

## Articles

# The Fourth Amendment Status of Stored E-mail: The Law Professors' Brief in *Warshak v. United States*

By SUSAN FREIWALD & PATRICIA L. BELLIA\*

### Introduction

THIS VOLUME'S SYMPOSIUM EXPLORES the crucial conflict American companies that store electronic communications face when they mediate their customers' right to privacy and their government's demands for information. On the one hand, customers should not be subject to fishing expeditions through their stored electronic communications. On the other hand, government agents would like to access those communications to pursue potential criminals and terrorists. Electronic surveillance law requires government agents to justify, to some degree, their need for the information they seek before a service provider may be compelled to provide it to them. But what does "to some degree" actually mean? What procedural hurdles must government agents overcome, and what oversight will judges apply? *Warshak v. United States*<sup>1</sup> raises these very questions because it asks the Sixth Circuit to determine what showing a court should require of the Government, under the Stored Communications Act ("SCA"),<sup>2</sup> before the

---

\* Copyright © 2007, Susan Freiwald, Professor, University of San Francisco School of Law and Patricia L. Bellia, Visiting Professor of Law, University of Virginia School of Law; John Cardinal O'Hara, C.S.C. Associate Professor of Law, Notre Dame Law School. We would like to thank the law professors who signed the amicus brief published in this article for their input and support, and our research assistants: John Cannavino (U.S.F.), Alex Miller (U.S.F.), and Jeffery Houin (Notre Dame), as well as Matthew Chivvis, our editor, for their hard work and insights.

1. Oral argument was held on April 18, 2007.

2. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1860 (codified as amended at 18 U.S.C.A. §§ 2701-09, 2711-12 (West 2000 & Supp. 2007)).

court orders a service provider to turn over its customer's stored electronic communications. The case also asks whether those statutory requirements satisfy the Fourth Amendment.

The *Warshak* case poses the first constitutional challenge to the SCA, which Congress passed in 1986 as part of the Electronic Communications Privacy Act ("ECPA").<sup>3</sup> Steven Warshak, the plaintiff, seeks to enjoin the Government from using a court order obtained under 18 U.S.C. § 2703(d) ("D order") to demand his stored e-mail messages from his service providers.<sup>4</sup> Warshak maintains that agents violate the Fourth Amendment when they use a D order to get stored e-mail, because judges grant such orders without first finding probable cause.<sup>5</sup> The Government admits to having used D orders to obtain Warshak's e-mail and defends that practice on the ground that users lack a reasonable expectation of privacy in their stored e-mails.<sup>6</sup>

We submitted an amicus brief to the Sixth Circuit on behalf of fifteen professors of electronic privacy and internet law.<sup>7</sup> The Sixth Circuit's decision in *Warshak* could significantly clarify the murky law of electronic surveillance and could affirm that our electronic communications receive meaningful protection under the Fourth Amendment. As Kevin Bankston and Al Gidari describe in their contributions to this volume, when the Government demands electronic communications from service providers, it does so behind the scenes, without either notice to the targets or to the public.<sup>8</sup> Warshak is the rare plain-

3. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848.

4. Warshak's complaint also requested a declaratory judgment that the SCA is unconstitutional on its face and as applied. *See* Complaint for Declaratory Judgment and Injunctive Relief at 14, *Warshak v. United States*, No. 1:06-CV-357 (S.D. Ohio June 12, 2006). Unless otherwise noted, the pleadings and briefs from the *Warshak* case are on file with the authors.

5. Warshak also complained that the Government's practices violate the SCA as a matter of statutory law. *Id.* at 11-14.

6. The nature of the stored e-mails sought is complex and we take it up later in this introduction. *See infra* notes 13-14 and accompanying text.

7. The Electronic Frontier Foundation also filed an amicus brief on behalf of itself, the American Civil Liberties Union, the ACLU Foundation of Ohio, and the Center for Democracy and Technology. *See* Brief of *Amici Curiae* Electronic Frontier Foundation et al. Supporting Appellee and Urging Affirmance, *Warshak v. United States*, No. 06-4092 (6th Cir. Nov. 22, 2006), *available at* [http://www EFF.org/legal/cases/warshak\\_v\\_usa/warshak\\_amicus.pdf](http://www EFF.org/legal/cases/warshak_v_usa/warshak_amicus.pdf).

8. We will discuss notice to the target *infra* text accompanying notes 23-24. As for notice to the public, a court order issued under the SCA generally forbids the service provider who receives it from disclosing that to anyone. *See* 18 U.S.C. § 2705(b) (2000); *In re* Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(d), Misc. No. 1105MJ00135 (S.D. Ohio May 6, 2005) (issuing an order to a service

R

R

tiff who learned of the Government's surveillance and decided to sue.<sup>9</sup> His case asks the Sixth Circuit to provide the first decision on the legality of government practices that have largely been immune from suit.<sup>10</sup> It also invites the court to establish what judicial oversight the Fourth Amendment requires for government surveillance of stored e-mail.<sup>11</sup> That question, up until now, has had no clear answer. If the Constitution in fact leaves us vulnerable to government fishing through the vast array of personal information available in our stored e-mails, then our use of modern communications technologies will require that we sacrifice essential privacy interests.

As part of a criminal investigation into Steven Warshak's operation of his company,<sup>12</sup> government agents applied for D orders in May and September of 2005. As requested, a magistrate judge in the Southern District of Ohio ordered two of Warshak's internet service providers ("ISPs") to turn over all of Warshak's stored e-mails and account

---

provider to reveal Warshak's communications including any e-mail communications that had been accessed, viewed, or downloaded and precluding the service provider from disclosing to anyone, including Warshak, the existence of the order or the investigation).

9. It seems that Warshak sought a temporary restraining order to stop the Government from using D orders to obtain his stored e-mail during the pendency of its investigation against him. See Transcript of Proceedings (Telephone Conference) at 10–11, *Warshak v. United States*, No. 1:06-CV-357 (S.D. Ohio July 5, 2006) ("[W]e're asking for a restraining order against unconstitutional further conduct."); Plaintiff-Appellee Steven Warshak's Opposition to United States' Motion to Stay Preliminary Injunction at 4–5, *Warshak v. United States*, No. 06-4092 (6th Cir. filed Nov. 2, 2006) [hereinafter *Warshak Stay Opposition*]; see also Susan N. Herman, *The USA PATRIOT Act and the Submajoritarian Fourth Amendment*, 41 HARV. C.R.-C.L. L. REV. 67, 71, 103–04, 120–21 (2006) (discussing reasons targets of stored e-mail surveillance do not sue).

10. In most cases, targets learn of searches, if at all, after those searches are complete, at which point they may lack a strong incentive to sue. See, e.g., Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1269 (2004); Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 64 (2004) [hereinafter Freiwald, *Online Surveillance*]. For example, were Warshak to succeed on a claim that the Government's practices violated the SCA, he would be entitled to minimal financial damages and he would not be afforded the benefit of a statutory exclusionary rule. See, e.g., Susan Freiwald, *First Principles of Communications Privacy*, STAN. TECH. L. REV. (forthcoming 2007 Symposium) (manuscript at 3, on file with the authors) [hereinafter Freiwald, *First Principles*]; Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1436 (2004); see also Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Law*, 54 HASTINGS L.J. 805, 807 (2003) (arguing that absence of a statutory suppression remedy has reduced judicial oversight of Governments' surveillance practices in the criminal context).

11. See Brief of Plaintiff-Appellee Steven Warshak, *Warshak v. United States* at 27, 30–32, No. 06-4092 (6th Cir. Nov. 13, 2006) [hereinafter *Warshak Brief*].

