
No. 08-4085

IN THE
UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

STEVEN WARSHAK,
Appellant

v.

UNITED STATES OF AMERICA,
Appellee

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

BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION, ACLU OF OHIO FOUNDATION, INC. AND CENTER FOR DEMOCRACY AND TECHNOLOGY SUPPORTING THE APPELLANT AND URGING ACQUITTAL OR ORDER FOR NEW TRIAL

Kevin S. Bankston
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333 x 126
(415) 436-9993 – facsimile

Attorney for *Amici Curiae*

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER ENTITIES WITH A DIRECT FINANCIAL INTEREST IN LITIGATION

Pursuant to FRAP 26.1, *amici* Electronic Frontier Foundation ("EFF"), ACLU of Ohio Foundation, Inc. ("ACLU of Ohio") and Center for Democracy and Technology ("CDT"), 501(c)(3) non-profit corporations incorporated in the States of Massachusetts, Ohio, and Washington, D.C., respectively, make the following disclosure:

1. No *amicus* is a publicly held corporation or other publicly held entity.

2. *Amici* have no parent corporations.

3. No publicly held corporation or other publicly held entity owns 10% or more of any *amicus*.

4. No *amicus* is a trade association.

/s/Kevin S. Bankston June 9, 2009
Kevin S. Bankston
Senior Staff Attorney
Electronic Frontier Foundation

STATEMENT OF AMICI CURIAE

Amici are non-profit public interest organizations seeking to ensure Fourth Amendment protections in the face of advancing technology.

The Electronic Frontier Foundation ("EFF") is a non-profit, member-supported civil liberties organization working to protect free speech and privacy rights in the online world. As part of that mission, EFF has served as counsel or *amicus* in key cases addressing electronic privacy statutes and the Fourth Amendment as applied to the Internet and other new technologies. With more than 10,000 dues-paying members, EFF represents the interests of technology users in both court cases and in broader policy debates surrounding the application of law in the digital age, and publishes a comprehensive archive of digital civil liberties information at one of the most linked-to web sites in the world, www.eff.org.

The ACLU of Ohio Foundation, Inc. ("ACLU of Ohio") is devoted to the preservation and advancement of civil liberties for all Ohioans through public education and litigation. The ACLU of Ohio regularly appears in this Court as either direct counsel or *amicus* to serve those ends. Because of its particular commitment to rights of privacy and due process, the ACLU of Ohio has a special interest in, and expertise to address, the application of the law in this case.

The Center for Democracy and Technology ("CDT") is a non-profit public interest organization focused on privacy and other civil liberties issues affecting the Internet and other communications networks. CDT represents the public's interest in an open, decentralized Internet and promotes the constitutional and democratic values of free expression.

Appellee United States of America has chosen not to consent to the filing of this brief, which is therefore accompanied by a motion seeking leave to file pursuant to FRAP 29(b).

NOTE REGARDING RECORD CITATIONS

As in the Appellants' Brief, citations to the record which appear in this Brief are by record document number and, where relevant, the page number. For example, "R1" refers to docket number 1, the indictment; "R489:20" refers to docket number 489, the transcript of proceedings for January 9, 2008, at page 20. The Addendum to Appellants' Brief contains a list of the relevant entries in the electronic case record. The trial exhibits referenced in the Brief may be found in the Appendix filed with Appellants' Brief, along with transcripts and other documents which are not part of the electronic record. Citations to "A____" refer to materials contained in that Appendix.

STATEMENT OF ISSUES

1. Did the government rely in good faith on the Stored Communications Act in seizing Warshak's emails, when it violated both that statute and the Justice Department's own search and seizure manual by ordering Warshak's email provider to prospectively "preserve" emails that the government otherwise could only have obtained using a court order based on probable cause issued under the Wiretap Act?

2. Did this "back door wiretap" of Warshak's emails, equivalent to a telephone wiretap requiring a search warrant under the Fourth Amendment, violate Warshak's reasonable expectation of privacy such that the emails should have been suppressed?

STATEMENT OF RELEVANT FACTS

On October 25, 2004, the government issued to Warshak's email service provider NuVox a directive, purportedly based on the authority of 18 U.S.C. § 2703(f), requiring that NuVox prospectively "preserve" copies of Warshak's incoming and outgoing emails. R114, Exh. 6. NuVox did not create or maintain such copies in the ordinary course of its business: incoming emails were deleted from NuVox's system as soon as Warshak downloaded them, *see Warshak v. United States*, no. 06-357, R43, Exh. 2, while there is no indication that outgoing emails were stored except temporarily while in the process of transmission. However, NuVox complied with the "preservation" request and began to archive copies of Warshak's emails based on the government's demand. Warshak was not notified.

After NuVox had secretly collected several months' worth of Warshak's emails, the government sought their disclosure using the Stored Communications Act. First, in January 2005, the government issued a subpoena to NuVox under 18 U.S.C. § 2703(b) to obtain the emails preserved up until that point, A00, and then returned for even more in May 2005 with a court order issued under 18 U.S.C. § 2703(d). A1-7. All told, approximately 27,740 of Warshak's private emails were "preserved" and disclosed to the government by NuVox. R114:15. The government did not notify Warshak of this until the summer of 2006. R114:31.

