Fourth Amendment Protection for Stored E-mail

Patricia L. Bellia  
Notre Dame Law School, patricia.l.bellia.2@nd.edu

Susan Freiwald

Follow this and additional works at: https://scholarship.law.nd.edu/law_faculty_scholarship

Part of the Fourth Amendment Commons, and the Internet Law Commons

Recommended Citation
Available at: https://scholarship.law.nd.edu/law_faculty_scholarship/453

This Article is brought to you for free and open access by the Publications at NDLScholarship. It has been accepted for inclusion in Journal Articles by an authorized administrator of NDLScholarship. For more information, please contact lawdr@nd.edu.
Fourth Amendment Protection for Stored E-mail†

Patricia L. Bellia and Susan Freiwald‡

INTRODUCTION 122
I. THE WARSHAK DECISION 126
   A. The Legal Framework 126
   B. The Warshak Investigation 130
   C. The Warshak Litigation 131
      1. The district court decision. 131
      2. The government's arguments on appeal. 131
      3. The panel's decision. 133
II. WHY THE FOURTH AMENDMENT'S WARRANT REQUIREMENT PROTECTS STORED E-MAIL: THE NATURE OF STORED E-MAIL SURVEILLANCE 135
III. REFUTING THE GOVERNMENT'S ARGUMENTS 141
   A. The Compelled Disclosure Argument 141
   B. The Third Party Argument 147
      1. Stored e-mails are neither "corporate" nor "business" records. 149
      2. Assumption of risk. 153
      3. A clean slate. 157
   C. Internet Service Providers and Reasonable Expectations of Privacy 158
      1. Evaluating the government's claims. 159
      2. Summary. 168
   D. Comparison of the Warshak Panel's Approach 169
      1. Reasonable expectations of privacy in ISP relationships. 169
      2. Raising Fourth Amendment claims. 170

† Copyright © 2008 Patricia Bellia and Susan Freiwald.
‡ Professor of Law and Notre Dame Presidential Fellow, Notre Dame Law School, and Professor of Law, University of San Francisco School of Law. Research librarian Christopher O'Byrne (Notre Dame) and law students Cameron Cloar, Alex Miller, Amy Morganstern, and Anthony Phillips (USF) and Jeffery Houin (Notre Dame) provided excellent research assistance. We also thank Suzanne Mounts and Steven Shatz for their helpful comments.
INTRODUCTION

Imagine that government agents believe that Alice and Bob are engaged in criminal activity and that communications between them will yield incriminating evidence of money laundering. As the agents contemplate how to obtain the pair's conversations from Alice, they may choose among three investigative methods that impose dramatically different procedural hurdles. Under the government's interpretation of current law, agents may much more easily obtain the electronic communications stored by Alice's internet service provider ("ISP") than search her home for records of their conversations or wiretap her phones to intercept their calls.2

According to the Department of Justice ("DOJ"), government agents may compel ISPs to disclose most stored e-mail messages without first obtaining a warrant based on a showing of probable cause and in some cases without even providing notice to the subscriber.3 Instead, government agents may merely establish to a court that they have reason to believe that the electronic messages they seek are relevant to an ongoing investigation. According to the DOJ, there is no limit on how much information the ISP must disclose; the government may compel ISPs to disclose a substantial portion of a customer's e-mail account, even though the agents obtain no meaningful judicial review before, during, or after their demand for information.

---

1 Alice and Bob are archetypal characters frequently used in discussions of cryptography and computer security. See, for example, Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C 47 (Wiley 2d ed 1996); A. Michael Froomkin, The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution, 143 U Pa L Rev 709, 754 (1995).

2 Agents may also choose to intercept e-mails in real time, but to do that they must follow procedures that are similar to those that regulate the wiretapping of traditional telephone calls. See, for example, James G. Carr & Patricia L. Bellia, The Law of Electronic Surveillance § 1:14 (Thomson West 2007); Susan Freiwald, Online Surveillance: Remembering the Lessons of the Wiretap Act, 56 Ala L Rev 9, 42-73 (2004) (comparing the procedures for online surveillance to those for wiretapping).

3 We discuss the government's approach to various categories of e-mail in Part I A.
If agents had instead sought a search warrant to obtain Alice's e-mails from her home, they would have had first to persuade a judge that they had probable cause to believe that the search would yield evidence of a crime. To obtain a wiretap on Alice's phone line, the agents would have had to establish probable cause, demonstrate that there was no less intrusive way to obtain the information, and satisfy other procedural requirements. Both the home search and the wiretap would be subject to much more penetrating judicial oversight and review, despite the fact that neither technique is more obviously intrusive. In fact, it is unlikely that the home search would yield as much evidence of Alice's communications with Bob as the demands for information from the ISP. Similarly, a wiretap would yield only those communications that take place after the tap is placed and would not yield the richness of data available from the ISP's servers.

The government has derived support for this oddly disparate treatment from the provisions of the Stored Communications Act ("SCA"). Congress passed the SCA in 1986 as part of the Electronic Communications Privacy Act ("ECPA"), which was designed to bring privacy protections to the newly emerging communications media. Interestingly, despite the explosion in use of electronic communications technologies since the SCA's passage, Congress has not updated its terms or significantly changed its structure. More fundamentally, until last year, no Article III court had opined on the constitutionality of the government's compelled disclosures of electronic communications.

---

4 FRCrP 41.
6 See Brief for Professors of Electronic Privacy Law and Internet Law as Amici Curiæ Supporting the Appellee and Urging Affirmance, Warshak v United States, No 06-4092, *6-7 (6th Cir filed Nov 21, 2006) (available on Westlaw at 2006 WL 4670944) ("Warshak Law Professors' Brief"). We were the authors of the Professors' brief.
9 See United States v Ferguson, 508 F Supp 2d 7, 9 (D DC 2007) (noting that, prior to the district court's ruling in Warshak, no court had ruled the SCA unconstitutional). The Court of Appeals for the Armed Forces, a non-Article III court, had previously opined that users generally do have an expectation of privacy in e-mail. See United States v Long, 64 MJ 57, 64–67 (Ct App Armed Forces 2006) (applying Fourth Amendment precedents outside of the e-mail context to find that defendant had a reasonable expectation of privacy in her e-mails); United States v Maxwell, 45 MJ 406, 418 (Ct App Armed Forces 1996) ("[T]he transmitter of an e-mail message enjoys a reasonable expectation that po-
Despite the government’s admission that demands for stored e-mails represent an “important, widely-used tool in criminal investigations involving fraud, terrorism, child pornography, drug trafficking, and other crimes,” no court had considered what constraints, if any, the Fourth Amendment prohibition of unreasonable searches and seizures imposes. Because the government appears to rely heavily on the technique, its unconstitutionality would mean that the government has been committing innumerable constitutional violations.

In June 2007, a federal appellate court finally translated the benchmark Fourth Amendment standard of the reasonable expectation of privacy into the language of stored e-mail. The news was not good for the government. In Warshak v United States, the U.S. Court of Appeals for the Sixth Circuit held that subscribers generally enjoy an expectation of privacy in e-mail messages they store with an ISP, which means that government agents ordinarily cannot compel providers to disclose those stored e-mails without first securing a judicial warrant based on a showing of probable cause. Under the panel’s decision, government agents seeking to compel a service provider to disclose e-mail must acquire a warrant, establish to a court that no warrant is needed because the target lacks an expectation of privacy in the e-mails sought, or provide to the target notice and an opportunity to be heard. The Court thus invalidated the SCA to the extent that it permits access to stored e-mails without adherence to these procedures.