12. Warshak was subsequently indicted by a federal criminal jury on criminal counts of bank and wire fraud, money laundering, and other federal crimes. See Brief for Defendant-Appellant the United States of America at 8, *Warshak v. United States*, No. 06-4092 (6th Cir. Oct. 11, 2006) [hereinafter *Government Brief*].

information, except those e-mails that had been neither accessed, viewed, nor downloaded (“unaccessed e-mails”).<sup>13</sup> Both orders excluded unaccessed e-mails, because the Government lacked the probable cause warrant that it interpreted the SCA to require for unaccessed e-mails.<sup>14</sup> A strict word limit on our brief precluded us from critiquing the Government’s position that the SCA’s warrant requirement extends only to unaccessed e-mails, but numerous commentators, including amici, have criticized it in their scholarship.<sup>15</sup> As a practical matter, it seems unlikely that an e-mail account stored with an ISP will contain many unaccessed e-mails, as users tend to download or otherwise access their e-mails soon after receiving them.

In fact, the court orders encompassed an extensive amount of information.<sup>16</sup> They granted access to “all customer account information for any accounts registered or services rendered to” Warshak, including the “contents of wire or electronic communications . . . that were placed or entered in directories or files owned or controlled by [Warshak’s accounts] at any time during the hosting of the electronic communications” (but excluding unaccessed e-mails).<sup>17</sup> In addition, at least one of the orders required the ISP “to turn over all log files and backup tapes; customer account identifiers; application information; contact information; email addresses; billing information to include bank account numbers; and any other information pertaining

---

13. The Government also requested unopened e-mails stored more than 180 days, based on its construction of the SCA. *See also* *Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001), *aff’d in part on other grounds*, 352 F.3d 107, 114 (3d Cir. 2004) (accepting Government’s statutory construction). Yahoo!, one of the ISPs, did not release any e-mails stored fewer than 180 days, apparently in response to a Ninth Circuit precedent. *See* Warshak Brief, *supra* note 11, at 2 n.2 (citing *Theofel v. Farey-Jones*, 359 F.3d 1066, 1077 (9th Cir. 2004) (rejecting Government’s statutory interpretation), *cert. denied*, 125 S. Ct. 48 (2004)); Warshak Stay Opposition, *supra* note 9, at 5 n.3 (citing *Theofel*, 359 F.3d 1066).

14. The Government also considers sent and draft e-mail to be available without a probable cause warrant. *See* United States of America’s Memorandum in Opposition to Plaintiff’s Motion for Temporary Restraining Order and/or Preliminary Injunction at 2, Warshak v. United States, No. 1:06-CV-357 (S.D. Ohio filed July 5, 2006) (“Unopened e-mail stored on a service provider’s servers fall within the scope of ‘electronic storage,’ but opened e-mail, draft e-mail, and copies of sent e-mail do not.”).

15. *See* Freiwald, *Online Surveillance*, *supra* note 10, at 56–57.

16. The judge who reviewed them interpreted one of the orders as requesting information “‘about accounts registered or services rendered to’ Warshak or ‘associated parties.’” Warshak v. United States, No. 1:06-CV-357, 2006 U.S. Dist. LEXIS 50076, at \*3 (S.D. Ohio July 21, 2006). Warshak’s mother intervened as a plaintiff because she claimed that the ISPs had disclosed her e-mail accounts as well. *Id.* at \*32 n.19; *United States v. Contents of Nationwide Life Insurance Account in the Name of Warshak*, No. C-1-05-196, 2006 WL 971978 (S.D. Ohio Apr. 12, 2006).

17. *Warshak*, 2006 U.S. Dist. LEXIS 50076, at \*3–\*4.

to the customer, including setup, synchronization, etc.”<sup>18</sup> According to Warshak, the Government seized thousands of e-mails, of a “deeply personal nature, of no conceivable relevance to the government’s investigation.”<sup>19</sup>

The magistrate judge who granted the orders found that the Government satisfied the legal requirements for a D order because the Government had “offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation.”<sup>20</sup> By contrast, to obtain a warrant, government agents must show probable cause to believe that their search of the records will yield evidence of a crime.<sup>21</sup>

A few weeks after the Government notified Warshak of the ISP court orders in May of 2006, Warshak sued to enjoin the Government from acquiring his e-mails without first obtaining a probable cause warrant. Warshak argued that the Fourth Amendment generally requires warrants for access to letters and sealed packages, which Warshak claimed were analogous to his stored e-mails. The Government pressed the court to analogize stored e-mails to post-cards, searches of which do not implicate the Fourth Amendment. Judge Dlott, who heard the case, preferred the letter analogy for stored e-mails and decided that Warshak had shown a substantial likelihood of success on his Fourth Amendment claim.<sup>22</sup> At least for purposes of the preliminary injunction, the court rejected the Government’s claim that Warshak surrendered his reasonable expectation of privacy in his e-mails by storing them in subscriber accounts with his ISPs.

---

18. *Id.* at \*3 (internal quotation marks omitted); *see also In re Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(d)*, Misc. No. 1105MJ00135 (S.D. Ohio May 6, 2005).

19. Warshak Stay Opposition, *supra* note 9, at 2, 4 n.1. Warshak expresses concern not only about Government access to his own communications, but about the disclosure of the private communications of those with whom he communicated. *See Memorandum in Support of Issuance of a Temporary Restraining Order and/or Preliminary Injunction at 18, Warshak v. United States*, No. 1:06-CV-357 (S.D. Ohio filed June 30, 2006).

20. *See In re Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(d)*, Misc. No. 1105MJ00135 (S.D. Ohio May 6, 2005); 18 U.S.C. § 2703(d) (2000).

21. *See* FED. R. CIV. P. 41(c)(1).

22. Judge Dlott declined to address the statutory argument as well. *See Warshak*, 2006 U.S. Dist. LEXIS 50076, at \*20 (“Because Warshak has demonstrated a sufficient likelihood of success on his Fourth Amendment claim to support an injunction . . . , the Court need not reach, for purposes of the present Motion, the merits of Warshak’s secondary claim that the 2703(d) orders obtained and/or threatened by the United States in this matter violate the SCA.”). Similarly, our amicus brief concentrated on the constitutional question.

Judge Dlott's opinion expressed significant concern about the Government's practice of obtaining D orders and then delaying notification to the targets of those orders. The SCA requires that targets be notified before law enforcement agents use a D order to obtain the contents of communications, but permits agents to request that such notice be delayed for ninety-day increments, when prior notice would seriously jeopardize the investigation.<sup>23</sup> The D orders that the Government used in the *Warshak* case permitted notice to be delayed for ninety days, yet Warshak was not informed of the searches for more than a year. Judge Dlott found that the Government had not obtained any extension of the original ninety-day period.<sup>24</sup>

Judge Dlott's order reflected her "grave constitutional concerns" about the Government's practices.<sup>25</sup> She decided, provisionally, that the "combination of a standard of proof less than probable cause and potentially broad *ex parte* authorization cannot stand."<sup>26</sup> While unprepared to declare as facially invalid any SCA provisions that authorize use of D orders to obtain stored e-mail, Judge Dlott preliminarily enjoined the United States from using D orders to seize "the contents of any personal email account maintained by an internet service provider in the name of any resident of the Southern District of Ohio, including but not limited to Steve Warshak, without providing the relevant account holder or subscriber prior notice and an opportunity to be heard."<sup>27</sup>

The Government devotes a substantial amount of its brief to arguing that the court lacked subject matter jurisdiction over the case because Warshak had not established a sufficient risk that the Government would continue to pursue his e-mails.<sup>28</sup> Warshak counters that the Government's failure to commit to not using future D orders to obtain his stored e-mail, combined with the fact that they did so in the past without notifying him for long periods, permitted

---

23. See 18 U.S.C. § 2705 (2000) (describing the following adverse results: "(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").

24. See *Warshak*, 2006 U.S. Dist. LEXIS 50076, at \*30 n.18.

25. *Id.* at 26–28.

26. *Id.* at 31.

27. *Id.* at 32.

28. See Government Brief, *supra* note 12, at 18–29. The Government contends that Warshak lacks standing and that his claims are not ripe for review. *Id.*

him to petition for protection of his constitutional rights.<sup>29</sup> If the Sixth Circuit fails to reach the merits of Warshak's case, that will preserve the status quo, under which it is uncertain how, if at all, the Fourth Amendment protects stored e-mails. We do know, however, that the Government views stored e-mails as subject to search on minimal process and that agents will surely continue their current practices until another lawsuit arises or Congress intervenes.