INTRODUCTION AND SUMMARY OF ARGUMENT

Amici respectfully submit this brief in support of Appellant Steven Warshak on the first two of the issues he has presented on appeal: first, whether the government's search and seizure of Warshak's emails without notice and without a search warrant violated the Fourth Amendment, and second, whether this search and seizure was undertaken in good faith reliance on the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701-2712. *See* Appellants' Br. ("Warshak Br.") 1.

Amici urge this Court to find that Warshak had a reasonable expectation of privacy in the contents of his email even when those messages were in the possession of his email provider NuVox, and that the Fourth Amendment required the government to obtain a probable cause warrant before seizing those emails. *Amici* further urge this Court to find that those emails should have been suppressed by the District Court, as the

government did not rely in good faith on the SCA but instead violated that statute and the Justice Department's own policies when seizing Warshak's emails.

As *Amici* show in Section I, the government blatantly exceeded the scope of the SCA and violated the Wiretap Act, 18 U.S.C. §§ 2510-2522, by secretly compelling NuVox to *prospectively* "preserve" Warshak's emails, emails that the government later obtained improperly and without a probable cause warrant using the SCA's procedures. Put simply, the government misused the SCA to conduct a "back door wiretap" of Warshak's emails and bypass the Wiretap Act's strict requirements, including its requirement of probable cause. Because the government unreasonably exceeded the SCA's authority and violated the Wiretap Act, the District Court erred in applying the exception to the exclusionary rule established in *Illinois v. Krull*, 480 U.S. 340 (1987), for Fourth Amendment violations undertaken based on an objectively reasonable reliance on statutory authority.

In Section II, *Amici* demonstrate that the Fourth Amendment was indeed violated and that the government's "back door wiretap" of Warshak's emails, which violated Warshak's reasonable expectation of privacy, was a search and seizure requiring a probable cause warrant and not a compelled disclosure requiring only reasonableness. This conclusion is mandated by the Supreme Court's electronic eavesdropping decisions, is consistent with recent persuasive authority concerning the Fourth Amendment's application to email and other electronic communications, and is supported by the

reasoning of this court in *Warshak v. United States*, 490 F.3d 455 (6th Cir. 2007) ("*Warshak I*"). Though that panel decision was vacated *en banc* on ripeness grounds,[1] its reasoning is still sound, has been adopted by other courts, and should be applied here.

ARGUMENT

I. THE GOVERNMENT'S SEARCH AND SEIZURE OF WARSHAK'S PROSPECTIVELY "PRESERVED" EMAILS WAS NOT SUPPORTED BY AN OBJECTIVELY REASONABLE RELIANCE ON THE STORED COMMUNICATIONS ACT.

The District Court erred in finding that the exclusionary rule does not apply to Mr. Warshak's emails under the good faith exception established by *Illinois v. Krull*, 480 U.S. 340 (1987). In *Krull*, the Supreme Court held that evidence obtained in violation of the Fourth Amendment is not subject to the exclusionary rule if the government relied in good faith on a statutory authority, even if that statute is later held unconstitutional. *Id.* at 349-50. However, the *Krull* exception applies only where the government's reliance on the statute was objectively reasonable and where its conduct was within the scope of its authority under the statute. *Id.* at 355, 360 n.17. Here, neither condition is satisfied. The government plainly exceeded its statutory authority, and did so unreasonably, in violation of the statute's plain language and the Justice Department's own policies.

---

[1] *See Warshak v. United States*, 532 F.3d 521 (6th Cir. 2008) (*en banc*) ("*Warshak II*").

The government's lack of a good faith reliance on the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701-2712, is evidenced not only by that statute's obvious unconstitutionality, Warshak Br. 32-33, but also by the government's various failures to comply with that statute. Warshak Br. 33-39. *Amici* here focus on one of those failures, which by itself is enough to dispose of the issue: the government's misuse of 18 U.S.C. § 2703(f) to compel email provider NuVox to prospectively "preserve" Warshak's emails for the government, rather than seeking a court order based on probable cause authorizing the interception of Warshak's emails pursuant to the Wiretap Act, 18 U.S.C. §§ 2510-2522.

Such an end-run around the warrant requirement is just the kind of conduct that the exclusionary rule was meant to deter. The District Court's failure to apply that rule to the fruits of the government's "back door wiretap" represented the creation of a new good faith exception with no basis in law: an exception for Fourth Amendment violations based on incorrect and unreasonable reliance on a statutory authorization. This Court should not affirm such an unwarranted extension of *Krull* to protect the government's patently illegal and unconstitutional conduct.

A. The Stored Communications Act Did Not Authorize the Government to Demand the Prospective "Preservation" of Warshak's Emails and Circumvent the Strict Procedures of the Wiretap Act.

Unlike in *Krull*, the government here acted far outside the bounds of the relevant statute, using the SCA's provision for the preservation of

evidence at 18 U.S.C. § 2703(f) to prospectively acquire Warshak's emails in a manner that otherwise could only have been authorized under the much stricter procedures of the Wiretap Act.

