2004), Warshak's claim epitomizes the kind of dispute that would profit from "a concrete factual context," *Ammex*, 351 F.3d at 706.

Think of just one of these moving parts—the variety of internet-service agreements and the differing expectations of privacy that come with them. An agreement might say that a service provider will "not . . . read or disclose subscribers' e-mail to anyone except authorized users." *United States v. Maxwell*, 45 M.J. 406, 417 (C.A.A.F. 1996) (describing testimony about AOL's then-existing policy). An agreement might say that a service provider "will not intentionally monitor or disclose any private email message" but that it "reserve[s] the right" to do so in some cases. *See* Privacy Statement for Juno Members, http://www.juno.com/legal/privacy.html (last visited July 7, 2008). An agreement might say that a service provider "may or may not pre-screen Content, but . . . shall have the right (but not the obligation) in [its] sole discretion to pre-screen, refuse or move any Content that is available via the Service"—as indeed Warshak's Yahoo! account did. JA 89, 163 n.3. An agreement might say that e-mails will be provided to the government on request—as indeed the same Yahoo! account did. An agreement might say that other individuals, besides the recipient of the e-mail, will have access to it and will be entitled to use the information in it. *See, e.g.*, JA 208 (explaining that Gmail, a service provided by Google, gives users "an enormous amount of storage capacity . . . in exchange for . . . terms of service which say that Google is allowed . . . [to] take a look at the content of [users'] e-mail and . . . target advertising at [users] accordingly"). Or an agreement might say that the user has no expectation of privacy in any of her communications. *See, e.g.*, JA 207 (government counsel explaining that "every day when we log into our e-mail account, we agree that we have no expectation of privacy in the account").

Some of these service-provider agreements could cast doubt on the validity of § 2703(d) in a given case; others might not. Better, we think, to decide the validity of the statute in the context of a specific internet-service agreement and a specific search and seizure.

Nor can we rely on *previous* government searches of Warshak's e-mails to hypothesize the factual context of the next search. Even if the record contained the full text of the NuVox and Yahoo! service-provider agreements (it does not; it contains just part of the Yahoo! agreement), we

would run into a similar conjecture problem. Just as there is little basis for assuming the government will conduct another *ex parte* search of Warshak's e-mails, there is little basis for assuming any future search will concern e-mails facilitated by these service providers, as opposed to e-mails facilitated by other service providers. In view of Warshak's knowledge of the investigation and knowledge of his pre-existing service-provider agreements before he filed the complaint, it is surely possible that he might switch to a service provider that gave him a greater expectation of privacy—say, by contracting with a paid-subscription service provider that promises not to screen e-mail. Or he might decide that the convenience of free, web-based e-mail is ultimately worth the tradeoff of allowing the service provider to screen his e-mail. We simply have no way of knowing what kind of accounts Warshak is likely to possess in the future and no basis for assuming that future e-mails will be controlled by the same type of service-provider agreement he used in the past. "The operation of the statute," in short, will be "better grasped when viewed in light of a particular application." *Texas*, 523 U.S. at 301.

Concerns about the premature resolution of legal disputes have particular resonance in the context of Fourth Amendment disputes. In determining the "reasonableness" of searches under the Fourth Amendment and the legitimacy of citizens' expectations of privacy, courts typically look at the "totality of the circumstances," *Samson v. California*, 547 U.S. 843, 848 (2006) (internal quotation marks omitted), reaching case-by-case determinations that turn on the concrete, not the general, and offering incremental, not sweeping, pronouncements of law, *see O'Connor v. Ortega*, 480 U.S. 709, 718 (1987). Courts thus generally review such challenges in two discrete, *post-enforcement* settings: (1) a motion to suppress in a criminal case or (2) a damages claim under § 1983 or under *Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics*, 403 U.S. 388 (1971), against the officers who conducted the search. In both settings, the reviewing court looks at the claim in the context of an actual, not a hypothetical, search and in the context of a developed factual record of the reasons for and the nature of the search. A pre-enforcement challenge to future e-mail searches, by contrast, provides no such factual context. The Fourth Amendment is designed to account for an unpredictable and limitless range of factual circumstances, and accordingly it generally should be applied after those circumstances unfold, not before.