In defending the constitutionality of its practices, the Government claims that the Fourth Amendment warrant requirement does not apply because Warshak had no reasonable expectation of privacy in his stored e-mails. According to the Government, because Warshak agreed, either implicitly or explicitly, to permit his service providers to monitor his accounts, he cannot claim a reasonable expectation of privacy in those accounts. We argue in our brief that, although service providers may monitor their users' accounts to maintain their service, such monitoring does not constitute a waiver of their users' constitutional claims vis-à-vis the Government. Moreover, we contend that service providers are state actors when they give over the contents of their users' e-mail accounts in response to mandatory process, notwithstanding whatever private right they had to monitor.<sup>30</sup> We find significant support for our position in a recent case issued by the United States Court of Appeals for the Armed Forces.<sup>31</sup> But so far no Article III court has weighed in on the question.

The Government also defends a right to compel a third party to disclose information it holds subject only to a constitutional reasonableness requirement, notwithstanding the user's reasonable expectation of privacy. It posits a "simple rule," under which "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities."<sup>32</sup> The Government bases its "third party rule" on a broad reading of decades old Supreme Court precedents.<sup>33</sup> In our brief, we argue that the Government misreads those precedents, which should not be con-

---

29. See Warshak Brief, *supra* note 11, at 11–26. Warshak's papers indicate that he was not notified of the prior orders until he requested notification himself, having apparently learned of the orders another way. *Id.* at 1.

30. Warshak makes a similar argument in his appellate brief. *See id.* at 41–43.

31. See *United States v. Long*, 64 M.J. 57 (C.A.A.F. 2006).

32. See Reply Brief for Defendant-Appellant United States of America at 17, *Warshak v. United States*, No. 06-4092 (6th Cir. Jan. 11, 2007) (quoting *Smith v. Maryland*, 442 U.S. 735, 744 (1979)).

33. See *id.* (drawing the rule from both *Smith* and *United States v. Miller*, 425 U.S. 435, 443 (1976)).

strued to permit compelled disclosure upon mere reasonableness in those cases in which the target retains a reasonable expectation of privacy. The Government's purported third party rule has come under substantial criticism from law professors, including several amici.<sup>34</sup> But the Government finds limited support for its claim in some judicial opinions that have curtailed privacy protection of electronic information (though not the content of stored e-mails) on similar reasoning.<sup>35</sup> The Sixth Circuit, in *Warshak*, has the opportunity to delineate the scope of the third party rule, and, we hope, to limit its application. If the Government's broad third party rule stands, it precludes any meaningful constitutional protection for internet-based information, which almost always resides with third parties.<sup>36</sup>

In defending the merits of Judge Dlott's order, Warshak attacks the Government's claims that mere reasonableness suffices as a constitutional matter in this context. He also demonstrates at length how administrative subpoenas, which the Government claims to be analogous to D orders, offer protections to the target that D orders do not and why, therefore, D orders should be analyzed differently.<sup>37</sup> Warshak presses the Sixth Circuit to recognize that the constitutional question must precede the statutory one. If the Fourth Amendment does not tolerate the warrantless procedures by which the Government currently obtains stored e-mails, as Warshak claims, then that trumps whatever Congress may have intended when it drafted the SCA. If the Sixth Circuit agrees that the Fourth Amendment requires the Government to obtain a probable cause warrant prior to compelling production of stored e-mails, then the court will endeavor to interpret the SCA consistently with that requirement. Any SCA provisions that may not be read to conform to the Fourth Amendment will have to be overturned.

---

34. See, e.g., Bellia, *supra* note 10, at 1397–1412; Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1576–82 (2004); Peter P. Swire, *Katz is Dead. Long Live Katz*, 102 MICH. L. REV. 904, 923–33 (2004).

35. See, e.g., *Guest v. Leis*, 255 F.3d 325, 335–36 (6th Cir. 2001); *United States v. Hambrick*, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999), *aff'd*, 225 F.3d 656 (4th Cir. 2000), *cert. denied*, 531 U.S. 1099 (2001); *United States v. Kennedy*, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000).

36. See, e.g., Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357, 367–68 (2003) (discussing role of third-party service providers in transmitting and storing e-mail and observing that, under one perspective of how the Fourth Amendment applies to the Internet, law enforcement officials can compel service providers to disclose e-mails with a mere subpoena).

37. Our amicus brief addresses the Government's claimed "compelled disclosure" rule at some length as well.

Because our amicus brief could not exceed 8000 words, we had to severely limit the topics that that we covered and the treatment of those that we did cover. Besides refraining from a critique of the Government’s statutory construction, we also significantly condensed our refutation of the Government’s third party rule.<sup>38</sup> In addition, we cut short an argument for imposing the higher procedural hurdles of the Wiretap Act to government surveillance of stored e-mails.<sup>39</sup> If those procedural hurdles had applied, as they do to real-time interceptions, then government investigators would have needed to establish a tighter nexus between the surveillance sought and Warshak’s criminal liability. They would also have needed to establish that their search was necessary as a last resort and would proceed only for a limited time. In addition, government investigators would have had to submit to greater judicial oversight, for example to ensure that they minimized the acquisition of non-incriminating information. Importantly, they would have needed to notify each target as soon as they completed their search.<sup>40</sup>

As Al Gidari describes in his article in this volume, service providers currently respond to a huge number of inquiries for stored communications data.<sup>41</sup> The procedures imposed on government agents before they may obtain such data determine whether a member of the judiciary provides meaningful oversight to ensure respect for Fourth Amendment values. The more government monitors avoid judicial scrutiny of their practices, the more citizens must depend on the Department of Justice to conform its behavior to those legal standards that it sets for itself. As Kevin Bankston discusses, government investigators do not seem to be choosing the right standards, and of course, there is no way, without judicial oversight, to ensure that they even abide by those standards.<sup>42</sup> The Sixth Circuit may alter this concentra-

38. For further critique of the Government’s third-party rule, see sources cited *supra* note 34.

39. For more information on the subject, see Freiwald, *First Principles*, *supra* note 10.

40. See 18 U.S.C. § 2518 (2000); Freiwald, *Online Surveillance*, *supra* note 10, at 25.

41. See A. Gidari, *Companies Caught in the Middle*, 41 U.S.F. L. REV. 535, 553 (manu. 17–18) (2007); cf. OFFICE OF THE INSPECTOR GENERAL: A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION’S USE OF NATIONAL SECURITY LETTERS xviii (2007) (finding that, from 2003 through 2005, the FBI issued at least 143,000 requests for records of telephone use, electronic mail, financial information, and credit data under statutes permitting access to such records in national security investigations) [hereinafter OIG REPORT]. See generally Herman, *supra* note 9 (discussing the provisions that regulate National Security Letters).

42. See Kevin S. Bankston, *Only the DOJ Knows: The Secret Law of Electronic Surveillance*, 41 U.S.F. L. REV. 587 (2007); see also OIG REPORT, *supra* note 41, at xxviii–xli, 66–107 (documenting pervasive failures by FBI agents to satisfy statutory requirements and several different means by which agents acquired information from service providers improperly).

R  
R  
R  
  
  
  
R  
  
R

tion of surveillance power in the executive branch by proclaiming that the Fourth Amendment provides significant protection for stored e-mail. Our amicus brief urges it to do so.

### **Interest of Amici**<sup>43</sup>

Amici are scholars who teach, write about, or have an interest in electronic privacy law and internet law. Amici have no stake in the outcome of this case, but are interested in ensuring that electronic privacy law develops with due regard for the vital role electronic communications play in our lives. A full list of amici is appended to the signature page. Both defendant-appellant and plaintiff-appellee have consented to the filing of this brief.