In particular, by letter to NuVox on October 25, 2004, the government requested under the purported authority of section 2703(f) that NuVox "preserve" Warshak's emails, including future emails that did not yet exist: "In the event of pop-server type messages, *prospective* preservation is requested…. This preservation request applies to … all stored or *future* electronic communications…." A00 (emphasis added).[2] The government then later obtained those "preserved" emails, emails that NuVox would not otherwise have had in its possession, without a warrant, first using a subpoena, and later a court order under 18 U.S.C. § 2703(d).

However, the plain language of section 2703(f) does not authorize the government to request the prospective preservation of future emails, and the government's reliance on that section despite its plain language was outside the statute's scope and was not objectively reasonable. In relevant part, that section provides that:

> 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

---

[2] Although referred to as a "request," preservation letters issued under section 2703(f) "shall"—and therefore, must—be complied with. *Id.* *See also*, *e.g.*, *Alabama v. Bozeman*, 533 U.S. 146, 153 (2001) ("The word 'shall' is ordinarily the 'language of command.'") (quoting *Escoe v. Zerbst*, 295 U.S. 490, 493 (1935)).

> other evidence *in its possession* pending the issuance of a court order or other process.

18 U.S.C. § 2703(f)(1) (emphasis added). Based on this plain language, section 2703(f) may be used only to preserve pre-existing evidence already in a service provider's possession and cannot be used to require a service provider to create or collect evidence that has not yet come into being. One cannot "preserve" that which one does not possess, and Warshak's future correspondence was not yet "in [NuVox's] possession" when the government made its request. Nor would those emails, when they came into existence, have remained in NuVox's possession but for the government's "request."

The Justice Department's own surveillance manual reiterates section 2703(f)'s plain meaning and instructs that such prospective surveillance of communications content may be authorized only under the procedures of the Wiretap Act:

> Agents may direct providers to preserve existing records pending the issuance of compulsory legal process. *Such requests have no prospective effect*, however…. Agents who send § 2703(f) letters to network service providers should be aware of [a] limitation[]. [T]he authority to direct providers to preserve records and other evidence *is not prospective*. That is, § 2703(f) letters can order a provider to preserve records that have already been created, but *cannot order providers to preserve records not yet made*. If agents want providers to record information about future electronic communications, they *must* comply with the electronic surveillance statutes discussed in Chapter 4 [*i.e.*, the Wiretap Act for communications content, and the Pen Register Statute for non-content communications information].

Computer Crime and Intellectual Property Section, Criminal Division, U.S. Department of Justice, *Searching and Seizing Computers and Obtaining Evidence in Criminal Investigations* ("DOJ Manual"), ch. III, § (G)(1) at 104-05, *available at* http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.pdf (last visited June 9, 2009) (emphasis added).[3]

Notably, the DOJ Manual's appendices provide model letters and applications for officers to implement SCA processes, including a model letter requesting preservation under section 2703(f). The third paragraph of the first page of that model letter is solely devoted to ensuring that the service provider does not mistakenly engage in prospective surveillance based on the letter: "This request applies only retrospectively. It does not in any way obligate you to capture and preserve new information that arises after the date of this request." DOJ Manual, App. C at 173. The government conspicuously omitted this paragraph from the preservation letter it sent to NuVox, which instead expressly commanded that NuVox capture new emails sent and received after the date of the request. A00.

---

[3] This plain language reading is shared by the U.S. Internet Service Provider Association ("USISPA") as explained in its legal compliance guide for providers: "Preservation requests only apply to stored communications and records that the provider has in its possession at the time of the request." USISPA, *Electronic Evidence Compliance—A Guide for Internet Service Providers*, 18 Berkeley Tech. L.J. 945, 970 (2003).

As the DOJ Manual reflects, the plain language reading of 18 U.S.C. § 2703(f) is consistent with the overall structure of the surveillance statutes, where the SCA is reserved for retrospective surveillance of previously stored information and the Wiretap Act and the Pen Register Statute regulate the prospective surveillance of communications yet to be created. *See* DOJ Manual at 104-05; *see also id.* at ix, 24 ("Any real-time interception of electronically transmitted data in the United States must comply strictly with the requirements of Title III, 18 U.S.C. §§ 2510-2522 [The Wiretap Act], or the Pen/Trap statute, 18 U.S.C. §§ 3121-3127," while "18 U.S.C. §§ 2701-12 ("ECPA") [*i.e.*, the SCA]…governs how investigators can obtain stored account records and contents from network service providers….").

This retrospective/prospective dichotomy in the surveillance statutes is uncontroversial and widely recognized by academic experts, including both critics and advocates of the government's authority under those statutes. *See, e.g.*, Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 Geo. Wash. L. Rev. 1557, 1565 (2004) ("The Wiretap Act and Pen Register statute regulate prospective surveillance…and the SCA governs retrospective surveillance…."); Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 Nw. U. L. Rev. 607, 618 n.47 (2003) ("[T]he law draws a distinction between prospective Internet surveillance…governed by the Wiretap Act and the Pen Register Statute…and retrospective

surveillance…governed by the [SCA portion of] Electronic Communications Privacy Act….").[4] The SCA's limitation to retrospective surveillance has also been reiterated by federal magistrate courts recently grappling with the question of what statutory authority if any the government may use to conduct prospective surveillance of a cell phone's location.[5] As one such court has held, "the SCA simply is not and never was intended to be a statute that authorizes prospective surveillance." *In re U.S. for Orders Authorizing Installation and Use of Pen Registers & Caller Identification Devices on Telephone Numbers*, 416 F. Supp. 2d 390, 395 (D. Md. 2006).