The Sixth Circuit reheard the case en banc in December 2007, after having vacated the panel’s decision. The en banc court recently issued a decision in which it vacated the preliminary injunction because it found Warshak’s claim not ripe for lice officials will not intercept the transmission without probable cause and a search warrant. . . . The sender enjoys a reasonable expectation that the initial transmission will not be intercepted by the police.”)


12 Warshak, 490 F3d at 473 (“[W]e have little difficulty agreeing with the district court that individuals maintain a reasonable expectation of privacy in e-mails that are stored with, or sent or received through, a commercial ISP.”).

13 See id at 475–76, 482. We discuss what issues the target should be able to raise in such a hearing in Part III D 2.

judicial resolution. The court did not address the constitutionality of the SCA and the government's practices pursuant to it. Because the en banc court rejected Warshak's claim on procedural grounds, whether the Fourth Amendment permits government agents to compel disclosure of stored e-mail without a warrant or an applicable exception will persist as a pressing question. As the only available analysis of the question by an Article III court, the Sixth Circuit's panel decision deserves close scrutiny. Moreover, in the short period between the time it was issued and when it was vacated, Warshak's reasoning proved influential in several cases involving communications surveillance practices.

In this Article, we argue that the panel got it right when it found that e-mail users generally retain a reasonable expectation of privacy in the e-mails stored on their ISPs' computers. Government agents' invasion of that reasonable expectation of privacy constitutes a search under the Fourth Amendment, and agents ordinarily cannot proceed with a search without first obtaining a warrant from a neutral magistrate based on a showing of probable cause. According meaningful judicial oversight to the compelled disclosure of stored e-mails brings the regulation of modern surveillance practices in line with traditional methods such as wiretapping and searching and seizing traditional letters. It also appropriately recognizes the vital nature of e-mail

15 Warshak v United States, 532 F3d 521 (6th Cir 2008) (en banc).

16 The decision indicated that the en banc court viewed the question of whether the target entertains a reasonable expectation of privacy in his stored e-mail to be quite fact specific, and to depend, in some fashion, on the nature of the ISP's contract and relationship with the target. Id at 526-28. That view is fairly close to the panel's approach, and so we do not separately analyze it. We explain our disagreement with this approach in Part III D.


18 See, for example, United States v D'Andrea, 497 F Supp 2d 117, 121-22 (D Mass 2007) (relying on Warshak's analysis that a user assumes the risk of losing the expectation of privacy when sharing information with others, depending upon how such information is shared); Platte v Thomas Township, 504 F Supp 2d 227, 239 (E D Mich 2007) (striking down as unconstitutional under a facial challenge a state statute authorizing warrantless breath tests); In re United States, 515 F Supp 2d 325, 337-38 (E D NY 2007) (explaining that under the Warshak standard, telephone users held a reasonable expectation of privacy in post-cut-through dialed digits (digits dialed after a telephone call has commenced)).
today and the need to rein in government access to it. Not only is the court’s conclusion that the Fourth Amendment’s warrant requirement protects e-mail right, but it has significant salutary effects on both constitutional and statutory law regarding communications surveillance. It clarifies that electronic communications are constitutionally private, notwithstanding the necessary involvement of third parties in their transmission and storage. It also dramatically simplifies the application of the SCA to new technologies, which in turn facilitates both compliance by agents and ISPs and review by courts of that compliance.

In Part I, we briefly review the statutory background, the Warshak case itself, the government’s arguments in support of its agents’ practices, and the panel’s response. In Part II, we discuss how according the same constitutional protection to e-mail as is afforded to telephone calls and first class letters resolves concerns about the irrationality of the disparate treatment and properly assesses users’ reasonable expectations of privacy. In Part III, we consider the government’s arguments in greater depth and conduct a detailed analysis of the precedents. We argue that courts should not accept the government’s invitation to extend those precedents well beyond their holdings. Instead, courts should clarify that the Fourth Amendment’s warrant requirement does play a role in regulating law enforcement access to our electronic communications, wherever they may be. In Part IV, we explain how warrant-level protection for stored e-mail significantly simplifies the application of the SCA and strengthens its protections. We conclude with some questions about whether the Warshak panel went far enough in recognizing Fourth Amendment protection for stored e-mail.

I. The Warshak Decision

A. The Legal Framework

To understand the issues at stake in the Warshak case, one must understand the structure of the SCA and the Department of Justice’s interpretation of it. The SCA establishes procedures for government access to electronic communications held by ser-

---

vice providers. The statute does not, however, establish uniform access rules for all stored electronic communications. In Part IV, we argue that recognizing that the Fourth Amendment’s warrant requirement protects stored e-mail does lead to a much simpler and more unified approach, but for now, the government proceeds as though the warrant requirement does not apply. Though scholars, including ourselves, have criticized the government’s approach extensively, it appears clear from the government’s arguments in the Warshak case that it views most, if not all, stored e-mails as not subject to the warrant requirement.

The SCA provides the most protection to communications that are in “electronic storage” with the provider of an “electronic communication service” for 180 days or less. More specifically, under 18 USC § 2703(a), government agents seeking to acquire such communications must obtain a search warrant. A warrant issues only after a judge finds probable cause to believe that a specific crime has been, is being, or will be committed and that the search will yield evidence, instrumentalities, or fruits of the crime. The warrant requirement thus places a neutral magistrate between the law enforcement agent and the target of the investigation. The probable cause finding provides a record of justification that the target may challenge in court before evidence from the search may be used against him.

According to the DOJ’s interpretation of it, the SCA does not require agents to obtain a warrant if they are seeking communications that are not in “electronic storage” with the provider of an “electronic communication service” or if they are seeking communications that remain in storage for more than 180 days. Instead, agents can compel disclosure through procedures that are less protective of the subscriber’s interests. First, government investigators can obtain communications by presenting


22 FRCrP 41.

23 The target’s ability to challenge the search depends upon the target having been notified of the search. Standard principles of criminal procedure require such notice. FRCrP 41. The Justice Department, however, interprets § 2703(a) of the SCA not to require notice to the target, apparently on the theory that the service provider, rather than the target, is the searched entity. *DOJ Search Manual* at 97–99 (cited in note 19). We return to this issue in Part IV A.

24 See 18 USC § 2703(b) (2000 & Supp IV 2004). Agents can rely on a warrant if they choose. Here the statute is clear that if agents do use a warrant, they need not provide prior notice to the subscriber. Id at § 2703(b)(1)(A).
a special court order issued under § 2703(d) of the SCA. To obtain such an order, government agents must present "specific and articulable facts" demonstrating that the material they seek is "relevant" to an ongoing criminal investigation—a standard that is lower than probable cause. Second, government investigators can compel production of communications by presenting a service provider with a trial subpoena, a grand jury subpoena, or an administrative subpoena. Subpoenas typically require only a showing that agents seek information that is "relevant" to an ongoing criminal investigation, rather than a showing of probable cause that a specific crime is being committed. Moreover, the government’s showing is typically not evaluated by a judge.