That is why Warshak's rejoinder—that this case presents a "purely legal question," *Toilet Goods*, 387 U.S. at 163—carries little weight. In addition to the fact that this "purely legal question" remains a purely *speculative* legal question, this case presents a legal question that may be answered differently in different settings and a legal question that "depend[s] . . . on an understanding of" complex factual issues. *Id.* In such cases, "judicial appraisal . . . is likely to stand on a much surer footing in the context of a specific application of [the law] than could be the case in the framework of [a] generalized challenge." *Id.* at 164.

Making matters worse, Warshak's complaint sought, and the district court's injunction gave him, pre-enforcement relief not just on behalf of himself but on behalf of *all* e-mail users. The point of this attack on the statute, like all facial challenges, was to leave nothing standing—to prevent § 2703(d) from ever being enforced without a warrant and probable cause, no matter the circumstances, no matter the individual's expectation of privacy, no matter the government's interests in obtaining the information without tipping the suspect off to the investigation.

That is not how constitutional litigation typically proceeds, and that is why the federal courts do not lightly uphold facial challenges. Many of the concerns that underlie the ripeness doctrine—that "[t]he operation of the statute [will be] better grasped when viewed in light of a particular application" and that "the proper exercise of the judicial function" avoids deciding abstract and speculative questions, *Texas*, 523 U.S. at 301 (internal quotation marks omitted)—underlie, and are indeed echoed by, the courts' reluctance to grant relief in the face of facial, as opposed to as-applied, attacks on statutes. When "determining whether a law is facially invalid," as when determining whether a case is ripe, "we must be careful not to . . . speculate about

'hypothetical' or 'imaginary' cases" or to "premature[ly] interpret[] . . . statutes on the basis of factually barebones records." *Wash. State Grange v. Wash. State Republican Party*, 128 S. Ct. 1184, 1190–91 (2008) (internal quotation marks omitted). "Exercising judicial restraint in a facial challenge frees the Court not only from unnecessary pronouncement on constitutional issues, but also from premature interpretations of statutes in areas where their constitutional application might be cloudy." *Id.* at 1191 (internal quotation marks omitted); *see also United States v. Raines*, 362 U.S. 17, 22 (1960). As-applied challenges—the "basic building blocks of constitutional adjudication"—remain the preferred route. *Gonzales v. Carhart*, 127 S. Ct. 1610, 1639 (2007) (internal quotation marks omitted); *cf. Nat'l Wildlife Fed'n*, 497 U.S. at 894 (noting that the ripeness doctrine turns in part on the fact that "[t]he case-by-case approach . . . is the traditional, and remains the normal, mode of operation of the courts").

Litigation by hypothetical becomes particularly risky in the face of ever-evolving and ever-more-complicated technology. *Cf. Carhart*, 127 S. Ct. at 1638. The complexities of modern electronic communications, which already have changed markedly since 1986, make it especially difficult to do what facial invalidation requires—"to consider every conceivable situation which might possibly arise in the application of complex and comprehensive legislation." *Id.* at 1639 (internal quotation marks omitted).

The Supreme Court has been especially reluctant to invalidate statutes on their face under the Fourth Amendment. "The constitutional validity of a warrantless search is pre-eminently the sort of question which can only be decided in the concrete factual context of the individual case." *Sibron v. New York*, 392 U.S. 40, 59 (1968). On this basis, *Sibron* refused "to be drawn into . . . the abstract and unproductive exercise" of entertaining a Fourth Amendment challenge to the facial validity of New York's "stop-and-frisk" statute, which authorized police to stop and search individuals in certain circumstances. *Id.* at 43–44, 59. *See generally Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 632 n.10 (1989); *Bell v. Wolfish*, 441 U.S. 520, 560 (1979).