If the government had complied with the SCA by seeking only the preservation and the disclosure of emails in NuVox's possession at the time of its request, it would only have obtained the few unread emails awaiting download in Warshak's email inbox at that moment, rather than the six months of incoming and outgoing correspondence that it actually obtained. Put another way, the government's preservation request to NuVox was a

---

[4] *See also* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 Ala. L. Rev. 9, 46-52 (2004) (providing overview of different categories of surveillance).

[5] *See*, *e.g.*, *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747, 760-61 (S.D. Tex. 2005) ("If Congress had not intended the SCA to be retrospective in nature, it would have included the same prospective features it built into the wiretap and pen/trap statutes."); *In re Application of United States for Order*, 497 F. Supp. 2d 301, 309 (D.P.R. 2007) ("Congress's decision not to include in the SCA any provisions typical of prospective surveillance statutes indicates its intent that the SCA be used for the disclosure of historic and not prospective data.").

"but-for" cause of its obtaining the email without a warrant using the SCA. *See* R247:12 (noting government's argument, based on *Hudson v. Michigan*, 547 U.S. 586 (2006), that only violations of the statute that were a "but-for" cause of the email seizure are relevant to the question of good faith reliance).

Absent misuse of section 2703(f), the Wiretap Act is the only statutory authority the government could have used to command NuVox's "preservation"—*i.e.*, interception—of Warshak's future emails. *See generally* 18 U.S.C. §§ 2511 (generally prohibiting interception of electronic communications) and 2518 (providing procedures for issuance of court order authorizing interception); *see also infra* Section II(B) (describing the Wiretap Act's requirements). Indeed, the Justice Department itself has argued elsewhere that conduct similar if not identical to NuVox's prospective "preservation" of Warshak's emails constitutes an interception subject to the Wiretap Act. In *United States v. Councilman*, the government prosecuted under the Wiretap Act an email provider that had allegedly reconfigured its facilities to surreptitiously make copies of customers' incoming emails for its own use. 418 F.3d 67, 70-71 (1st Cir. 2005) (*en banc*). There, the First Circuit sitting *en banc* held that the email provider's copying of incoming emails while in "transient electronic storage that is intrinsic to the communication process for such communications" was an interception of those communications in violation of the Wiretap Act. *Id.* at 79-80.

Councilman's reasoning applies here. It is undisputed that NuVox's only storage of Warshak's email in the ordinary course of its business was transient and intrinsic to the communication process. Incoming messages were only stored in a customer's email inbox up until the customer first downloaded them from NuVox's email server. *See Warshak v. United States*, no. 06-357, R43, Exh. 2 (email from NuVox explaining that emails are automatically deleted from NuVox's email servers as soon as they are received by the user). Similarly, there is nothing in the record indicating that NuVox stored outgoing messages except for during the momentary transmission of those emails through the NuVox servers.[6] Under *Councilman*, NuVox's copying of Warshak's emails while they were in such intrinsic transient storage was an interception of those communications. 418 F.3d at 79-80.

The SCA does not and was not intended to enable such a "back door wiretap" to avoid the stricter procedures of the Wiretap Act. As explained by Professor Orin Kerr, who co-authored the DOJ Manual while an attorney for the government and is now a noted academic expert in the field:

> When stored communications are accessed in a way that makes the access the functional equivalent of a wiretap, the surveillance should be regulated by the Wiretap Act, not the SCA. For example, if an agent lines up a string of 2703(a) orders and serves one order per hour, I think that is the

[6] Although some types of email services provide archival storage of sent messages—for example, web-based email services such as Microsoft's Hotmail or Google's Gmail—there is no indication in the record that NuVox provided any such service to Warshak.

> functional equivalent of a wiretap. It is reasonable to infer that the purpose of the surveillance is to obtain copies of all incoming messages, not to look for communications stored in a target's inbox. Similarly, it is the functional equivalent of a wiretap if an agent installs software that copies incoming messages a few milliseconds after they arrive.

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, 1232 (2004). NuVox's reconfiguration of its service to capture Warshak's emails outside the ordinary course of business, like the examples posed by Kerr, was the functional equivalent of a wiretap. Indeed, as *Councilman* confirmed, such conduct *is* a wiretap, *i.e.*, an interception regulated by the Wiretap Act. If the government had wanted to procure NuVox's assistance in conducting a wiretap, it should have obtained an order requiring such assistance under the Wiretap Act.[7] *See* 18 U.S.C. § 2518(4) (providing for orders to communications providers requiring their assistance in accomplishing court-authorized interceptions).

Instead, the government misused the SCA to avoid the strictures of the Wiretap Act. The appropriate counter-incentive to prevent such illegal and (as explained *infra* Section II) unconstitutional surveillance is application of the Fourth Amendment's exclusionary rule, which could and should have been applied below.