### **Summary of Argument**

Electronic mail (“e-mail”) has become an essential medium of communication and assumed a vital role in our lives. The contents of our e-mail accounts reveal extensive and detailed information about our interests, our views, and our actions. Yet, the Government in this case claims the right to obtain the entirety of our personal e-mail accounts from our service providers, without first establishing probable cause or providing us notice, so long as we have previously accessed our e-mails in some way. Acceptance of this radical claim would dramatically limit judicial oversight of an immensely powerful surveillance tool and eviscerate the privacy of electronic communications.

Though the Government presents the question as well settled, no federal courts have addressed government acquisition of e-mail from a service provider without prior notice (“stored e-mail surveillance”), although two military courts have found that it requires a probable cause warrant.<sup>44</sup> More fundamentally, when the Government argues that a constitutional “reasonableness” standard applies to stored e-mail surveillance because the applicable statute apparently approves of subpoena-like authority, it begs the essential question: does stored e-mail surveillance by the Government on less than probable cause satisfy the Fourth Amendment? Amici, law professors who write and teach in the areas of electronic privacy law and internet law, believe that it does not.

---

43. From this point forward, the text of this Article has been adapted from the authors’ amicus brief, with only minor revisions.

44. Amici do not address what procedural requirements apply when the Government does give the target prior notice.

Because it invades a reasonable expectation of privacy, stored e-mail surveillance constitutes a search under the Fourth Amendment, and may not be conducted without first obtaining a warrant based on probable cause. “Compelling” a service provider to produce a person’s e-mail does not entitle government agents to evade that constitutional requirement.

## Argument

### I. Stored E-mail Surveillance Is a Search Under the Fourth Amendment that Requires, at a Minimum, a Warrant Based on Probable Cause

Courts, and not Congress, must determine the threshold issue: how does the Constitution regulate stored e-mail surveillance? Because government agents intrude upon users’ reasonable expectation of privacy when they acquire private e-mails, they conduct a search under the Fourth Amendment.<sup>45</sup> That expectation of privacy obtains whether the e-mails acquired are stored or in transit, and whether or not their recipients have accessed them. Nothing in the private contracts between users and their internet service providers affects the application of those constitutional protections.

#### A. Users Maintain a Reasonable Expectation of Privacy in Their E-mails, Whether or Not Those E-mails Have Been Stored or Accessed

Users maintain a reasonable expectation of privacy in their e-mail, whether that e-mail is in transit or has come to rest.<sup>46</sup> The reasonable expectation of privacy test, which is used to determine whether a particular investigatory technique constitutes a search under the Fourth Amendment, asks whether a target of an investigation entertains an actual expectation of privacy in the object of the search (subjective prong), and whether that expectation of privacy is one that society deems reasonable (objective prong).<sup>47</sup>

---

45. The First Amendment also supports imposing significant burdens on law enforcement access to e-mails, because they are communications. *See, e.g., Stanley v. Georgia*, 394 U.S. 557, 564 (1969) (“It is now well established that the Constitution protects the right to receive information and ideas.”); *see also* Daniel Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. (forthcoming 2007).

46. *United States v. Long*, 64 M.J. 57, 65 (C.A.A.F. 2006); *United States v. Maxwell*, 45 M.J. 406, 418 (C.A.A.F. 1996).

47. *See Kyllo v. United States*, 533 U.S. 27, 32–33 (2001); *Katz v. United States*, 389 U.S. 347, 361 (1967).

## 1. Warshak Had a Subjective Expectation of Privacy in the E-mails Stored with His Service Providers

Warshak's use of his e-mail demonstrates his subjective expectation of privacy in it.<sup>48</sup> The subjective prong precludes affording constitutional protection to those who themselves did not view the object of the investigation as private. To require that government agents refrain from viewing information easily seen by others is unfair and unnecessary. It is unfair because the Government should not be disadvantaged vis-à-vis the average member of the public. It is unnecessary because we assume that before people make information available to all they have either determined the repercussions to be harmless, or assumed the risk of those repercussions. The Constitution does not protect information that one has "knowingly expose[d] to the public."<sup>49</sup>

In this case, there is no evidence that Warshak knowingly exposed the entirety of his e-mail accounts to the public. Instead, Warshak used the e-mail accounts the Government seized to send e-mails "of a deeply personal nature."<sup>50</sup> As we discuss in Part I.B below, that Warshak maintained e-mail accounts with service providers did not vitiate his subjective expectation of privacy.

## 2. Warshak's Expectation of Privacy in His E-mails Was Objectively Reasonable

E-mail has become so indispensable that it must be reasonable for us to expect that it is private. One who looks at our e-mails obtains a detailed view into our innermost thoughts; no previous mode of surveillance exposes more. When we compose private and professional e-mails, embed links to internet sites in some, and attach documents, pictures, sound files, and videos to others, we rely on the privacy of the medium. Society does not make us rely at our peril but rather accepts as reasonable our expectations of privacy in e-mail.

The public reasonably expects e-mail to be private, despite the fact that e-mail may be vulnerable to surveillance. The Supreme Court found the expectation of privacy in telephone calls to be reasonable in *Katz*, despite public awareness of the vulnerability of those calls to interception. In the years preceding *Katz*, the public had learned of rampant illegal wiretapping from numerous influential books, schol-

---

48. See Warshak Stay Opposition, *supra* note 9, at 11 n.6.

49. *Katz*, 389 U.S. at 351.

50. See Warshak Stay Opposition, *supra* note 9, at 4 n.1.

arly articles, and newspaper accounts.<sup>51</sup> In the same period, Congress considered new legislation and convened numerous hearings and commissioned lengthy expert reports that detailed communications' vulnerability.<sup>52</sup> The *Katz* Court nonetheless found warrantless wiretapping to be unconstitutional, despite the lack of absolute privacy in telephone calls.<sup>53</sup> Similarly, a government pronouncement that e-mails are vulnerable may not defeat our reasonable expectations of privacy in it.<sup>54</sup> Otherwise, the Constitution would be powerless to prevent executive branch overreaching.

In *Katz*, the Supreme Court based constitutional protection of telephone calls on the overriding importance of the telephone system.<sup>55</sup> In other words, whatever people actually thought or knew about the privacy of their telephone calls, they were *entitled to believe* in the privacy of telephone calls, because any other result would be destructive of society's ability to communicate.<sup>56</sup>

Because e-mails typically contain much richer data than telephone calls, e-mail surveillance intrudes much more on personal privacy than does an analogous wiretap. Although many modern e-mails incorporate other media, even a simple text e-mail can reveal a lengthy back-and-forth exchange between the parties to the correspondence. People reveal in their e-mails much more about their political opinions, religious beliefs, personal relationships, intellectual interests, and artistic endeavors than they ever revealed over the telephone. Stored e-mails, in particular, contain a vast archive of people's past activities.

Society now relies on e-mail and its powerful features much more than it relied on the telephone system at the time of *Katz*. Because of e-mail's vital role in modern communications, users have a reasonable expectation of privacy in it, and agents must secure at least a probable-cause warrant under the Fourth Amendment before they obtain it.<sup>57</sup>

---

51. See Freiwald, *Online Surveillance*, *supra* note 10, at 38–39.

52. *Id.* at 74–75.

53. See *id.* at 38 & n.203.

54. See *Smith v. Maryland*, 442 U.S. 735, 740 n.5 (1979) (recognizing that the expectation of privacy analysis must be replaced by a normative analysis when “subjective expectations had been ‘conditioned’ by influences alien to well-recognized Fourth Amendment freedoms”).

55. *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.”).

56. *Id.* (holding that one who places a telephone “call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world”).