Because the government’s approach accords warrant-level protection only to those communications held in "electronic storage" by the provider of an "electronic communication service," a crucial question concerns how to determine which communications those are. By cross-reference to the federal Wiretap Act, the SCA defines "electronic storage" to include "temporary, intermediate storage of a wire or electronic communication incidental to the transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection."

The Department of Justice has long interpreted the "electronic storage" definition to cover only communications that have not yet been accessed by their recipients. Once a subscriber retrieves an e-mail and does not delete it from the provider’s system, the Justice Department claims, such an e-mail is no longer

---

25 Id at § 2703(b)(1)(B)(ii).
26 Id at § 2703(d).
27 Id at § 2703(b)(1)(B)(i). If investigators rely on a § 2703(d) order or a grand jury or administrative subpoena rather than a warrant, they generally must provide prior notice to the subscriber. The SCA also allows the government to compel production of communications without prior notice to the subscriber if there is "reason to believe that notification" will have an "adverse result": endangering the life or physical safety of an individual; causing flight from prosecution; causing destruction or tampering with evidence; causing intimidation of potential witnesses; or otherwise seriously jeopardizing an investigation or unduly delaying a trial. In such a case, notice may be delayed by renewable periods of up to ninety days. 18 USC § 2705 (2000).
28 See William J. Stuntz, O.J. Simpson, Bill Clinton, and the Trans substantive Fourth Amendment, 114 Harv L Rev 842, 864 (2001) (describing subpoenas as equivalent to a "blank check"). Trial subpoenas are typically issued by a clerk of court (or in some cases an attorney); grand jury subpoenas are typically issued by the clerk of court on behalf of the grand jury; and administrative subpoenas are issued by administrative agencies with appropriate statutory authority.
"temporarily" stored but remains on the provider's system indefinitely.\textsuperscript{31} The Justice Department contends that an e-mail that continues to be stored on a provider's system is akin to a remotely stored file,\textsuperscript{32} entitled at most to the statute's lesser, subpoena-like protections and falling outside of the statute altogether when stored on a system that does not provide services to the public.\textsuperscript{33}

We have each discussed elsewhere the difficulties with the government's interpretation and the anomalies it produces.\textsuperscript{34} For now, the key point is that the Justice Department's narrow understanding of the statutory term "electronic storage"—an understanding that has achieved limited success in the few cases to consider it\textsuperscript{35}—implies that government agents may acquire, by compelled disclosure, a large category of stored e-mails. That category includes those downloaded, accessed, or opened; sent or drafted; or stored more than 180 days; without obtaining a warrant based on probable cause. Because the Justice Department has never articulated a \textit{constitutional} (as opposed to \textit{statutory}) distinction between e-mail not yet accessed by a subscriber and e-mail already retrieved by a subscriber, its position necessarily depends on the premise that the Fourth Amendment's warrant requirement does not apply to stored e-mail at all—that the government must obtain a warrant before compelling a service provider to produce e-mail in electronic storage only because the

\textsuperscript{31} Id at 86–87.

\textsuperscript{32} Id at 87–89. Note that it is not clear if the shift takes place when the user accesses the contents of the e-mail or when the user downloads the e-mail from a central server to her own personal computer. See id at 88–89 (describing shift as taking place when user "accesses" her ISP and "retrieves" her message).

\textsuperscript{33} How the statute protects an e-mail that remains on a provider's system depends, in the Justice Department's view, on whether the provider offers services to the public, such as Gmail. Non-public providers include universities and corporations that provide e-mail services to their students and/or employees. The crux of the Justice Department's argument is that a provider that holds an e-mail after a recipient has accessed it no longer acts as an "electronic communication service" with respect to that communication. Rather, with respect to that communication, it acts, if anything, as a "remote computing service." \textit{DOJ Search Manual} at 87–89. Since the SCA defines a remote computing service as "the provision to the public of computer storage or processing services," 18 USC § 2711(2) (2000 & Supp IV 2004), communications already accessed by a subscriber qualify for statutory protection only if they are stored with a provider that offers services to the public.

\textsuperscript{34} See Freiwald, 56 Ala L Rev at 49–52, 57–60 (cited in note 2); Bellia, 75 U Chi L Rev at 174–75 (cited in note 20); Bellia, 72 Geo Wash L Rev at 1417–26 (cited in note 20).

SCA requires it and not because such compulsion constitutes a search or seizure under the Fourth Amendment.

We provide our own critique of the government's position in Parts II and III. What follows is our recounting of the history of the Warshak case, because the district court and Sixth Circuit panel stand as the only Article III courts to directly confront the constitutional issue raised by the government's construction of the SCA.

B. The Warshak Investigation

In the course of investigating Steven Warshak and his company, Berkeley Premium Nutraceuticals, for suspected mail and wire fraud and money laundering activities, the United States sought access to Warshak's e-mail. In 2005, federal investigators applied for court orders compelling two of Warshak's internet service providers, NuVox Communications and Yahoo!, to disclose the contents of "wire or electronic communications (not in electronic storage unless greater than 181 days old) that were placed or stored in directories or files owned or controlled by" Warshak. 36 NuVox and Yahoo! complied with the orders, apparently producing thousands of electronic communications that Warshak had sent or received over the previous nine years. 37

Instead of obtaining a warrant based on probable cause for access to Warshak's e-mail accounts, the government sought and obtained court orders pursuant to § 2703(d) of the SCA. As noted, to obtain a § 2703(d) order, government investigators must merely provide the issuing court with "specific and articulable facts" that demonstrate that the material they seek is "relevant" to an ongoing criminal investigation. 38 The government did not notify Warshak of the seizures of his e-mail until more than a year after issuance of the first court order. 39 Soon thereafter, Warshak

---

36 See Warshak v United States, 2006 WL 5230332, *1 (S D Ohio 2006). The order further explained that e-mails "not in electronic storage" meant those e-mail communications "received by the specified accounts that the owner or user of the accounts has already accessed, viewed, or downloaded." Id. The Yahoo! order was similar. Id at *2.

37 Yahoo! did not disclose e-mails stored for fewer than 180 days; however, NuVox "turned over to the government many emails which were less than 181 days old." See Final Brief of Plaintiff-Appellee Steven Warshak, Warshak v United States, No 06-4092, *2–3 (6th Cir filed Nov 13, 2006) (available on Westlaw at 2006 WL 4670943).


39 See Warshak, 2006 WL 5230332 at *2. The statute permits government agents to delay notice to the target for 90 days, unless the agents obtain orders for extensions. 18 USC § 2705(a) (2000). The government never obtained any orders for extension. See Warshak, 490 F3d at 460–61 & n 1. The SCA itself does not contain a penalty for the govern-
filed suit against the government in the Southern District of Ohio, claiming that the government's court orders violated both the SCA and the Fourth Amendment. After Warshak's counsel sought and was denied assurances from the government that it would not again use a § 2703(d) order or similar procedure to compel disclosure of further e-mails, Warshak moved for a preliminary injunction prohibiting such conduct.