---

[7] Notably, even if the government had properly obtained a court order under the Wiretap Act, that order would only have authorized the interception of Warshak's emails for thirty days, as opposed to the *six months* of email obtained here. *See* 18 U.S.C. § 2518(5).

B. The District Court Erred by Failing to Suppress Warshak's Emails, Based on its Misapplication of the Reasonable Reliance Exception to the Exclusionary Rule.

Despite its recognition that the government plainly exceeded the SCA's authority in ordering the prospective "preservation" of Warshak's emails, the District Court summarily concluded in a few sentences that the illegally obtained evidence should not be suppressed:

> [T]he Court holds [that *Krull*'s] good-faith exception to the exclusionary rule applies…. The alleged violations of the SCA do not amount to unreasonable actions in violation of the Fourth Amendment. The government's prospective requests did not comply with the SCA or with the D.O.J.'s guidelines, and yet, such infraction does not constitute unreasonable government action in the context of the alleged large-scale mail and bank fraud at hand.

R247:12-13. The District Court misconstrued *Krull* and then misapplied its limited exception so as to turn the Fourth Amendment on its head. First, the District Court's conclusion that the government did not violate the Fourth Amendment is a contradiction unto itself. If there were no Fourth Amendment violation, there would be no need to consider an exception to the exclusionary rule because that rule would not apply. Second, rather than follow *Krull*'s actual rule—that evidence derived from Fourth Amendment violations undertaken based on good faith reliance on a statutory authority are not subject to the exclusionary rule—the District Court instead created a new exception out of whole cloth, based on the "large[]scale" of the alleged crime being investigated. *Id.* Such a "big crime" exception, which would eviscerate the the protections of the surveillance statutes and the Fourth

Amendment, simply does not exist; under a proper application of *Krull*, the emails should have been suppressed.

In *Krull*, the Supreme Court extended the good faith exception to the exclusionary rule established in *United States v. Leon*, 468 U.S. 897 (1984), for evidence obtained by officers acting in reasonable reliance on a search warrant. Looking to the exclusionary rule's ultimate purpose—the deterrence of officers' violation of the Fourth Amendment—the Court in *Krull* relied on *Leon* in holding that "application of the exclusionary rule to suppress evidence obtained by an officer acting in objectively reasonable reliance on a statute would have as little deterrent effect on the officer's actions as…when an officer acts in objectively reasonable reliance on a warrant." 480 U.S. at 349. Paraphrasing *Leon*, the Court held: "Penalizing the officer for the [legislature's] error, *rather than his own*, cannot logically contribute to the deterrence of Fourth Amendment violations," *id.* at 350 (emphasis added, brackets in original), "because the officer [is] merely carrying out [his] responsibilit[y] in implementing the statute," *id.* at 355, n.12. Importantly, the inquiry into whether an officer acted in good faith reliance "is confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal…." *Leon*, 468 U.S. at 922, n.23.

Consistent with *Leon*'s analysis of the exclusionary rule's deterrent effect, the *Krull* court expressly refused to extend the good faith exception to conduct that was *not* authorized by the relied-upon statute:

> *[W]e decline the State's invitation to recognize an exception for an officer who erroneously, but in good faith, believes he is acting within the scope of a statute*…. [T]he question whether the exclusionary rule is applicable in a particular context depends significantly upon the actors who are making the relevant decision that the rule is designed to influence. The answer to this question might well be different when police officers act outside the scope of a statute, albeit in good faith. In that context, the relevant actors are not legislators or magistrates, but police officers who concededly are "engaged in the often competitive enterprise of ferreting out crime." *Johnson v. United States*, 333 U.S. 10, 14 (1948).

Krull, 480 U.S. at 360, n. 17 (emphasis added). In other words, where the error *was* the officer's, rather than that of the legislature or the magistrate, the good faith exception to the exclusionary rule does not apply—even if that error was objectively reasonable.

In the present case, not only did the officers err and act outside of the scope of the SCA, but that error was not even objectively reasonable. A reasonably well trained officer, faced with the plainly limited language of 18 U.S.C. § 2703(f) and the Justice Department's own guidance on the issue, would not toss aside the Justice Department's model preservation request and instead draft her own request seeking prospective "preservation" of emails in violation of the SCA and the Wiretap Act. By applying the good faith exception here, the District Court not only ignored the *Krull* court's refusal to extend the exception to an officer's erroneous but objectively reasonable reliance on a statute, *Krull*, 480 U.S. at 360 n. 17, but went a step farther, applying the exception even when the error was *not* in good faith.

There is no basis in law for such a "bad faith erroneous reliance" exception,[8] and as one court has explained at length, the extension of *Krull* to even good faith mistakes would be as dangerous as it is unsupported:

> [U]nder *Leon* and *Krull* the officer's good faith alone is not sufficient to validate the search and seizure; the officer must also be acting on the authority of a seemingly valid warrant or statute. Here, there is no such reliance, but quite the opposite. The officers were acting in defiance of, not reliance on, the language of a statute limiting the authority of officers…. [T]o adopt the extension of the good-faith exception proposed by the State would essentially eviscerate the exclusionary rule as it is currently enforced. Police officers would be encouraged to defy the plain language of statutes as written in favor of their own interpretations in conducting searches and seizures.