57. Several Courts of Appeals imposed the heightened procedural requirements for wiretapping on silent video surveillance because it was just as intrusive, continuous, hid-

**3. Warshak Had a Reasonable Expectation of Privacy in His E-mails After His Service Provider Stored Them and He Accessed Them**

Stored e-mail should not receive less constitutional protection than e-mail in transit.<sup>58</sup> More extensive e-mail correspondence may be found on a third party’s server than may be intercepted. When a government agent intercepts e-mails in transit, she acquires only the e-mail traveling at that moment. The agent must continue the surveillance for so long as she hopes to track the target’s correspondence. To obtain e-mails covering a vast length of time, it would be far simpler and easier to conduct stored e-mail surveillance afterwards in a single shot. For example, rather than running an e-mail wiretap for three months from January 1 to March 31, an agent may obtain the same electronic communications from the service provider by demanding, on March 31, prior e-mails going back three months. That the Government apparently obtained thousands of e-mails, both sent and received, from Warshak’s service providers, from accounts over nine years old, starkly illustrates the power and scope of stored e-mail surveillance.<sup>59</sup>

By the same token, a user should enjoy full Fourth Amendment protection for e-mail messages that she has accessed.<sup>60</sup> Nothing in the reading of an e-mail (let alone its being opened) makes the correspondence less private or its acquisition less intrusive. Users leave copies of their already-read e-mails in their accounts for many reasons, and almost never out of a lack of concern for the privacy of those e-mails. In fact, most users delete their least important, least sensitive e-mails, and retain the others for later use. Users store private e-mails in their accounts because they do not know how to do otherwise, or because they are not aware that their service providers maintain cop-

den, and indiscriminate. *See, e.g.*, United States v. Koyomejian, 970 F.2d 536, 542 (9th Cir. 1992) (en banc), *cert. denied*, 506 U.S. 1005 (1992) (imposing the following constitutional requirements in addition to probable cause: particular description, last resort, limited time, and minimization). Because e-mail surveillance threatens privacy and risks abuse as much as wiretapping, it too should be subject to the heightened requirements. *See* Freiwald, *Online Surveillance*, *supra* note 10, at 14.

58. *See* United States v. Long, 64 M.J. 57 (C.A.A.F. 2006); United States v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996); *supra* note 46 and accompanying text.

59. *See* Warshak Stay Opposition, *supra* note 9, at 2, 11.

60. Amici use the term “accessed” to cover accessed, opened, viewed, and downloaded e-mail. The Government claims the right to acquire accessed e-mails, draft e-mails, and sent e-mails without a probable cause warrant.

R

R

R

ies.<sup>61</sup> Many users simply neglect to delete e-mails until they run out of storage space; that retention does not indicate that users have knowingly exposed those e-mails to public or law enforcement view. The Government's strained statutory argument should not confuse the fact that a user's access to his e-mail does not affect its constitutional protection.

Before obtaining disclosure of the contents of an e-mail account stored on a service provider's computer, the Fourth Amendment requires that government agents obtain, at a minimum, a probable cause warrant, or that they invoke a proper exception to the warrant requirement. "The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech."<sup>62</sup> That stored e-mail surveillance takes place entirely outside of the reach and knowledge of the target makes it particularly prone to abuse. The warrant requirement protects e-mails whether in transit or stored, and whether accessed or not.<sup>63</sup>

**B. E-mail Users Do Not Forfeit an Expectation of Privacy in Their Communications Merely by Storing Those Communications with a Service Provider, Even Where the Service Provider Retains a Right of Access**

The Government's argument that an e-mail user forfeits any expectation of privacy and exposes her e-mail to indiscriminate government surveillance when she relies on a service provider to transmit and store that e-mail ignores a range of cases in which courts have recognized an expectation of privacy in items held by a third party. Moreover, it misunderstands the significance to this dispute of the Stored Communications Act<sup>64</sup> and of service providers' policies and practices regarding access to the communications they store.

---

61. Service providers may retain e-mails as a matter of practice or government compulsion. *See* 18 U.S.C. § 2704 (2000) (compelling backup preservation of electronic communications).

62. *United States v. United States Dist. Ct.*, 407 U.S. 297, 317 (1972).

63. As discussed, a probable cause warrant alone may be constitutionally insufficient. *See supra* note 57.

64. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1860 (codified as amended at 18 U.S.C.A. §§ 2701-09, 2711-12 (West 2000 & Supp. 2007)).

### 1. Allowing a Third Party to Carry or Store an Item Does Not Eliminate Any Expectation of Privacy in That Item<sup>65</sup>

Placing something in the care of a third party does not, without more, make the Government free to acquire it without a warrant. The Government's argument to the contrary appears to stem from a broad reading of the Supreme Court's "business records" cases.<sup>66</sup> The post-*Katz v. United States* foundation for this line of cases is *United States v. Miller*,<sup>67</sup> where the Supreme Court held that a bank customer had no reasonable expectation of privacy in financial records held by his banks, because "[a] depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."<sup>68</sup>

*Miller* and its progeny do not support the Government's position that communications placed in the hands of a third party are subject to compelled disclosure merely because a third party holds them. *Miller* relied on two lines of cases to arrive at the assumption-of-risk language quoted above. First, *Miller* relied on pre-*Katz* cases evaluating the compelled disclosure of business records under a reasonableness standard. The Court confirmed the post-*Katz* vitality of the reasonableness analysis by concluding that financial records that form part of a business relationship with the bank are not the kind of items in which one can expect privacy.<sup>69</sup> Second, *Miller* drew upon a series of cases involving communications revealed, recorded, or transmitted to the Government by an informant or undercover agent who is a party to the communication.<sup>70</sup> In those cases, the Court had reasoned that "no interest legitimately protected by the Fourth Amendment is involved," because the Fourth Amendment does not protect "a wrongdoer's mis-

65. Portions of this discussion are drawn from Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1397-1413 (2004).

66. See Government Brief, *supra* note 12, at 36-40, 43-45.

67. 425 U.S. 435 (1976). In a prior case, *Couch v. United States*, 409 U.S. 322 (1973), the Court addressed a Fourth Amendment challenge to an IRS summons compelling an accountant to surrender records used in preparing the defendant's tax return. The Court gave the Fourth Amendment claim only brief treatment because it "[did] not appear to be independent of [the taxpayer's] Fifth Amendment argument." *Id.* at 325-26 n.6. The Court's reasoning was similar to that which it later employed in *Miller*. See *id.* at 336 n.19.

68. *Miller*, 425 U.S. at 443; see also *Smith v. Maryland*, 442 U.S. 735 (1979) (holding that user has no expectation of privacy in telephone numbers revealed to the telephone company to connect calls).

69. See *Miller*, 425 U.S. at 440-42.

70. *Id.* at 443.

placed belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.”<sup>71</sup>

Neither of the two lines of cases on which *Miller* relies points toward the Government’s categorical rule that one loses one’s expectation of privacy by allowing a provider to transmit or store communications. Communications are not business records of the sort contemplated in *Miller* and its progeny. And to place a communication in the hands of a third party for carriage or storage is not to “confide” or “reveal” that communication in the same sense that one “confides” or “reveals” something to a government informant or agent by speaking to that person, or in the sense that a depositor “reveals” something to a bank so that the bank can process a transaction, or in the sense that one “reveals” a telephone number so that the telephone company can connect a call. Indeed, any categorical rule that a provider’s involvement eliminates a user’s reasonable expectation of privacy runs headlong into the Court’s holding in *Katz v. United States*. *Katz*, after all, involved communications carried over a telephone line by a communications carrier that undoubtedly had the technical ability to monitor the communications.<sup>72</sup> If the Government’s reasoning in this case were correct, *Miller* would have overruled *Katz sub silentio*, even while the *Miller* Court purported to affirm and apply *Katz*.

Moreover, in a range of contexts, courts have recognized that a third-party’s involvement in carrying or storing property does not leave government agents free to inspect that property. When the United States Postal Service carries mail or a sealed package, for example, government agents cannot open the items without obtaining a warrant. As the Supreme Court has recognized, “[l]etters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy; warrantless searches of such effects are presumptively unreasonable.”<sup>73</sup>

Similarly, when someone maintains personal property on a third party’s premises, she retains an expectation of privacy in it, so long as

---

71. *Hoffa v. United States*, 385 U.S. 293, 302 (1966); *see also* *United States v. White*, 401 U.S. 745, 749, 751 (1971) (plurality opinion); *Osborn v. United States*, 385 U.S. 323, 331 (1966); *Lopez v. United States*, 373 U.S. 427 (1963).