Even outside the case-by-case imperatives of Fourth Amendment decisionmaking, the Supreme Court has expressed increasing skepticism of facial challenges in recent years. In *United States v. Salerno*, 481 U.S. 739 (1987), the Court held that the Bail Reform Act is not facially invalid under the Due Process Clause of the Fifth Amendment or the Excessive Bail Clause of the Eighth Amendment, *id.* at 755. The Court reasoned that "[a] facial challenge to a legislative Act is . . . 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. The fact that the Bail Reform Act might operate unconstitutionally under some conceivable set of circumstances is insufficient to render it wholly invalid . . . ." *Id.* at 745. In *Sabri v. United States*, 541 U.S. 600 (2004), the Court rejected a facial challenge to a bribery statute, explaining that "[f]acial adjudication carries too much promise of premature interpretatio[n] of statutes on the basis of factually barebones records," *id.* at 609 (internal quotation marks omitted) (second alteration in original). "Although passing on the validity of a law wholesale may be efficient in the abstract," the Court explained, "any gain is often offset by losing the lessons taught by the particular, to which common law method normally looks." *Id.* at 608–09. Even in the abortion context, where in the past it has applied a more relaxed standard to facial challenges, *see Planned Parenthood of Se. Pa. v. Casey*, 505 U.S. 833, 895 (1992), the Court recently expressed its preference for as-applied challenges. In *Carhart*, the Court refused to engage in conjecture about potential applications of an abortion statute, saying that "it would indeed be undesirable for this Court to consider every conceivable situation which might possibly arise in the application of complex and comprehensive legislation." 127 S. Ct. at 1639 (internal quotation marks omitted).

This trend continued in the Supreme Court's most recent Term. In *Crawford v. Marion County Election Board*, 128 S. Ct. 1610 (2008), the Court explained that plaintiffs mounting facial challenges "bear a heavy burden of persuasion," then rejected a facial challenge to Indiana's voter-

identification requirements, *id.* at 1621–23. In *Washington State Grange*, the Court explained that "[f]acial challenges are disfavored, raise the risk of premature interpretation[,] . . . run contrary to the fundamental principle of judicial restraint" and "threaten to short-circuit the democratic process." 128 S. Ct. at 1191. Refusing to hold Washington's primary system unconstitutional in all its applications, the Court reasoned that the plaintiffs' claim rested on "sheer speculation" that the system would confuse voters and that there was "no evidentiary record" to provide guidance. *Id.* at 1193–94. That the system "could conceivably be" implemented in a constitutional manner was "fatal" to the facial challenge, leaving fact-specific claims of voter confusion to "await an as-applied challenge." *Id.* at 1194–95. A similar conclusion applies here: Because we can only speculate as to the sorts of accounts and privacy terms that different users may have today and may have in the future, it is far more prudent to "await an as-applied challenge" to decide whether the Act is constitutional in a discrete factual setting.

In the face of these considerations and this case law, *Berger v. New York*, 388 U.S. 41 (1967), offers Warshak little help. *Berger*, it is true, appeared to invalidate a New York eavesdropping statute on its face. *Id.* at 43 n.1. But the Court did not discuss the distinction between as-applied and facial challenges, and accordingly did not reach, and necessarily did not discuss, the question whether it would have made sense to proceed differently. One year later, when the Court decided *Sibron*, it did discuss this distinction, it interpreted *Berger* narrowly and it advised courts to consider challenges to "[t]he constitutional validity of a warrantless search" on an as-applied basis. *Sibron*, 392 U.S. at 59. Unlike *Berger* and *Sibron*, moreover, this case involves not just the risk of guessing about other fact patterns in which a statute might be applied but the risk of guessing how the statute will be applied even to *this* individual—a fact that makes the facial invalidation of this statute especially inappropriate.

No doubt, Warshak is correct that the Court has issued Fourth Amendment rulings that effectively invalidated statutes in whole or in part. *See, e.g.*, *Payton v. New York*, 445 U.S. 573, 589–90, 598 & n.46 (1980); *Torres v. Puerto Rico*, 442 U.S. 465, 471, 474 (1979). But in these cases, too, the Court reviewed applications of statutes in concrete settings—motions to suppress that sought to prevent the information obtained in a search from being used against the defendant. *See Payton*, 445 U.S. at 576–79, 589–90; *Torres*, 442 U.S. at 467, 474. That is a distant cry from the relief Warshak seeks today.