People v. Madison, 520 N.E.2d 374, 380 (Ill. 1988), *cert. denied*, *Illinois v. Madison*, 488 U.S. 907 (1988).

Here, the government did not rely on but instead defied the SCA and the Wiretap Act by obtaining Warshak's prospectively "preserved" emails, and such conduct cannot be condoned by application of the good faith exception. "A ruling admitting evidence in a criminal trial...has the necessary effect of legitimizing the conduct which produced the evidence, while an application of the exclusionary rule withholds the constitutional imprimatur." *Terry v. Ohio*, 392 U.S. 1, 13 (1968). This Court should not

---

[8] The District Court's apparent reliance on *United States v. Ferguson*, 508 F. Supp. 2d 7 (D.D.C. 2007), is inapposite. *See* R247:13 (citing *Ferguson*). Although the court in that case applied the *Krull* exception to the government's use of the SCA to obtain already stored email without a warrant, that case did not involve the prospective "preservation" of emails that is dispositive here.

legitimize the government's conduct here, but instead withhold the constitutional imprimatur by finding that the District Court erred in failing to suppress the Warshak email evidence. To hold otherwise would incentivize similarly blatant misuse of the SCA and defiance of the Wiretap Act in the future, in violation not only of statute but also the Fourth Amendment, as detailed next.

II. THE GOVERNMENT'S SEIZURE OF MR. WARSHAK'S EMAILS VIOLATED THE FOURTH AMENDMENT.

This Court should conclude, as it did in *Warshak I*, that "individuals maintain a reasonable expectation of privacy in e-mails that are stored with, or sent or received through, a commercial ISP," and that the government's secret seizure of Warshak's emails required a warrant. 490 F.3d at 473, 475. Although its decision was vacated on ripeness grounds, the reasoning of *Warshak I* is sound and should be followed here as it has been elsewhere. *See*, *e.g.*, *In re Applications of United States for Orders Authorizing the Use of Pen Registers & Trap & Trace Devices*, 515 F. Supp. 2d 325, 337-38 (E.D.N.Y. 2007) (following *Warshak I*'s reasoning to conclude that telephone users have a reasonable expectation of privacy in the content digits dialed after a telephone call has commenced); *United States v. D'Andrea*, 497 F. Supp. 2d 117, 121 (D. Mass. 2007) (noting the persuasiveness of *Warshak I* when finding that "a person who avails herself of a website's password protection should be able to claim a reasonable expectation of privacy in the site's contents").

Because the issue of the Fourth Amendment's application to email was addressed so capably in *Warshak I*, supported by extensive briefing from *Amici*[9] and others,[10] *Amici* will focus here on briefly summarizing and providing additional support for that decision's conclusions, and on pointing out how this case's narrow focus on the prospectively "preserved" NuVox emails makes it an even easier case than *Warshak I*.

A. Warshak Possessed a Reasonable Expectation of Privacy in His Emails Under *Katz v. United States*.

This Court is now faced with a decision that will impact the privacy rights of millions of email users. Faced with a similarly momentous decision regarding the Fourth Amendment's application to a new communications technology—the telephone—and over Justice Brandeis' famously prescient objections, the Supreme Court in 1928 took the wrong path and held that the Fourth Amendment did not protect the privacy of telephone calls. *Olmstead v. United States*, 277 U.S. 438, 464-65 (1928). This mistake was not corrected until 1967. *See Berger v. New York*, 388

---

[9] Brief of *Amici Curiae* Electronic Frontier Foundation, *et al*. Supporting the Appellee and Urging Affirmance, *Warshak v. United States*, 490 F.3d 455 (6th Cir. 2007), *available at* http://w2.eff.org/legal/cases/warshak_v_usa/warshak_amicus.pdf (last visited June 9, 2009).

[10] Brief for Professors of Electronic Privacy Law and Internet Law as *Amici Curiae* Supporting the Appellee and Urging Affirmance, *Warshak v. United States*, 490 F.3d 455 (6th Cir. 2007), *available at* http://w2.eff.org/legal/cases/warshak_v_usa/amicus_final_law_profs.pdf (last visited June 9, 2009).

U.S. 41 (1967) (finding state's electronic eavesdropping statute facially unconstitutional for lack of adequate Fourth Amendment safeguards); *Katz v. United States,* 389 U.S. at 347 (finding a Fourth Amendment expectation of privacy in telephone calls made by defendant from a closed phone booth). This Court should avoid the mistake of *Olmstead* and instead follow the lessons of *Berger* and *Katz*, as it did in *Warshak I*.

The Supreme Court in *Katz* wisely rejected *Olmstead*'s strictly property-based conception of the Fourth Amendment, holding instead that "the Fourth Amendment protects people, not places," and in particular, people's reasonable expectations of privacy. *Id*. at 351; *see also id*. at 360-61 (Harlan, J., concurring) (Fourth Amendment protections apply where "a person [has] exhibited an actual (subjective) expectation of privacy…that society is prepared to recognize as [objectively] 'reasonable.'"). In this regard, Warshak's emails are no different from Mr. Katz's phone calls.