C. The Warshak Litigation

1. The district court decision.

The district court did not directly consider Warshak's SCA claim, but the court did hold that Warshak had demonstrated a likelihood of success on the merits of his constitutional claim. With regard to senders' expectations of privacy, the court reasoned that stored e-mails are analogous to sealed letters or packages shipped by public or private carriers.\(^4\) The Supreme Court has held that "warrantless searches of such effects are presumptively unreasonable."\(^4\) In resisting this analogy before the district court in Warshak, the government had argued that ISPs differ from public or private carriers of sealed letters or packages because they typically reserve the right to access and delete e-mails and to provide e-mails to law enforcement agents where appropriate. Nonetheless, the district court concluded "as an initial matter" that it was not persuaded that "an individual surrenders his reasonable expectation of privacy in his personal e-mails once he allows those e-mails (or electronic copies thereof) to be stored on a subscriber account maintained on the server of a commercial ISP."\(^4\)

2. The government's arguments on appeal.

On appeal before the Sixth Circuit panel, the government challenged the court's Fourth Amendment analysis using three interrelated arguments.\(^4\) The government's broadest argument concerns the fact that agents proceed by compelling disclosure of

---

41 United States v. Jacobsen, 466 US 109, 114 (1984) ("Letters 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.").
42 Warshak, 2006 WL 5230332 at *5.
43 The government also made various procedural arguments not discussed here.
the e-mails they seek. According to the “compelled disclosure argument,” the Fourth Amendment’s warrant requirement does not apply when the government chooses to compel disclosure or production of an item rather than conduct a more traditional search, such as of a home, or a more traditional seizure, such as of a person. Instead, the argument posits, courts evaluate compelled disclosure under a reasonableness inquiry, irrespective of whether the target of the investigation retains an expectation of privacy in the material the government seeks. According to the government, so long as it seeks relevant information in a manner that is not unduly burdensome, compelled disclosure of stored e-mail without a warrant satisfies the Fourth Amendment, without any consideration of a user’s reasonable expectation of privacy or lack thereof.

Under the second argument—which we call the “third party argument” or “third party rule”—when a user relies on a third party to hold his or her communications, that alone defeats any expectation of privacy that otherwise might exist in those communications. The government’s logic seems to be that because a subscriber necessarily “reveals” e-mail communications to her ISP by allowing the ISP to store them, she assumes the risk that the ISP might choose or even be compelled to disclose those records to the government.

As an alternative, under the third argument, which we call the “ISP relationship” argument, the government claims that the typical subscriber-ISP relationship defeats any expectation of privacy that otherwise might exist in stored electronic communications. The government focuses in particular on (1) ISPs’ technical ability to access the contents of communications; (2) ISP terms of service, which typically reserve to the ISP the right to access the contents of users’ communications for various reasons; and (3) actual ISP practices of screening the contents of communications for viruses, spam, and child pornography. According to the government, when a user accedes to an ISP relationship with these parameters, she forfeits any claim to an ex-

---

44 The government’s pleadings and briefs reverse the order of the arguments above. We treat the compelled disclosure argument first, however, because it is broader and thus logically prior to the third party argument. That is, if the government is correct that compelled disclosure is subject to a reasonableness inquiry in all circumstances—even if the user retains an expectation of privacy in the materials sought to be compelled—then the question whether the user does retain an expectation of privacy in the materials becomes irrelevant.

45 See Part III C for further discussion of the ISP-user relationship.
pectation of privacy in her stored communications, and thereby forfeits any claim that government acquisition of her stored communications is a search for purposes of the Fourth Amendment.

3. The panel’s decision.

In concluding that users generally retain an expectation of privacy in e-mails held by commercial service providers, the Warshak panel explicitly or implicitly rejected each one of governments’ arguments. First, the court rejected a blanket “compelled disclosure” exception to the Fourth Amendment’s warrant requirement and concluded that protection must instead turn on whether the user retains a reasonable expectation of privacy with respect to the entity compelled to make the disclosure and with respect to the information to be disclosed. Second, the panel rejected the third party argument by implicitly concluding that the mere fact that a service provider has possession of or control over a user’s communications does not, without more, eliminate the user’s expectation of privacy. Finally, regarding the ISP relationship argument, the court found that a provider’s technical ability to access the contents of the communication does not, without more, eliminate the user’s expectation of privacy. In rejecting each of government’s arguments, the court necessarily refined in important ways the expectation of privacy inquiry, at least as it applies to material held by a third party. First, rather than being purely positive, the court’s inquiry was normative. That is, rather than focusing exclusively on actual societal expectations with respect to the privacy of communications, the court considered the vital role e-mail plays in private

---

46 Warshak, 490 F3d at 471. In this respect, the court relied on the necessary implications of Katz v United States, 389 US 347 (1967), the decision in which the Supreme Court first recognized that interception of telephone communications requires a warrant. The Court could not have reached that result in Katz if the telephone provider’s technical ability to access the contents of a telephone communication had any Fourth Amendment significance.

47 More specifically, the court observed that the use of software to screen messages for spam, viruses, or child pornography does not expose the contents of communications to any person at the ISP or elsewhere and that many instances in which ISPs reserve rights to monitor communications involve “extraordinary” circumstances rather than the ordinary course of business (as, for example, where a communication is claimed to violate a third party’s rights or jeopardize the provider’s property). Warshak, 490 F3d at 474.
communications: "protecting shared communications through this medium is as important to Fourth Amendment principles today as protecting telephone conversations has been in the past." The court supplemented this inquiry with a positive inquiry designed to determine whether specific circumstances defeated this privacy interest. This positive analysis, however, essentially reduced to a question of how a third party's access to a communication affects the privacy interest that a normative analysis would yield. The court first focused on the party with whom the subscriber "shares" the communication, and precisely what the subscriber discloses. A subscriber shares a communication with or discloses a communication to its recipient. The subscriber does not disclose a communication to a provider in any way relevant to the Fourth Amendment analysis merely by virtue of the fact that the provider has a technical ability to access the communication, or by virtue of the fact that, in the ordinary course of business, the provider must access limited additional information necessary to route the communication properly.

In the end, the panel held that, except in limited circumstances, law enforcement agents must obtain a warrant based on probable cause before they may compel a commercial service provider to disclose the e-mails it stores. The panel elaborated that the government does not need to obtain a prior warrant when it establishes to a reviewing court's satisfaction that the ISP has extinguished its user's expectation of privacy in her communications by (a) explicitly reserving the right to monitor (b) the contents of communications and (c) exercising that right in the ordinary course of its business. Alternatively, the government may avoid obtaining a prior warrant if it instead provides the target with notice and an opportunity to be heard. As the district court recognized, if the government were to choose the third option of forgoing either a warrant or a showing that the target lacked a reasonable expectation of privacy in the stored e-mail, the target would be able to raise a claim at the hearing that the compelled disclosure invades his reasonable expectation of privacy. We revisit the issue of the target's claims in such hear-

48 Warshak, 490 F3d at 473.
49 Id at 475–76. The panel also specified that the government must comply with the particularity requirement by not obtaining e-mails as to which the subscriber had not waived a reasonable expectation of privacy. Id at 475–76 & n 8.
50 Id at 473–74.
51 Warshak at 475–76, 482.
52 See Warshak, 2006 WL5230332 at *8 ("Warshak should have the opportunity to
ings and the panel's ambiguous comments on them in Part III D 2.