72. 389 U.S. 347, 353 (1967).

73. *United States v. Jacobsen*, 466 U.S. 109, 114 (1984); *see also* *Ex parte Jackson*, 96 U.S. 727, 733 (1877) (“Letters and sealed packages . . . are as fully guarded from examination and inspection . . . as if they were retained by the parties forwarding them in their own domiciles.”).

the property is secured against others' access and the third party's right of access to the premises is limited.<sup>74</sup>

This case is analogous to cases involving a third party's carriage or storage of physical property. Agents here sought to remove e-mail communications from a storage area set aside exclusively for the use of the subscriber and to which nobody but the provider had physical access. Yet the Government does not cite or discuss these cases. Instead, it seeks a categorical rule that third-party involvement extinguishes an expectation of privacy.

## 2. Service Provider Assistance to Government Agents Does Not Reduce the Government's Constitutional Obligations

The Government builds much of its case on the fact that its agents obtained Warshak's stored e-mail from his service providers. But the Government may not avoid its constitutional obligations by engaging an intermediary in its surveillance. The Government also argues that service providers' technical ability to access and scan communications for harmful content and attachments, or terms of service announcing that they may do so, can eliminate users' expectation of privacy in communications stored with such providers.<sup>75</sup> Crediting that claim would misconstrue the applicable statute, the nature of a service provider's right to protect its own property, and the nature of the contractual relationship between users and their service providers.

---

74. See, e.g., *Stoner v. California*, 376 U.S. 483, 489 (1964) (search of hotel room without warrant violated Fourth Amendment, even though one who engages a hotel room gives implied permission to hotel personnel to enter to perform their duties); *Chapman v. United States*, 365 U.S. 610, 616–18 (1961) (search of house occupied by tenant violated Fourth Amendment, even though landlord had authority to enter house for some purposes); *United States v. Johns*, 851 F.2d 1131, 1133–35 (9th Cir. 1988) (implicitly recognizing reasonable expectation of privacy in rented storage unit); cf. *United States v. Rahme*, 813 F.2d 31, 34 (2d Cir. 1987) (where hotel guest failed to pay rent and rental period expired, hotel could lawfully take possession of items in room and guest had no reasonable expectation of privacy); *United States v. Poulsen*, 41 F.3d 1330, 1336 (9th Cir. 1994) (renter of storage unit loses expectation of privacy when he fails to pay rent, and facility manager may seize property and turn it over to law enforcement).

75. Government Brief, *supra* note 12, at 49.

**a. The Involvement of a Service Provider in the Government's Stored E-mail Surveillance Does Not Impact the Government's Constitutional Obligations**

A service provider acts as the Government's agent when it accedes to surveillance requests.<sup>76</sup> When the Government initiates the search of the target's e-mail account, as it did in this case, the service provider's actions to facilitate the search do not convert the Government's surveillance from state action subject to Fourth Amendment requirements to a private search.<sup>77</sup> In addition, when electronic communications providers furnish stored e-mail to government investigators, that parallels the common practice of telecommunications companies providing telephone line access to government wiretappers. Wiretapping assistance is not only statutorily mandated,<sup>78</sup> it has never reduced the Government's constitutional obligations.<sup>79</sup> Service provider involvement in stored e-mail surveillance does not reduce the constitutional regulation of that practice either.

**b. Terms of Service Providing that the Government May Be Granted Access Do Not Affect the Constitutional Requirements for Stored E-mail Surveillance**

The Government argues that most service providers have policies stating that they will disclose communications in response to legal process, and that this fact eliminates any expectation of privacy in e-mail communications.<sup>80</sup> A service provider's policy of complying with legal process, however, cannot defeat a user's reasonable expectation of privacy. E-mail users must be entitled to presume that agents will present *appropriate* legal process, not that they will present *any* legal process. It would turn the law on its head if service providers could merely notify their users that they intend to comply with unconstitutional govern-

76. See *United States v. Long*, 64 M.J. 57, 65 (C.A.A.F. 2006) (describing seizure of stored e-mail by network administrator as "a part of a search for law enforcement purposes").

77. See *United States v. Maxwell*, 45 M.J. 406, 422 (C.A.A.F. 1996) (service provider's search of stored e-mail at the Government's request not a "private search"); see also *McClelland v. McGrath*, 31 F. Supp. 2d 616, 619 (N.D. Ill. 1998) (noting that when telephone company employees act "at the request or direction of police officers," they act as government agents and the Fourth Amendment applies).

78. See 18 U.S.C. § 2518(4) (2000) (requiring and regulating provider assistance).

79. Service provider assistance in government surveillance does impose statutory obligations on the service provider in addition to any constitutional ones. See 18 U.S.C. § 2707 (2000 & Supp. IV 2004) (permitting civil suits against service providers for improper disclosure).

80. See Government Brief, *supra* note 12, at 34–35.

ment demands and thereby immunize the Government from constitutional claims.

**c. The Fact that Service Providers Can and Do Screen E-mail Under Certain Circumstances Does Not Eliminate a User's Expectation of Privacy Vis-à-vis Government Agents**

The Government errs when it claims that Congress, through adoption of the Stored Communications Act (“SCA”), granted service providers an unfettered right to access users’ e-mail and thereby extinguished any expectation of privacy. Congress simply cannot extinguish a constitutional right by statute. Moreover, the SCA grants no such unfettered right of access. It is true that a service provider is not subject to *federal criminal prosecution and civil liability* under the SCA for unauthorized access of its subscribers’ communications. Contrary to the Government’s suggestion, however, immunity from criminal or civil liability under one particular federal statute is not the same thing as an unfettered right of access, for it says nothing about other sources of law (including other federal statutes, contractual provisions, state statutes, or common law protections) that might limit a service provider’s access to a user’s communications.<sup>81</sup>

If communications providers retain broad rights of access to user e-mails in their own terms of service, those provisions do not concern the relationship between the user and the Government. Terms of service set forth the ways in which a service provider may need to protect its system and business from fraud, hacking, unauthorized use, and the like. Whatever rights the service provider might have to access communications to perform those functions, those rights do not give the service provider the right to disclose communications for the fundamentally different purpose of assisting law enforcement investigations of unrelated crimes.<sup>82</sup>

---

81. See *United States v. Councilman*, 418 F.3d 67, 82 (1st Cir. 2005) (en banc) (declining to dismiss federal Wiretap Act charge against service provider despite absence of SCA liability).

82. *United States v. Long*, 64 M.J. 57, 63 (C.A.A.F. 2006) (consent to monitoring did not imply consent to “engage in law enforcement intrusions by examining the contents of particular e-mails in a manner unrelated to maintenance of the e-mail system.”). Whether a user forfeits an expectation of privacy when he violates those terms of service is not at issue in this case. See *United States v. Young*, 350 F.3d 1302, 1308 (11th Cir. 2004) (expectation of privacy in package unreasonable when user shipped large amounts of cash in violation of clear carrier contract after acknowledging carrier’s unqualified right to inspect).

Notwithstanding its terms of service, a service provider's right to protect its own property does not release the Government from the constraints of the Constitution. Any third party that holds property on behalf of another, such as a storage company, may retain the right to inspect units to prevent damage that might occur to its property or that of other customers. The fact that the storage company has or exercises such a right, however, says nothing about the relationship between the storage customer and government agents. A storage company may, on its own initiative and independently of government action, provide to the Government the fruits of its own inspection. But that does not give government agents license to conduct their own warrantless search of a storage unit or to demand that the storage company search it on the Government's behalf. When the Government or its agent examines the contents of the storage locker, it invades a reasonable expectation of privacy, even though the storage company retained some right of access to protect its property.

In short, Warshak retained an expectation of privacy in his e-mails stored on his service providers' systems, notwithstanding their involvement in the search, their contract with him, or their business practices. As a result, the Government needed to obtain at least a probable-cause warrant before conducting the stored e-mail surveillance in this case.