First, there is no apparent dispute over the fact that Warshak subjectively expected that his emails would remain private, as evidenced by the extensive private and personal uses to which he put his NuVox email account. *See* Warshak Br. 39-40 (describing Warshak's use of NuVox account and concluding that, "[i]n sum, Warshak's entire business and personal life was contained within the compass of the six months of seized emails."). Courts in similar contexts have found a subjective expectation of privacy based on the private and personal nature of the communications at issue. *See United States v. Maxwell*, 45 M.J. 406, 417 (C.A.A.F. 1996)

(looking to "tenor and content" of emails to determine subjective expectation of privacy); *see also Gonzales v. Google, Inc.*, 234 F.R.D. 674, 687 (N.D. Cal. 2006) (noting that the prevalence of internet searches on sensitive topics, including "the prevalence of Internet searches for sexually explicit material," indicates that searchers do not expect Google's logs of their queries to be publicly revealed).

The remaining question of objective reasonability must be considered in the context of one overriding fact: millions of Americans such as Warshak use email every day for practically every type of personal business. Private messages and conversations that once would have been communicated via postal mail or telephone now occur through email. It is so obvious as to "g[o] without saying that like the telephone earlier in our history, e-mail is an ever-increasing mode of private communications, and protecting shared communications through this medium is as important to Fourth Amendment principles today as protecting telephone conversations has been in the past." *Warshak I,* 490 F.3d at 473, *citing 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."); *see also Kyllo v. United States*, 533 U.S. 27, 34 (2001) (recognizing that technological advances must not be allowed to erode society's expectation of privacy against the government).

As correctly held in *Warshak I*, the myriad private uses of email demonstrate society's expectation that their email messages are as private as

a sealed letter, a telephone call, or papers that are kept in the home or a safety deposit box. *See Warshak I*, 490 F.3d at 469-72.[11] This conclusion is consistent with prior appellate rulings on the Fourth Amendment's application to modern communications technologies. *Id.* at 472-73 (discussing cases). It is additionally supported by two previous decisions of the U.S. Court of Appeals for the Armed Forces finding that email account holders have a reasonable expectation of privacy in email transmitted and stored by an email provider. *See Maxwell*, 45 M.J. 406; *United States v. Long*, 64 M.J. 57 (C.A.A.F. 2006).

Warshak I's conclusion is further bolstered by two more recent decisions from the Ninth Circuit.[12] First, in *United States v. Forrester*, the

---

[11] An equally apt analogy not mentioned by *Warshak I* is that of a rented residence or hotel room. *See Stoner v. California*, 376 U.S. 483, 489-90 (1964) (holding that hotel guest, like the renter of a home, retains an expectation of privacy against government intrusion despite her implied or express permission of the owner's entry for cleaning and repairs).

[12] Based in part on *Warshak I* and these newer rulings, there is a growing consensus in the academic literature that email stored with a provider should be protected by the Fourth Amendment. *See, e.g.*, Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, Stan. L. Rev. (forthcoming) (manuscript at 45, *available at* http://ssrn.com/abstract=1348322) (last visited June 9, 2009) (concluding that "the Fourth Amendment ordinarily requires a warrant for the collection of the contents of Internet communications," and that "[c]ontents stored in and transferred through Internet accounts should be protected with the same default warrant requirement" that already protects "homes, telephone calls, and postal letters."); Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-Mail*, 2008 U. Chi. Legal F. 121 (2008)
.

Ninth Circuit confirmed the protected status of email content under the Fourth Amendment. 512 F.3d 500 (9th Cir. 2008), *cert. denied*, 129 S. Ct. 249 (2008). "When the government obtains the to/ from addresses of a person's e-mails…it does not find out the *contents* of the messages…. *Smith* and *Katz* drew a clear line between unprotected addressing information and protected content information that the government did not cross here." *Id.* at 510 (emphasis added). That line was crossed in Warshak's case.

Next, in *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892 (9th Cir. 2008), the Ninth Circuit reinforced the reasoning of *Warshak I* by finding that the Fourth Amendment protected communications content in storage with a communications provider, although in that case, the stored communications were text messages stored with a wireless provider. The court held:

> We see no meaningful difference between the e-mails at issue in *Forrester* and the text messages at issue here. Both are sent from user to user via a service provider that stores the messages on its servers. Similarly, as in *Forrester*, we also see no meaningful distinction between text messages and letters. As with letters and e-mails…users do have a reasonable expectation of privacy in the content of their text messages vis-a-vis the service provider.

Id. at 905. Here, where in the ordinary course of business NuVox only stored messages incident to their transmission, the user's expectation of privacy is even clearer than in *Quon*, where the provider archived copies of past messages as a part of its service. *See id.* at 900.

In sum, these two recent decisions further confirm that *Warshak I* was correctly decided on the merits, and that email users—including Warshak—possess a reasonable expectation of privacy in the content of their emails even while it is in the possession of a service provider.

B. NuVox's Ability to Access Warshak's Emails, Like the Telephone Company's Ability to Access Phone Call Content, Did Not Diminish Warshak's Expectation of Privacy.