II. WHY THE FOURTH AMENDMENT'S WARRANT REQUIREMENT PROTECTS STORED E-MAIL: THE NATURE OF STORED E-MAIL SURVEILLANCE

Recognizing that the government's acquisition of stored e-mail constitutes a Fourth Amendment search would bring constitutional regulation of modern surveillance practices into the modern age and eliminate the strangely disparate treatment of mailed and telephonic communications on the one hand and electronic communications on the other. When stored e-mails receive proper Fourth Amendment protection, government agents will be able to access our stored electronic communications only when their actions are subject to meaningful judicial oversight.

The Supreme Court and lower courts have long recognized that the judiciary must play an active role in overseeing executive branch electronic surveillance. The Court emphasized that need in *Berger v New York*, when it overturned a New York statute that provided insufficient judicial involvement in executive branch surveillance practices. As a matter of Fourth Amendment doctrine, the Court opined that an electronic surveillance scheme that operated without sufficient procedural safeguards must be considered the sort of general warrant that the Fourth Amendment specifically prohibits.

Twenty years later, seven federal courts of appeals interpreted *Berger* and the Fourth Amendment requirements it im-

53 The ECPA currently provides significantly greater protection to wire communications, which are defined as including the human voice, than to electronic communications. See Freiwald, 56 Ala L Rev at 41–42 (cited in note 2); Carr & Bellia, The Law of Electronic Surveillance § 1:14 (cited in note 2).

54 388 US 41 (1967).

55 Id at 60 (concluding that the New York statute's "blanket grant of permission to eavesdrop is without adequate judicial supervision or protective procedures"); id at 56 (noting that indiscriminate use of eavesdropping devices in law enforcement "raises grave constitutional questions under the Fourth and Fifth Amendments," and imposes "a heavier responsibility on this Court in its supervision of the fairness of procedures," quoting Osborn v United States, 385 US 323, 329 n 7 (1966)).

56 *Berger*, 388 US at 59 ("As with general warrants [the statute's failure to require particularity] leaves too much to the discretion of the officer executing the order."); id at 64 ("Our concern with the statute here is whether its language permits a trespassory invasion of the home or office, by general warrant, contrary to the command of the Fourth Amendment.").
posed to establish the need for heightened oversight of electronic surveillance because of its unique features. In particular, the courts described electronic surveillance as intrusive, continuous, hidden, and indiscriminate, and therefore in need of even more judicial involvement than that accorded to searches of the home or seizures of persons. Interestingly, in those cases, the courts of appeals extended to the emerging practice of hidden video surveillance by government agents the same heightened protections that the Supreme Court had imposed in Berger. The 1968 precursor to the ECPA had not covered hidden video surveillance, likely because it was not sufficiently commonplace to garner congressional attention. The courts of appeals extended heightened protection to video surveillance as a matter of Fourth Amendment doctrine, based on their assessment that it shares the same key features as the wiretapping of traditional telephones.

Why then, have the courts not made the same finding with regard to government access to stored electronic communications? As one of us has argued elsewhere, surely government access to years of stored e-mail shares the characteristics of being hidden, intrusive, continuous, and indiscriminate. As we have both argued, there are strong arguments for viewing access to stored e-mail communications as much more informative than traditional wiretapping and more efficient for information gath-

---

57 Consider United States v Mesa-Rincon, 911 F2d 1433, 1439 (10th Cir 1990) (adopting the Berger requirements for determining the validity of video surveillance); United States v Biasucci, 786 F2d 504, 510 (2d Cir 1986) (discussing the constitutional requirements Berger imposes on electronic surveillance). See also United States v Torres, 751 F 2d 875, 882–84 (7th Cir 1984) (concluding that video surveillance is “exceedingly intrusive” and must comport with the Fourth Amendment, and holding that the government’s compliance with the federal Wiretap Act satisfied Fourth Amendment requirements); United States v Cuevas-Sanchez, 821 F2d 248, 251–52 (5th Cir 1987) (following Torres and Biasucci and concluding that the government’s compliance with the federal Wiretap Act’s requirements “protect[s] the constitutional rights of those under surveillance as they have been announced by the Supreme Court”); United States v Koyomejian, 970 F 2d 536, 542 (9th Cir 1992) (en banc) (concluding that, although the Wiretap Act does not directly regulate video surveillance, the Fourth Amendment requires adherence to the non-technical provisions of the Wiretap Act); United States v Falls, 34 F 3d 674, 680 (8th Cir 1994) (following prior cases in holding that video surveillance is “a very serious . . . invasion of privacy” and distilling from the Wiretap Act procedures to implement the Fourth Amendment); United States v Williams, 124 F 3d 411 (3d Cir 1997) (assuming the validity of the approach of the other circuits).

58 See Freiwald, 56 Ala L Rev at 79–80 (cited in note 2).

59 See cases cited in note 57.

erating than the more obvious analog of real-time access to e-mails in transmission.\textsuperscript{61}

Shortly after its decision in \textit{Berger}, the Supreme Court considered another Fourth Amendment challenge to government surveillance practices. In \textit{Katz v United States},\textsuperscript{62} the Court held that government agents' use of an electronic listening device to pick up Katz's end of a telephone conversation constituted a "search" and could not proceed without a warrant.\textsuperscript{63} The Court assessed whether government actions constituted a search by asking whether the target justifiably expected privacy in his telephone conversations.\textsuperscript{64} As developed in Justice Harlan's concur-

rence and in subsequent Supreme Court cases, the reasonable expectation of privacy test asks whether the 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).\textsuperscript{65}

Applying the \textit{Katz} test to stored e-mail yields the conclusion that it is reasonable to expect privacy in it. We set aside the subjective inquiry for now because it will necessarily be case- specific, although we think it clear that users, like Warshak, generally have a subjective expectation of privacy in e-mails they store with their ISPs.\textsuperscript{66} As the Court's reasoning in \textit{Katz} demonstrates, the objective inquiry requires normative rather than merely positive analysis.\textsuperscript{67} That is, in assessing whether a target's expectation of privacy is one that society is prepared to rec-

ognize as reasonable, a court must ask what society is \textit{entitled to believe}, even if society might perceive a communications medium to be vulnerable or insecure in some way. \textit{Katz} was decided at a time when the public was well aware of the vulnerability of telephone calls to interception. In the years preceding \textit{Katz}, the public had learned of rampant illegal wiretapping from numerous influential books, scholarly articles, and newspaper accounts.\textsuperscript{68} In the same period, as Congress considered new legislation, it

\begin{footnotesize}
\begin{enumerate}
\item Warshak Law Professors' Brief at *7–8 (cited in note 6).
\item 389 US 347 (1967).
\item Id at 348, 353.
\item Id at 353 ("The Government's activities in electronically listening to and recording petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a, 'search and seizure' within the meaning of the Fourth Amendment.").
\item Id at 361 (Harlan concurring); \textit{Kyllo v United States}, 533 US 27, 32–33 (2001).
\item See Warshak Law Professors' Brief at *4 (cited in note 6).
\item Freiwald, 2007 Stan Tech L Rev 3 at ¶ 28–31 (cited in note 60).
\item Freiwald, 56 Ala L Rev at 38–39 (cited in note 2).
\end{enumerate}
\end{footnotesize}
convened numerous hearings and commissioned lengthy expert reports that detailed communications' vulnerability. The *Katz* Court nevertheless concluded that an expectation of privacy in one's telephone calls was reasonable. The Court based constitutional protection on the overriding importance of the telephone system, noting that "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication." The Court reasoned 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."