Nor, for a separate reason, was it appropriate in this case to grant a preliminary injunction in favor of persons other than Warshak. "While district courts are not categorically prohibited from granting injunctive relief benefitting an entire class in an individual suit, such broad relief is rarely justified because injunctive relief should be no more burdensome to the defendant than necessary to provide complete relief to the plaintiffs." *Sharpe v. Cureton*, 319 F.3d 259, 273 (6th Cir. 2003) (emphasis omitted). Warshak did not seek class-action relief, and he has made no showing—below or here—why the injunction needed to run in favor of other individuals in order to protect him.

Our reluctance to hypothesize how the government might conduct a conjectural search of Warshak's e-mails, then resolve the constitutionality of that search as well as any others the government might conduct under the statute, is reinforced by another reality: The Stored Communications Act has been in existence since 1986 and to our knowledge has not been the subject of any successful Fourth Amendment challenges, in any context, whether to § 2703(d) or to any other provision. If it "is often true" that reviewing "legislation in advance of its immediate adverse effect in the context of a concrete case involves too remote and abstract an inquiry for the proper exercise of the judicial function," *Texas*, 523 U.S. at 301 (internal quotation marks omitted), the same is assuredly true when we have no precedent to guide us, *cf. Raines*, 362 U.S. at 23. Discretion, indeed, is the better part of valor.

B.

There also is no meaningful risk of "hardship" to Warshak "of withholding court consideration." *Abbott Labs.*, 387 U.S. at 149. The prototypical case of hardship comes from the claimant who faces a choice between immediately complying with a burdensome law or "risk[ing] serious criminal and civil penalties." *Id.* at 153; *compare id. with Toilet Goods*, 387 U.S. at 164–65. Yet Warshak faces no such conflict. The relevant provisions of the Act do not require Warshak to do anything. They do not "force [Warshak] to modify [his] behavior in order to avoid future adverse consequences," *see Ohio Forestry Ass'n, Inc. v. Sierra Club*, 523 U.S. 726, 734 (1998), or require Warshak "to engage in, or to refrain from, any conduct," *see Texas*, 523 U.S. at 301. Because the Act does not purport to regulate his primary conduct at all, much less impose criminal and civil penalties for non-compliance, it does not put Warshak in an untenable bind between undertaking an irreversible burden or risking criminal indictment.

Hardship is difficult to maintain on this record for another reason. Individuals subjected to allegedly unconstitutional searches and seizures have at least two alternatives short of a pre-enforcement, facial attack on the enabling statute. They may file a motion to suppress in the event the government tries to use the evidence against them in a criminal prosecution. Or they may file a § 1983 or a *Bivens* action against the officers who conducted the search. Warshak filed a motion to suppress in his criminal case and, for reasons of his own, has not filed a *Bivens* action.

Warshak responds that these options will not allow him to obtain what he wants: a constitutional ruling on the validity of § 2703(d). As he sees it, the courts could apply the *Leon* good-faith doctrine in denying his motion to suppress, *see United States v. Leon*, 468 U.S. 897 (1984), and they could reject his *Bivens* claim on the ground that the invalidity of the statute had not been "clearly established." Both rulings, he points out, would not generate a Fourth Amendment determination. Even accepting for a moment Warshak's premise that one of the "hardship" concerns that may ripen a claim into a justiciable controversy is a litigant's interest in obtaining a constitutional ruling, Warshak is only half right. Yes, *Leon* permits courts to decide the good-faith question without determining whether the search was valid. *See Leon*, 468 U.S. at 925; *Illinois v. Krull*, 480 U.S. 340, 349–50 (1987). And indeed, since the oral argument in this case, the district court has rejected Warshak's suppression motion solely on the ground that the officers acted in good faith. Opinion and Order, *Warshak*, No. 1:06-cr-00111, at 11–13 (S.D. Ohio Dec. 13, 2007).