Warshak I correctly rejected government's argument that because email providers have the technical ability to access—and in some cases may access—the email content stored on their computers, there is no expectation of privacy based on the Supreme Court's decisions in *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976). *See Warshak I*, 490 F.3d at 469-75; *see also* Bellia & Freiwald, *supra* at 147-169 (comprehensively addressing the same argument). However, *Amici* wish to reiterate, as *Katz* and *Smith* make clear, that the fact of provider access is irrelevant to the customer's expectation of privacy in the contents of their communications. "[A] telephone conversation itself must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment," yet is nevertheless protected under *Katz*. *Smith*, 442 U.S. at 746 (Stewart, J., dissenting).

Importantly, *Katz* found that the Fourth Amendment protected phone subscribers' privacy despite the fact that, at common law, they have impliedly consented to eavesdropping by the phone company that is

reasonably necessary to effectively maintain the phone service or prevent its fraudulent use. *See, e.g., Bubis v. United States*, 384 F.2d 643, 648 (9th Cir. 1967), *citing Brandon v. United States*, 382 F.2d 607 (10th Cir. 1967). This common law "provider exception" to statutory wiretapping claims existed when *Katz* was decided, and has since been codified in the Wiretap Act and subsequent amendments:

> It shall not be unlawful under this chapter for… a provider of wire or electronic communication service… to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to *the rendition of his service* or to the *protection of the rights or property of the provider* of that service….

18 U.S.C. § 2511(2)(a)(i) (emphasis added); *see also id.* at § 2702(b)(5) (similar exception in the SCA). Notably, NuVox's terms of service concerning the company's access to its customers' email closely track this existing provider exception: "NuVox commits to follow the controlling Federal and State laws respecting Subscriber privacy and data access…. NuVox may access and use individual Subscriber information *in the operation of the Service and as necessary to protect the Service*." NuVox, *Acceptable Use Policy*, *available at* http://www.nuvox.com/Legal/acceptableUse.htm (last visited June 9, 2009) (emphasis added). This is exactly the type of limited access by the provider that was and is irrelevant under *Katz*'s reasoning, as *Warshak I* recognized. *Warshak I*, 490 F.3d at 474 ("the terms of service in question here…clearly provide for access only in limited circumstances, rather than wholesale

inspection, auditing, or monitoring of emails.").

C. The Government Violated the Fourth Amendment by Failing to Obtain a Probable Cause Warrant Before Seizing Mr. Warshak's Email.

Warshak I persuasively rejected the government's argument that its acquisition of stored email is merely a "compelled disclosure" requiring only reasonableness rather than a probable cause warrant. *See id.*, 490 F.3d at 468-69; *see also* Bellia & Freiwald, *supra* at 141-47 (addressing same). This issue is even easier to dispose of here than in *Warshak I*. That decision dealt generally with email already stored with a provider, but NuVox did not store emails except as incident to transmission and would not have been able to disclose Warshak's emails but for the government's misuse of the SCA. This "back door wiretap" of Warshak's emails is not at all analogous to the compelled disclosures in cases such as *Miller*, where the evidence at issue was the company's own records, and is directly analogous to the prospective electronic eavesdropping in *Berger*, 388 U.S. at 59 (equating two-month eavesdropping order to "a series of intrusions, searches, and seizures").

Under the Wiretap Act, and consistent with *Berger*, such a series of intrusions into one's communications requires an order based on a judicial finding of probable cause, 18 U.S.C. § 2518(3)(a), and must comply with a broad range of strict procedural requirements.[13] Based on these strictures,

[13] Consistent with *Berger*, the Wiretap Act requires the following in addition to a showing of probable cause:

"[The Wiretap Act] does not suffer from the infirmities that the Court found fatal to the statute in *Berger* and to the surveillance in *Katz*." *United States v. Tortorello*, 480 F.2d 764, 775 (2d Cir. 1973), *cert. denied*, 414 U.S. 866 (1973). Instead of proceeding under these constitutionally tested procedures as it should have, the government violated not only the Wiretap Act but *Berger* itself.

CONCLUSION

For the foregoing reasons, *Amici* urge this Court to find that the District Court erred in failing to suppress Warshak's emails and all the evidence derived therefrom.

- Intercept orders must describe with particularity the communications to be intercepted;
- To address concerns about particularity, the government must minimize the collection of irrelevant information;
- There must be clear limits on the time period covered by the surveillance, and the search must end when the government obtains the evidence it seeks,
- the crime being investigated must be an enumerated serious crime;
- less intrusive means must not be available; and
- the police must return to the court with the fruits of their surveillance, and the required notice to the surveillance target is made by the court rather than left to the police.

18 U.S.C. § 2518.

DATED: June 9, 2009

By /s/Kevin S. Bankston

Kevin S. Bankston
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x 126
Facsimile: (415) 436-9993

Attorney for *Amici Curiae*

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 6,848 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6).

DATED: June 9, 2009

By /s/Kevin S. Bankston

Kevin S. Bankston
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x 126
Facsimile: (415) 436-9993

Attorney for *Amici Curiae*

CERTIFICATE OF SERVICE

I, Kevin S. Bankston, hereby certify that on this 10th day of June, 2009, I electronically filed the foregoing Brief with the Clerk of the Court using the CM/ECF system to effect service upon counsel of record.

_/s/Kevin S. Bankston__
Kevin S. Bankston