A normative analysis of stored e-mail reaches a similar result. First, like the telephone in *Katz*, e-mail plays a vital role in modern communications. A court assessing how e-mail contributes to modern life would likely conclude that its role in enhancing communication is at least as important as the telephone. The overriding importance of the medium should mean that we are entitled to assume that it is private; any other conclusion would be destructive of society's ability to communicate. Second, in functional terms, much e-mail substitutes for or displaces other forms of communication that society clearly views as private. We send e-mails when in the past we might have made telephone calls or had face-to-face conversations. We send e-mails when in the past we might have sent letters. Because we expect privacy in these more traditional forms of communication, we should be entitled to expect privacy in e-mail as well; any other conclusion would distort our incentives to use new communications technologies. Finally, e-mails often contain information of a highly private nature, making e-mail surveillance at least as intrusive as surveillance of other forms of communication. 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 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. We rely on the privacy of the medium to communicate. A normative ap-

---

69 Id at 74–75.
70 *Katz*, 389 US at 352.
71 Id (emphasis added).
proach to the expectation of privacy test ensures that we do not rely at our peril.

There are likely several converging reasons why the courts did not, prior to the Warshak panel, clearly affirm that stored e-mails enjoy the same constitutional protection as telephone calls and written letters. Some of it surely reflects the fact that the targets of such investigations rarely found out that they had been investigated because they were never told.\textsuperscript{72} Even when they were given notice, the lack of a statutory suppression remedy in the SCA as well as the lack of significant damages likely provided little financial incentive to sue.\textsuperscript{73} Many targets who might have found it worthwhile to mount a constitutional challenge likely lacked the resources to do so. That would be particularly true for defendants subject to other types of incriminating evidence, for whom having the stored e-mails excluded from trial would not likely lead to acquittal and for whom it would therefore not be worth incurring substantial cost to obtain such exclusion.

Part of the problem surely stems from courts' practices of relying on the executive branch to parse the SCA due its incredible complexity.\textsuperscript{74} Only recently have magistrate and trial judges begun to push the DOJ to better support its proffered interpreta-

\textsuperscript{72} In the Warshak investigation, for example, the government delayed the statutorily required notice for over a year, apparently without seeking the required judicial approval for an extension of the 90-day delay. See note 39 and accompanying text. See also Freiwald, 56 Ala L Rev at 65 (noting limited notice requirements in the SCA); Susan N. Herman, The USA PATRIOT Act and the Submajoritarian Fourth Amendment, 41 Harv CR-CL L Rev 67, 104 (discussing how "secrecy in many guises, combined with executive branch control of information as well as the venue and timing of litigation about its own actions, have created impediments to any meaningful form of judicial review" with respect to several provisions of the USA PATRIOT Act).

\textsuperscript{73} See note 208 (listing limited civil remedies). See also Freiwald, 56 Ala L Rev at 63–64 (discussing absence of suppression remedy and limited financial incentives to sue). See also Orin S. Kerr, Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Law, 54 Hastings L J 805 (2003) (arguing that a statutory suppression remedy would clarify the SCA by giving courts an opportunity to delineate permissible practices).

\textsuperscript{74} Courts frequently decry the complexity of electronic surveillance statutes. See, for example, Konop v Hawaiian Airlines, Inc, 302 F3d 868, 874 (9th Cir 2002) ("Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results"); Steve Jackson Games, Inc v US Secret Service, 36 F3d 457, 462 (5th Cir 1994) (calling the Wiretap Act "famous (if not infamous) for its lack of clarity"); United States v Smith, 155 F3d 1051, 1055 (9th Cir 1998) (suggesting that the Steve Jackson Games court "might have put the matter too mildly"). See also Patricia L. Bellia, Spyware and the Limits of Surveillance Law, 20 Berkeley Tech L J 1283, 1318–23 (2005) (discussing courts' perceptions of complexity); Daniel J. Solove, Reconstructing Electronic Surveillance Law, 72 Geo Wash L Rev 1264, 1292–93 (2004) (noting "profound complexity").
tions of the SCA and related statutes and, in several cases, courts have found those interpretations lacking.\textsuperscript{75} Finally, and perhaps most importantly, there seemed to be a rough consensus among academics and others that the third party rule would doom any arguments about the constitutional protection of stored e-mail.\textsuperscript{76} Surprisingly, given the length of time that we have been using e-mail extensively, it took until 2007 for a federal appellate court to evaluate the constitutional question itself.

Whatever explains the lack of cases contesting the constitutionality of the government's compelled disclosure of stored e-mails before Warshak, it is essential to recognize that no court has ever found the government's practice to satisfy the Fourth Amendment. There is thus no argument that the absence of case law considering the constitutionality of the government's practices forecloses claims that those practices violate the Fourth Amendment.\textsuperscript{77} Moreover, we agree with the Warshak panel's conclusion that, like telephone calls and written letters, stored e-mails are subject to meaningful Fourth Amendment protection. Except in exceptional circumstances, stored e-mails may not be searched, or compelled to be disclosed, without a warrant based on probable cause or a valid exception to the warrant requirement.\textsuperscript{78}


\textsuperscript{76} See, for example, \textit{DOJ Search Manual} at 94 (cited in note 19); Orin S. Kerr, \textit{The Problem of Perspective in Internet Law}, 91 Georgetown L J 357, 366–67 (2003) (assuming that when one sends an e-mail, one "disclos[es] the communication" to the ISP and describing "black letter rule that the Fourth Amendment permits the government to obtain information disclosed to a third party using a mere subpoena"); Daniel J. Solove, \textit{Digital Dossiers and the Dissipation of Fourth Amendment Privacy}, 75 S Cal L Rev 1083, 1135 (2002) ("Individuals ... probably do not have a reasonable expectation of privacy in communications and records maintained by ISPs or computer network system administrators."). We disagree strongly with that reading of the third party rule, and we explain our disagreement at length in Part III B.

\textsuperscript{77} The government nevertheless made this argument throughout the litigation in Warshak. for example, Brief for Defendant-Appellant United States of America, \textit{Warshak v United States}, No 06-4092, *3 (6th Cir filed Oct 13, 2006), available at <http://w2.eff.org/legal/cases/warshak_v_usa/warshak_final_proof_brief.pdf> (last visited Apr 11, 2008) ("Government Proof Brief") ("Until this case, no court had ever declared § 2703 to be unconstitutional."); id at *14 ("For twenty years, the Stored Communications Act has set forth the procedures that the government must follow to compel disclosure of e-mail, and no court has previously held it to be unconstitutional.").

\textsuperscript{78} In Part IV B, we discuss arguments for why the Fourth Amendment might impose an even higher procedural hurdle.
III. REFUTING THE GOVERNMENT'S ARGUMENTS

In this Part, we address directly the arguments that the government made before the Sixth Circuit panel in Warshak. As noted earlier, the central issue for the Warshak panel was how to apply the Fourth Amendment to government agents' compelled disclosure of communications from a third party service provider. We argue that the precedents not only support the Warshak panel's ultimate conclusion, they provide firmer ground than the panel itself recognized. In addition, the panel could have gone even further in rejecting the government's arguments and in clarifying the circumstances under which an e-mail user retains a reasonable expectation of privacy in stored e-mails.