But the same is not true of a *Bivens* action. The Court has "insist[ed]" on a strict order of engagement in *Bivens* (and § 1983) actions, requiring courts to "turn[] to the existence or nonexistence of a constitutional right as the *first inquiry*" and preventing them from "skip[ping] ahead to the question whether the law clearly established that the officer's conduct was unlawful in the circumstances of the case." *Saucier v. Katz*, 533 U.S. 194, 201 (2001) (emphasis added). If a constitutional ruling is what Warshak wanted, a *Bivens* action would have given it to him.

But even if a *Bivens* claim did not guarantee Warshak the constitutional ruling he seeks, *see Scott v. Harris*, 127 S. Ct. 1769, 1774 n.4 (2007) (saving for another day whether to reconsider the requirement that the constitutional issue must be resolved first in a § 1983 or *Bivens* action), that would not alter our conclusion. Warshak offers no authority for the proposition that an otherwise-unripe claim may be entertained on the ground that it will facilitate a judicial ruling on the merits. And we doubt that any such authority exists. A central tenet of the case-or-controversy requirement after all is that a general interest in a judicial ruling on the merits does not by itself confer jurisdiction on the federal courts. Otherwise, a claimant's interest in a judicial ruling itself would justify reaching the question, prematurely or not. And even if the Supreme Court were to permit lower courts to sidestep constitutional rulings in addressing motions to suppress *and* § 1983 (and *Bivens*) actions, that presumably would be because the Court took the view that in some settings it did not make sense to decide constitutional questions prematurely. *See Scott*, 127 S. Ct. at 1774 n.4.

That of course is the same concern underlying the ripeness doctrine—a concern we would hardly respect by permitting such claims through pre-enforcement, facial attacks instead.

Also unavailing is Warshak's concern that, without a constitutional ruling, he will be exposed to future unconstitutional searches. That contention, as we have shown, turns on a long list of speculative assumptions—that (1) the government will again seek to obtain his e-mail contents, even though he has already been indicted and convicted, (2) it will choose to do so through § 2703(d), as opposed to a search warrant or subpoena, (3) a court will determine that the § 2703(d) requirements are met, (4) the government will seek to invoke the delayed-notice provision and (5) a court will find that notice of the search would imperil the existence of an already-known investigation. That is not a plausible theory of hardship.

Warshak also has argued on appeal that the Act creates a "chilling effect" on his use of email. Although a chilling effect might relax ripeness requirements in a First Amendment case, *see, e.g.*, *Anderson v. Spear*, 356 F.3d 651, 669 (6th Cir. 2004), Warshak never made a First Amendment claim. The first time he claimed a "chilling effect" of any sort as to him was at oral argument before the en banc court. The only other "chilling effect" concern raised in the litigation was in his memorandum in support of a preliminary injunction, in which he alleged that denying the injunction would cause harm to *others* because it would "have a chilling effect on the [general public's] use of email as a form of communication because people and businesses would regard it as unsecured." JA 76. Because Warshak does not challenge the government's action on First Amendment grounds, this is a "non-First Amendment case[]" and the traditional ripeness requirements apply. *Nat'l Rifle Ass'n of Am. v. Magaw*, 132 F.3d 272, 285 (6th Cir. 1997).

* * * * *

The dissent makes two points that deserve a response: (1) that the court should "reach[] the question that is on everyone's mind"—the validity of the delayed-notice provision of the Act, Dissent at 12; *see id.* ("Why do today what can be done tomorrow?"), and (2) that the court should contain its "zeal to uphold the power of the government to intrude into the privacy of citizens," *id.* at 14, and that its decision "is but another step in the ongoing degradation of civil rights in the courts of this country," *id.* at 15.