## II. Government Agents Cannot Evade the Fourth Amendment's Warrant Requirement by Compelling Production of Communications from Third-Party Service Providers

For access to communications subject to a reasonable expectation of privacy, such as stored e-mails, the Fourth Amendment requires that government agents obtain (at a minimum) a warrant based on probable cause. Nevertheless, the Government argues that its agents need only satisfy a "reasonableness" standard when they "compel production" of materials.<sup>83</sup> To be clear, the Government does not argue merely that a reasonableness standard applies *when the target lacks a reasonable expectation of privacy* in the items the agents seek. Rather, the Government argues that the reasonableness standard applies *even when the target has a reasonable expectation of privacy*.<sup>84</sup> This argument

---

83. Government Brief, *supra* note 12, at 36.

84. *See id.* at 38 (arguing that "a target's reasonable expectation of privacy affects only his standing to challenge the reasonableness of compelled disclosure").

cannot withstand scrutiny. Government agents simply cannot write the warrant requirement out of the Fourth Amendment by compelling production of evidence whenever they wish, without regard for the underlying constitutionally-protected privacy interests.

The Government's error stems from an over-reading of cases applying a "reasonableness" standard where government agents have used a subpoena to compel production of documents or other items. Properly understood, those cases identify two overlapping circumstances in which a reasonableness standard may be appropriate: (1) where the target of an investigation has no reasonable expectation of privacy in the items the agents seek; and (2) when an agency uses a statutorily authorized administrative subpoena in aid of its regulatory mission, and pre-enforcement judicial process is available to evaluate the intrusiveness of its demands. Neither circumstance is present here.

**A. Use of a "Reasonableness" Test to Evaluate Compelled Production of Evidence Ordinarily Presumes or Follows a Determination that the Target of the Investigation Lacks a Reasonable Expectation of Privacy in the Items Agents Seek**

In arguing that there is a well established body of law applying a "reasonableness" standard to evaluate compelled production of materials,<sup>85</sup> the Government ignores a key unifying theme of this case law: that the use of a reasonable subpoena to compel production of materials is permissible where the target of the investigation *lacks any expectation of privacy* in those materials.

In its effort to draw a categorical distinction between searching for evidence and compelling its production, the Government relies on language in *United States v. Dionisio*,<sup>86</sup> a case involving whether a subpoena compelling individuals to appear before a grand jury and to give voice exemplars violated the Fourth Amendment.<sup>87</sup> *Dionisio* in fact undermines the Government's position, for it illustrates that use of a subpoena does not eliminate the need to inquire into a target's expectation of privacy. The Court bifurcated its analysis of the respondents' Fourth Amendment challenge, first concluding that the *order that the individuals appear* before the grand jury did not constitute an

---

85. Government Brief, *supra* note 12, at 38–39.

86. 410 U.S. 1 (1973).

87. *Id.* at 3; *see* Government Brief, *supra* note 12, at 39.

unlawful seizure,<sup>88</sup> and then examining whether, once the individuals were lawfully before the grand jury, the further *direction to make voice recordings* constituted an unlawful search.<sup>89</sup> The language on which the Government relies addressed only the first question, concerning the distinction between an arrest and a subpoena compelling one's appearance. On the second question, the Court concluded that no reasonable expectation of privacy existed, since the Fourth Amendment does not protect physical characteristics, such as the sound of one's voice, that an individual knowingly and necessarily exposes to the public.<sup>90</sup> What matters here is the Court's mode of analysis: the Court did not suggest that the mere use of a subpoena eliminates any need to inquire into any expectation of privacy. Rather, it recognized that compelled production of evidence can be sufficiently intrusive and immediate to constitute a search. Its assessment of whether the respondents had a reasonable expectation of privacy in voice characteristics would have been unnecessary if the Government's theory in this case were correct.

The "business records" cases on which the Government relies—in which courts applied a reasonableness standard in evaluating the use of subpoenas to compel production of corporate books and documents—carry similar import.<sup>91</sup> Many of those cases predated the Court's decision in *Katz v. United States*,<sup>92</sup> and thus have no bearing on whether use of a subpoena categorically defeats a reasonable expectation of privacy. In rejecting Fourth Amendment claims in such cases, the Court consistently underscored the fact that the records involved were merely corporate records.<sup>93</sup>

The Court's decision in *Katz* spurred new challenges to agents' acquisition of corporate records, on the theory that the owner or subject of the records had a reasonable expectation of privacy in the documents. The Supreme Court first squarely addressed such a claim in

---

88. *Dionisio*, 410 U.S. at 9–10.

89. *Id.* at 13–15.

90. *Id.* at 14.

91. See Government Brief, *supra* note 12, at 36–40, 43–45.

92. See Government Brief, *supra* note 12, at 36 (referring to "[a] century of Supreme Court case law"); *id.* at 38–89 (citing *Wilson v. United States*, 221 U.S. 361 (1911); *Okla. Press Publ'g Co. v. Walling*, 327 U.S. 186 (1946)).

93. See *Walling*, 327 U.S. at 208 (distilling prior case law as follows: "[I]n so far as [earlier cases] apply merely to the production of corporate records and papers in response to a subpoena or order authorized by law and safeguarded by judicial sanction," those cases establish that the Fourth Amendment "guards against abuse only by way of too much indefiniteness or breadth . . . if also the inquiry is one the demanding agency is authorized by law to make and the materials specified are relevant.").

*United States v. Miller*,<sup>94</sup> discussed above.<sup>95</sup> The Court concluded that the target of the investigation lacked any expectation of privacy in the documents and upheld the compelled disclosure, the reasonableness of which was uncontested by the banks to whom the subpoenas were issued.<sup>96</sup> Importantly, the Court never suggested that an inquiry into Miller's reasonable expectation of privacy was unnecessary because government agents proceeded by subpoena; it said that no expectation of privacy existed. Although *Miller* establishes the post-*Katz* vitality of a "reasonableness" analysis in cases involving compelled disclosure of business records, it is important to understand *why* a reasonableness analysis applies in *Miller* and subsequent cases. It is not because a target's expectation of privacy can always be overcome by a mere subpoena. Rather, it is because the targeted materials in cases such as *Miller* involve no expectation of privacy. Indeed, as the Court has observed, "[s]pecial problems of privacy" may be presented by attempts to compel production of items that are not business records, such as a personal diary.<sup>97</sup>

The subpoena cases on which the Government relies to suggest that use of a subpoena categorically eliminates the need to inquire into the target's expectation of privacy are additional cases in the *Miller* line.<sup>98</sup>

The Government cites only a single post-*Katz* case in which a court sustained the use of a subpoena to compel production of property despite the court's explicit assumption that the target of the investigation maintained an expectation of privacy in the property sought. In *United States v. Palmer*,<sup>99</sup> the Court of Appeals for the Ninth Circuit held that the Government did not violate the Fourth Amendment when it compelled a defendant's attorney to produce property held on the defendant's behalf. The court reasoned that "a properly limited subpoena does not constitute an unreasonable search and seizure under the fourth amendment."<sup>100</sup>

---

94. 425 U.S. 435 (1976).

95. See *supra* notes 64–73 and accompanying text.

96. See *Miller*, 425 U.S. at 446 n.9.

97. *Fisher v. United States*, 425 U.S. 391, 401 n.7 (1976).

98. See, e.g., *Donovan v. Lone Steer, Inc.*, 464 U.S. 408, 415 (1984) (seeking payroll and sales records, which the Court characterized as "corporate books or records"); *S.E.C. v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984) (seeking financial records).

99. 536 F.2d 1278 (9th Cir. 1976).

100. *Id.* at 1282.

In reaching this conclusion, *Palmer* relied on business cases pre-dating *Miller*, including *Walling*, *Hale v. Henkel*,<sup>101</sup> and others. *Palmer* was decided within six weeks of *Miller* and did not cite that decision. Because *Palmer* relied exclusively on cases that the *Miller* Court clarified involved no reasonable expectation of privacy, it is not persuasive authority for the proposition that a subpoena is appropriate even where a reasonable expectation of privacy exists.