A. The Compelled Disclosure Argument

Throughout the Warshak litigation, the government argued that agents need only satisfy a "reasonableness" standard when they compel an ISP to divulge its users' e-mails. To be sure, the government based much of its argument that it may proceed in such cases without a warrant on its claim that targets have no reasonable expectation of privacy in e-mail stored with their ISPs. That, in turn, follows from the government's reading of the "third party rule" that we critique in the next section. But the government also argued that, notwithstanding the target's reasonable expectation of privacy, law enforcement agents may satisfy the lesser requirement of reasonableness when they compel disclosure of stored e-mails because that is the standard of review for subpoenas and related court orders under § 2703(d).

As we pointed out in an amicus brief filed in the Sixth Circuit on behalf of professors of electronic privacy law and internet law, it would turn constitutional doctrine on its head if executive branch agents could select a procedure to follow, in this case a subpoena or § 2703(d) court order, and then justify that choice on the grounds that they met the reduced standard associated with that choice. Were the government correct, it could simply write the warrant requirement out of the Fourth Amendment by "compelling" production of evidence rather than searching for it.

79 See, for example, Government Proof Brief at *38–45 (cited in note 77).
80 Id at *45 ("[T]he constitutionality of a third-party subpoena turns on its reasonableness, not on whether the target has a reasonable expectation of privacy in the subpoenaed items.").
81 Warshak Law Professors' Brief at *20–21 (cited in note 6).
Fourth Amendment doctrine itself establishes procedural hurdles for executive branch agents that require judicial branch intervention commensurate with the intrusiveness of investigation and its need for supervision. When the government invades a reasonable expectation of privacy, the Supreme Court has made clear that the propriety of that action must be judged by a neutral magistrate, and not by agents in the field.

While we view it as obvious that executive branch agents may not select for themselves the level of judicial review to which their practices will be subject, as the government's claim would imply, we nonetheless address the government's argument here in greater depth. Ambiguous language in the Warshak panel decision, which suggested that, after notice, a target would be able to raise only reasonableness objections to the government's use of a subpoena or § 2703(d) court order to compel his ISP to disclose his e-mails, further supports the need to clarify what review attends compelled disclosure by subpoena or related court order.

Case law has established that recipients of subpoenas may challenge the compulsion to appear or produce documents on limited bases, namely that compliance with their issuance is either overbroad or unduly burdensome. But that standard gov-

---

82 See Berger, 388 US at 56 (noting that indiscriminate use of eavesdropping devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments, and imposes a heavier responsibility on this Court in its supervision of the fairness of procedures," quoting Osborn v United States, 385 US 329 n 7 (1966)).

83 Katz, 389 US at 356 (1967) (rejecting the argument that the Court should validate officers' conduct because they did no more than they might properly have done with prior judicial sanction; "It is apparent that the agents in this case acted with restraint. Yet the inescapable fact is that this restraint was imposed by the agents themselves, not by a judicial officer.").

84 Consider Doe v Gonzales, 500 F Supp 2d 379, 412 (S D NY 2007) (observing that Congress cannot dictate the degree of deference the judiciary must accord the executive in reviewing a challenged speech restriction).

85 More specifically, the panel stated that government agents need not obtain a warrant "if the government provides notice to the account holder in seeking an SCA order, according him the same judicial review he would be allowed were he to be subpoenaed." Warshak, 490 F3d at 476 (emphasis added). Other language in the opinion suggests that the target can raise broader objections, including that he or she has a reasonable expectation of privacy in the communications. See id at 469 (noting that government's argument "begs the critical question of whether an e-mail user maintains a reasonable expectation of privacy in his e-mails vis-à-vis the party who is subject to compelled disclosure—in this instance, the ISPs" and opining that, if the user does retain an expectation of privacy, "the Fourth Amendment's probable cause standard controls the e-mail seizure"). We discuss this issue at greater length in Part III D 2. See also note 52 (providing district court's language).

86 See, for example, Donovan v Lone Steer, Inc, 464 US 408, 415 (1984) (noting requirements that subpoena "be sufficiently limited in scope, relevant in purpose, and
erns the initial need to appear, and it does not necessarily apply to the investigation of all materials or information the compelled party may have. In cases in which subpoenas have been issued to obtain materials that the targets claimed were subject to a reasonable expectation of privacy, courts, including the Supreme Court, have recognized that reviewing courts must determine whether the precise information sought is indeed subject to a reasonable expectation of privacy.

In other words, courts that address challenges to a subpoena must employ a two-step process. In the first step, courts consider whether compelling the target to come forward by subpoena meets the reasonableness requirement. If so, they proceed to consider the target's claim that the precise information sought is subject to a reasonable expectation of privacy. In discussing the first step, courts have distinguished between compelled disclosure on the one hand and searches or seizures on the other. Because a compelled disclosure is significantly less intrusive than a search or seizure, and because it is subject to judicial oversight when challenged, the Supreme Court has stated that it may be challenged for lack of reasonableness only. For example, in its 1973 decision in United States v Dionisio, the Supreme Court quoted from the Second Circuit case of United States v Doe (Schwartz),88 when it explained:

"The latter [the seizure of a person] is abrupt, is effected with force or the threat of it and often in demeaning circumstances, and, in the case of arrest, results in a record involving social stigma. A subpoena is served in the same manner as other legal process; it involves no stigma whatever; if the time for appearance is inconvenient, this can generally be altered; and it remains at all times under the control and supervision of a court."89

While the Dionisio and Schwartz courts rejected the notion, based on the distinction just given, that government agents have to establish probable cause before using a subpoena to compel the target in each case to appear before the grand jury, they cer-

specific in directive so that compliance will not be unreasonably burdensome"), quoting See v City of Seattle, 387 US 541, 544 (1967). Of course targets may raise Fifth Amendment objections to being compelled to testify, but in this section we focus on Fourth Amendment claims.

88 457 F2d 895 (2d Cir 1972).
89 Dionisio, 410 US at 10, quoting Schwartz, 457 F2d at 898.
tainly did not establish that use of a subpoena obviated the need to consider the target's reasonable expectation of privacy in the actual materials sought. In both cases, the targets claimed that the Fourth Amendment prohibited use of a subpoena to compel them to furnish handwriting and voice exemplars to a grand jury, and in both cases the courts considered, in a second step, whether in fact the targets had a reasonable expectation of privacy in those exemplars.

In Schwartz, the Second Circuit court ultimately held that the target had no expectation of privacy in her handwriting or voice: "[W]hile the content of a communication is entitled to Fourth Amendment protection, the underlying identifying characteristics—the constant factor throughout both public and private communications—are open for all to see or hear." In Dionisio, the Supreme Court came to the same conclusion as the Second Circuit and held that the requirement to make voice recordings did not infringe any expectation of privacy since the Fourth Amendment provides no protection for physical characteristics, such as the sound of one's voice, that an individual knowingly and necessarily exposes to the public. As the Supreme Court said: "[n]o person can have a reasonable expectation of privacy that others will not know the sound of his voice, any more than he can reasonably expect that his face will be a mystery to the world."