As a matter of efficiency, the dissent is quite right. The ripeness doctrine, like all limitations on the "judicial Power," prevents us from "do[ing] today what can be done tomorrow" and, in the process, prevents us from announcing interpretations of the Constitution that some citizens and commentators may wish to hear today. But efficiency is not the only end of the Constitution, and it is hardly a value that necessarily favors the promotion of civil rights, at least if history is any guide. *See Stanley v. Illinois*, 405 U.S. 645, 656 (1972). Whatever value efficiency has when it comes to the interpretation of constitutional rights, at any rate, that consideration must be balanced against other judicial values: deciding constitutional questions correctly, which we are more likely to do on a case-by-case basis in the context of a concrete factual setting; and exercising the *Marbury* power only when the Constitution, Congress and precedent give us that authority. "Although passing on the validity of a law wholesale may be efficient in the abstract, any gain is often offset by losing the lessons taught by the particular." *Sabri*, 541 U.S. at 608–09.

The dissent's concern about the "ongoing degradation of civil rights" seems a bit overwrought. The whole point of not deciding the constitutionality of a law in an unripe setting is not to decide it—not to degrade, or for that matter uplift, *any* constitutional right until we are faced with a concrete, as-applied, challenge to the provision. And if it is true, as the dissent charges, that the majority has a "zeal to uphold the power of the government to intrude into the privacy of citizens"—needless to say, it is not—perhaps we should be commended for restraining ourselves by not making that view the law when we had the chance.

But, perhaps most acutely, both of the dissent's concerns have almost nothing to do with this case. Warshak has only himself to blame for choosing not to vindicate his civil rights when he had the chance—through a *Bivens* action. And, either way, he still retains the right to challenge the district court's resolution of his motion to suppress through an appeal of his criminal conviction.

III.

For these reasons, we vacate the preliminary injunction and remand the case to the district court to dismiss Warshak's constitutional claim.

## DISSENT

BOYCE F. MARTIN, JR., Circuit Judge, dissenting, with whom Judges Daughtrey, Moore, Cole and Clay join. Apparently taking a page from the Supreme Court, today the majority dismisses this case by concluding that it is not ripe for adjudication. Why do today what can be done tomorrow? I dissent because I not only believe this case is ripe for review, but because the majority gives unwarranted deferential treatment to the government. Such treatment would not be afforded a private litigant defending against a motion for preliminary injunction, and should not be given here.

I.

The majority adequately recites the facts, but conveniently leaves out what I believe to be an essential element of the case. As the majority correctly states, § 2703(d) allows a court to issue an order based on less than probable cause, allowing the government to search a suspect's email communications stored with an electronic service provider for more than 180 days. Typically, in order to effect such a search, the Stored Communications Act requires the government to notify the suspect of the search. However, § 2703(b)(1)(B) allows the court to grant the government a 90-day delay of the notice if notification would result in "(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." 18 U.S.C. § 2705(a)(2), (b). What the majority leaves out is the fact that while the government was initially granted a 90-day delay before being required to notify Warshak of its searches of his email accounts, when the 90 days expired, the government ignored the statute and failed to notify Warshak of its searches. Over a year went by before Warshak became aware that his emails had been searched. While members of this Court may argue over whether or not the delayed notification section of the Stored Communications Act is constitutional, it is uncontroverted that the government violated the law by failing to notify Warshak 90 days after searching his emails.

The fact that the government was unable to abide by an arguably unconstitutional provision of the Stored Communications Act informs any analysis of Warshak's motion for preliminary injunction. Not only is Warshak alleging that the delayed notification provision of the act is unconstitutional, but he is also alleging that the government cannot be trusted to abide by the actual requirements of that law as written.

II.

Instead of reaching the question that is on everyone's mind — whether or not the delayed notification provision of the Stored Communications Act is constitutional — the majority sidesteps the question and instead finds that Warshak's claims are unripe for judicial review. In finding that Warshak's claims are not quite "fit" for judicial review, the majority analyzes this case under the framework outlined by the Supreme Court in 1967 in *Abbott Laboratories v. Gardner*, 387 U.S. 136, 149 (1967). Under *Abbott Laboratories*, the majority asks whether (1) "the claim [is] 'fit [] . . . for judicial decision'? And (2) what is 'the hardship to the parties of withholding court consideration'?" *See* Maj. Op. at 6-7. My question is this: why not analyze the ripeness of Warshak's claims under the much more recent precedent of this Circuit? This Circuit has held that a ripeness analysis involves three — not two — questions: (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. U.S. Dept. of Justice*,

71 F.3d 563, 568 (6th Cir. 1995) (internal citations omitted). My guess is that it is easier to say that Warshak's case does not fall under the amorphous term "fit", than to confront the actual facts and assess the likelihood of his emails being searched in the future. Because the majority failed to analyze this case under this Circuit's precedent, I will do so here.