### B. Administrative Subpoena Cases Are Wholly Inapplicable in This Case

The Government also relies on administrative subpoena cases to support a categorical distinction between compelling production of evidence and searching for evidence.<sup>102</sup> The rationale for evaluating an administrative subpoena under a reasonableness inquiry does not apply in this case.

Case law concerning administrative subpoenas recognizes that, when a corporation's activities affect interstate commerce, the federal Government has an investigative power analogous to the "visitatorial" power of the incorporating state.<sup>103</sup> Accordingly, Congress may grant an agency a "power of inquisition" into whether the law that the agency administers is being violated,<sup>104</sup> and courts will test the use of such a subpoena under a reasonableness analysis.<sup>105</sup>

Although the Government contends that the § 2703(d) orders at issue in this case are analogous to administrative subpoenas,<sup>106</sup> they are not. Even those statutes authorizing the Attorney General to issue administrative subpoenas as a prelude to a criminal investigation specify the narrow regulatory function the subpoena authority must serve.<sup>107</sup> In contrast, § 2703 is a general rule of criminal procedure,

101. 201 U.S. 43, 70 (1906).

102. See Government Brief, *supra* note 12, at 40–41 (citing *In re Admin. Subpoena John Doe*, D.P.M., 253 F.3d 256 (6th Cir. 2001); *United States v. Morton Salt Co.*, 338 U.S. 632 (1950)); *id.* at 39 (citing *In re Subpoena Duces Tecum* (*United States v. Bailey*), 228 F.3d 341 (4th Cir. 2000)).

103. See *Okla. Press Publ'g Co. v. Walling*, 327 U.S. 186, 204 (1946).

104. See *Morton Salt*, 338 U.S. at 642, 652 (noting that "the privilege of engaging in interstate commerce" carries with it "an enhanced measure of regulation").

105. See *Doe*, 253 F.3d at 265.

106. See Government Brief, *supra* note 12, at 41 n.7 (characterizing § 2703(d) orders as "a form of agency investigative authority" analogous to that recognized in *Morton Salt*).

107. See, e.g., 21 U.S.C. § 876 (2000) (authorizing use of administrative subpoenas in investigations "relating to the [Attorney General's] functions under this subchapter with respect to controlled substances, listed chemicals, tableting machines, or encapsulating machines"); 18 U.S.C. § 1968 (2000) (authorizing a "civil investigative demand" for "documentary materials relevant to a racketeering investigation"); 18 U.S.C. § 3486(a)(1)(A)(i)

R

R

analogous to Rule 41 of the Federal Rules of Criminal Procedure and untethered to any specific regulatory function. Cases concerning administrative subpoenas are thus wholly inapplicable in this case.

Even if administrative subpoena cases were relevant here, those cases do not support the Government's position that an inquiry into a reasonable expectation of privacy is irrelevant whenever government agents choose to compel production of, rather than search for, evidence. Administrative subpoena cases recognize not only that such subpoenas must serve a narrow regulatory mission, but also that the legitimacy of an administrative subpoena derives from the judicial process available to test the intrusiveness of the subpoena before it is enforced. Two of the administrative subpoena cases on which the Government relies—both dealing with administrative subpoenas in connection with health care fraud investigations—illustrate this principle. In *In re Subpoena Duces Tecum (United States v. Bailey)*,<sup>108</sup> the Court of Appeals for the Fourth Circuit explained that a subpoena “commences an adversary process during which the person served with the subpoena may challenge it in court before complying with its demands . . . . As judicial process is afforded *before any intrusion occurs, the proposed intrusion is regulated by, and its justification derives from, that process.*”<sup>109</sup> Similarly, in *In re Administrative Subpoena John Doe, D.P.M.*,<sup>110</sup> this Court recognized that the target of the administrative subpoena had an opportunity to challenge the intrusiveness of that subpoena before complying with it.<sup>111</sup> In both of these cases, the target of the subpoena was also the target of the investigation, and thus could assert any relevant privacy interests in the documents requested before a court enforced the subpoena.

An order to compel production of e-mail is distinct from the administrative subpoenas used in *Bailey* and *Doe* in two obvious respects. First, because the service provider on whom a § 2703(d) order is served is not the target of the investigation, and only the recipient of the order has an opportunity to challenge it, the target of the investigation has no opportunity parallel to that of *Bailey* or *Doe* to assert that the order is unduly intrusive. To be sure, as the Government notes, the Supreme Court has applied a reasonableness test to evalu-

---

(2000) (authorizing administrative subpoenas in connection with investigation of health care offenses or sexual exploitation or abuse of children).

108. 228 F.3d 341 (4th Cir. 2000).

109. *Id.* at 348 (emphasis added).

110. 253 F.3d 256 (6th Cir. 2001).

111. *Id.* at 264.

ate subpoenas even when agents compel disclosure of information held by parties who are not themselves the subject of an investigation.<sup>112</sup> As discussed above, however, the evaluation of a third-party subpoena under a reasonableness standard either presumes or follows a prior determination that the target of the investigation lacks an expectation of privacy in the items compelled.<sup>113</sup>

Second, in both *Bailey* and *Doe*, the documents the agents sought were records compiled in the ordinary course of a business relationship—records in which (as explained above) the Supreme Court has found any expectation of privacy to be unreasonable.<sup>114</sup>

In sum, contrary to the Government’s argument, the compelled production of evidence through use of a subpoena is not analytically distinct from a search for evidence. Both approaches require inquiry into a target’s reasonable expectation of privacy. To hold otherwise would be to suggest that government agents can evade the warrant requirement of the Fourth Amendment whenever it is convenient for them to do so, by “compelling production” of, rather than searching for, the evidence they seek.

## Conclusion

In sum, stored e-mail surveillance by the Government on less than probable cause violates the Fourth Amendment. Compelling a service provider to produce a person’s e-mail does not entitle government agents to evade constitutional prerequisites. A holding to the contrary would eviscerate the privacy of modern communications.

## List of Amici<sup>115</sup>

Ann Bartow  
Associate Professor of Law  
University of South Carolina School of Law

---

112. See Government Brief, *supra* note 12, at 43.

113. See *supra* notes 85–101 and accompanying text.

114. See *supra* notes 64–73 and accompanying text; *Bailey*, 228 F.3d at 344 (listing purchase records, bank records, records concerning requirements of filing health care claims, and records of patients whose services were billed to particular insurance companies); *id.* at 351 (noting that patient records involved were subject to agreement to release information to insurance companies); *Doe*, 253 F.3d at 260–61 (listing bank and financial records of Doe and family members, tax records, patient referral records, and records concerning Doe’s medical education).

115. The affiliations listed are for identification purposes only.

Patricia L. Bellia

Lilly Endowment Associate Professor of Law  
Notre Dame Law School

Eric. B. Easton

Professor of Law  
University of Baltimore School of Law

Susan Freiwald

Professor of Law  
University of San Francisco School of Law

Jennifer S. Granick

Director and Instructor of the Stanford Cyberlaw Clinic  
Stanford Law School

Stephen E. Henderson

Associate Professor  
Widener University School of Law

Deirdre Mulligan

Director, Samuelson Law, Technology and Public Policy Clinic  
University of California, Berkeley,  
Boalt Hall School of Law

Charles B. Meyer

Visiting Professor of Law  
University of Houston Law Center

Neil M. Richards

Associate Professor of Law  
Washington University in St. Louis

Michael L. Rustad

Thomas F. Lambert, Jr. Professor of Law  
Suffolk University Law School

Pamela Samuelson

Chancellor's Professor of Law and Information Management  
University of California, Berkeley

---

Christopher Slobogin  
Stephen C. O'Connell, Chair, Professor of Law  
University of Florida College of Law

Katherine J. Strandburg  
Associate Professor of Law  
DePaul University College of Law

Peter Swire  
C. William O'Neill Professor of Law  
Moritz College of Law of the Ohio State University

Mary W.S. Wong  
Professor of Law  
Franklin Pierce Law Center