The original panel found that the two prior searches of Warshak's email (which violated the terms of the Stored Communications Act), coupled with the government's continued threat of searching his emails without notification, satisfied the first ripeness prong. *Warshak v. U.S.*, 490 F.3d 455, 467 (6th Cir. 2007). The en banc majority disagrees with this conclusion. Instead, it argues that the only reason the government gave in its application for delaying notice of the searches was that disclosure would seriously jeopardize the investigation, and because Warshak has now been indicted, there is no longer any possibility that the investigation would be jeopardized by disclosing a subsequent search of his emails. From this reasoning, the majority further posits that because Warshak is aware of the investigation, the government has no reason for keeping the searches confidential, and the possibility that the government will conduct another *ex parte* search without notice has therefore become "exceedingly remote." Respectfully, I disagree with the majority's Pollyannish view of federal criminal investigations.

First, the government's stated reason in the prior applications for delayed notification is not the only reason recognized by the statute. The statute allows a court to delay notice if it would result in "(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." 18 U.S.C. § 2705(a)(2), (b). Even if we accept the majority's tenuous conclusion that once a suspect is indicted there is no longer a possibility the investigation will be jeopardized or unduly delayed, there are at least four more statutorily recognized reasons for delaying notice that are not negated by the fact of indictment. Post-indictment, there is always a risk that life or physical safety could be endangered. There is a risk that the suspect could flee or destroy evidence. There is a risk that a potential witness could be intimidated. It could always be stated that these issues remain and an application could support delayed notice to search Warshak's emails again. Let us not delude ourselves into thinking that the government's investigation automatically stops once a suspect is indicted. That is not the case at all. Warshak is still the subject of an ongoing investigation. The possibility that he may be the subject of another *ex parte* search is anything but "extremely remote."

Second, the majority makes much of the fact that Warshak "has ample notice of the investigation — indeed notice of the worst sort: He has been indicted." Maj. Op. at 4. The majority seems to suggest that once a suspect is indicted, the government no longer needs to give notice of any subsequent searches because the suspect now knows he is being investigated. Our Constitution suggests something entirely different. While it is true that Warshak knows he is being investigated and now is facing criminal prosecution, it is not true that he has ever been given notice of any clandestine searches of his email. It is certainly possible that Warshak may be subject to future searches, and it is certain that his rights under the Fourth Amendment have not been tolled because of his indictment. The United States must either give notice prior to any future searches or it must apply for a search warrant supported by probable cause. The notice we are concerned with is not whether or not Warshak is aware he is being investigated, but whether or not the United States has abided by the mandates of the Fourth Amendment. The fact that he is on "notice" that he is being investigated has no bearing on the ripeness of his claim.

Under the first prong of this Circuit's ripeness analysis, it is clear that given the factual context of Warshak's claim — the past e-mail seizures, the ongoing nature of the investigation against Warshak, and the government policy of seizing emails without a warrant or notice to the account holder — there is a sufficient "likelihood that the harm alleged by [the] plaintiffs will ever come to pass." *Adult Video Ass'n*, 71 F.3d at 568.

The second prong of our analysis looks to whether the factual record is sufficiently developed to allow for a fair adjudication of Warshak's claim. *Id.* The original panel held, and the district court concluded, that the past seizures of Warshak's e-mails presented 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 clearly renders them a sufficient backdrop for judicial review.

The majority disagrees and contends that the factual record is insufficient because it has "no idea" what types of email accounts the government might investigate and, thus, has no basis for determining whether Warshak has a reasonable expectation of privacy in any single account. I could not disagree more. The original panel opinion sufficiently addressed this issue, analyzing the relevant facts, and pertinent Supreme Court opinions, as well as the most recent precedents of our sister circuits. That panel, as well as the district court, concluded "that individuals maintain a reasonable expectation of privacy in e-mails that are stored with, or sent or received through, a commercial ISP." *Warshak*, 490 F.3d at 473. Rather than address the facts and law cited by the panel's opinion, the majority fails to cite one case dealing with electronic communications in the privacy context, instead relying on a single professor's law review article.

In its zeal to uphold the power of the government to intrude into the privacy of citizens, the majority has forgotten where this case lies procedurally. We are merely at the preliminary injunction stage. Every day in civil litigation across this country, private parties seek preliminary injunctions against other private parties relying on past relevant wrongful conduct and the threat of future wrongful conduct. The factual record necessary to support a preliminary injunction does not have to be complete. In fact, we have stated that "[t]he purpose of a preliminary injunction is merely to preserve the relative positions of the parties until a trial on the merits can be held." *Certified Restoration Dry Cleaning Network, L.L.C. v. Tenke Corp.*, 511 F.3d 535, 542 (6th Cir. 2007) (quoting *Univ. of Texas v. Camenisch*, 451 U.S. 390, 395 (1981)). "Given this limited purpose, a preliminary injunction is customarily granted on the basis of procedures that are less formal and evidence that is less complete than in a trial on the merits." *Id.* Warshak "is not required to prove his case in full at a preliminary injunction hearing and the findings of fact and conclusions of law made by a court granting the preliminary injunction are not binding at trial on the merits." *Id.* I challenge the majority to find a case where this or any other court has not granted a preliminary injunction against a defendant who has twice previously committed wrongful conduct, has a written policy in favor of committing the wrongful conduct, and refuses to promise not to commit the wrongful conduct in the future. Despite the fact that a violation of one of the bedrock principles of the Bill of Rights has been alleged, today the majority has decided to treat the government more favorably than a private litigant would be treated in a similar preliminary injunction setting.

Turning to the final prong of this Circuit's ripeness analysis, I believe the only party that would suffer undue hardship if the preliminary injunction were not granted is Warshak. 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. The government, on the other hand, suffers no hardship if the preliminary injunction is granted. By the terms of the modified preliminary injunction, the government is prohibited only "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. . . ." *Warshak*, 490 F.3d at 482. The United States may still seek a search warrant based on probable cause, or subpoena the contents of an email account, and the *ex parte* search and delayed notification procedures of § 2703(d) are still available if the terms of the email account establish that the account holder has

no reasonable expectation of privacy in the account. The only tool taken from the government is the one that allegedly violates the Fourth Amendment. While that one investigatory tool is now gone, Warshak's constitutional rights remain intact. Hopefully, given the mandates of the Constitution, we should strive to maintain that status quo through a preliminary injunction. We should not allow a citizen's constitutional rights to be violated when the United States is not even minimally burdened here in its criminal investigations.

Based on the foregoing, I respectfully dissent.

III.

While I am saddened, I am not surprised by today's ruling. It is but another step in the ongoing degradation of civil rights in the courts of this country. The majority makes much of the fact that facial challenges are no way to litigate the constitutional validity of certain laws. Yet our Supreme Court has no problem striking down a handgun ban enacted by a democratically elected city government on a facial basis. *See Dist. of Columbia v. Heller*, — U.S. —, 2008 WL 2520816 (June 26, 2008). History tells us that it is not the fact that a constitutional right is at issue that portends the outcome of a case, but rather what specific right we are talking about. If it is free speech, freedom of religion, or the right to bear arms, we are quick to strike down laws that curtail those freedoms. But if we are discussing the Fourth Amendment's right to be free from unreasonable searches and seizures, heaven forbid that we should intrude on the government's investigatory province and actually require it to abide by the mandates of the Bill of Rights. I can only imagine what our founding fathers would think of this decision. If I were to tell James Otis and John Adams that a citizen's private correspondence is now potentially subject to *ex parte* and unannounced searches by the government without a warrant supported by probable cause, what would they say? Probably nothing, they would be left speechless.