Again, in both cases, the Fourth Amendment review of subpoenas involved two distinct questions: (1) did the order that the individuals appear before the grand jury violate the Fourth Amendment; and (2) once the individuals were lawfully before the grand jury, did the further direction to make voice recordings violate the Fourth Amendment. While the answer to the first question was clearly no, the answer to the second turned on an

90 Schwartz, 457 F2d at 898 (citation omitted).
92 Id at 14 (analyzing the giving of voice exemplars according to the decision in Katz, 389 US at 351).
93 Id at 8 ("As the Court made clear in Schmerber [v California], the obtaining of physical evidence from a person involves a potential Fourth Amendment violation at two different levels—the 'seizure' of the 'person' necessary to bring him into contact with government agents and the subsequent search for and seizure of the evidence.") (citation omitted); Dionisio, 410 US at 13–14 ("But the conclusion that Dionisio's compulsory appearance before the grand jury was not an unreasonable 'seizure' is the answer to only the first part of the Fourth Amendment inquiry here. Dionisio argues that the grand jury's subsequent directive to make the voice recording was itself an infringement of his rights under the Fourth Amendment.").
94 Id at 10.
analysis of the reasonable expectation of privacy and was entirely independent of the first.\textsuperscript{95} As the Second Circuit made plain:

\begin{quote}
[T]he fact that compulsory appearance before a grand jury is not a seizure of the person does not lead automatically to the conclusion that nothing the grand jury may require could constitute a search. The test must be whether the requirement invades a ‘reasonable expectation of privacy.’\textsuperscript{96}
\end{quote}

The government’s compelled disclosure argument in the \textit{Warshak} case essentially asked the Sixth Circuit to collapse these two questions into one.\textsuperscript{97} Although it is possible to identify numerous cases in which courts have assessed the compelled production of documents under a reasonableness standard, the cases involve corporate or business records that are not subject to a reasonable expectation of privacy.\textsuperscript{98} The cases therefore do not undermine the \textit{Dionisio} Court's approach of independently assessing the two Fourth Amendment interests in question. Even the case of \textit{United States v Miller},\textsuperscript{99} upon which the government’s \textit{Warshak} argument lays heavy emphasis, is consistent with the approach the Court laid out in \textit{Dionisio}. In \textit{Miller}, the

\begin{flushleft}
\textsuperscript{95} \textit{Dionisio}, 410 US at 13–15.
\textsuperscript{96} Schwartz, 457 F2d at 898 (emphasis added).
\textsuperscript{97} Although some appellate courts have used language that seems to blur the distinction the Court made in \textit{Dionisio}, those cases actually rejected the notion that a subpoena to produce documents, not subject to reasonable expectation of privacy, required a probable cause warrant. See, for example, \textit{In re Bailey (Subpoena Duces Tecum)}, 228 F3d 341, 348 (4th Cir 2000) (noting that if the “assertion that investigative subpoenas may be issued only upon probable cause” were correct, the result would be a paradox where “the object of many such investigations—to determine whether probable cause exists to prosecute such a violation—would become a condition precedent for undertaking the investigation.”). See also \textit{Doe v United States}, 253 F3d 256, 264 (6th Cir 2001) (quoting Bailey, 228 F3d at 348).
\textsuperscript{98} See \textit{Donovan}, 464 US at 415 (sustaining enforcement of a subpoena of restaurant-motel’s payroll and sales records and emphasizing that “[i]t is now settled that, when an administrative agency subpoenas corporate books or records, the Fourth Amendment requires” only reasonableness), quoting \textit{See v City of Seattle}, 387 US at 544 (emphasis added); \textit{SEC v Jerry T. O’Brien, Inc}, 467 US 735, 743 (1984) (rejecting a Fourth Amendment challenge to officials’ failure to provide notice of a third-party subpoena to the target of an investigation, when the subpoena sought financial records in the hands of firms with whom target had engaged in transactions); \textit{Fisher v United States}, 425 US 391, 401 n 7 (1976) (noting the absence of arguments of a Fourth Amendment nature in a case involving the subpoena of accountants’ records from taxpayers’ attorneys, and observing that “[s]pecial problems of privacy which might be presented by subpoena of a personal diary are not involved here”).
\end{flushleft}
Supreme Court assessed whether a subpoena compelling a bank to disclose its customer's financial records violated the Fourth Amendment. 100 Miller, the target of the investigation, claimed a reasonable expectation of privacy in the records. 101 Although it rejected Miller's argument, the Supreme Court never suggested that mere use of a subpoena defeated the need to inquire into Miller's expectation of privacy or converted the applicable standard to one of reasonableness. The Court concluded that a reasonableness standard applied to the compelled disclosure of Miller's records not because use of a subpoena, without more, overcomes a target's expectation of privacy, but because the sorts of records at issue in Miller—"business records," in the Court's terminology 102—involves no expectation of privacy. 103 If the Fourth Amendment required only reasonableness in compelled disclosure cases, the Miller Court could have sustained the government's conduct without ever inquiring into whether Miller had a reasonable expectation of privacy.

Despite the fallacy of the government's compelled disclosure argument, the Warshak panel, relying on broad dictum from a prior Sixth Circuit case, 104 began its analysis by stating that, in

100 The subpoenas required the banks to produce, for specified time periods, "all records of accounts" in Miller's name. The banks showed agents microfilm records of Miller's accounts and gave agents copies of checks, deposit slips, financial statements, and monthly statements. Id at 437-38.

101 Id at 442.

102 The Court's focus on business records is evident from its quotation of language from Oklahoma Press Publishing Co v Walling, 327 US 186 (1946). The Miller Court quoted that case's observation that "the Fourth [Amendment], if applicable [to subpoenas for the production of business records and papers], at the most guards against abuse only by way of too much indefiniteness or breadth in the things required to be 'particularly described,' if also the inquiry is one the demanding agency is authorized by law to make and the materials specified are relevant." Miller, 425 US at 445-46, quoting Oklahoma Press Publishing, 327 US at 208. The bracketed language is that of the Miller Court, and its narrow characterization of Oklahoma Press Publishing is accurate. The Oklahoma Press Publishing Court distilled case law that dealt "merely" with "production of corporate records and papers in response to a subpoena." Oklahoma Press Publishing, 327 US at 208 (emphasis added).

103 The Miller Court did not in fact apply the reasonableness standard because the banks upon which the subpoenas were served did not contest their validity. Miller, 425 US at 446 n 9. The Court nevertheless implied that the reasonableness standard was the appropriate one. Id at 446.

104 Doe v United States, 253 F3d at 263-64. In Doe, a doctor who was under investigation for health care fraud moved to quash an administrative subpoena issued under the Health Insurance Portability and Accountability Act ("HIPAA"). The court applied a reasonableness standard to the question of disclosure of Doe's records. The court's observation that "whereas the Fourth Amendment mandates a showing of probable cause for issuance of search warrants, subpoenas are analyzed only under the Fourth Amendment's general reasonableness standard" was dictum because the target raised no claim on appeal that a probable cause standard should apply. Id.
FOURTH AMENDMENT PROTECTION FOR STORED E-MAIL

general, subpoenas are tested only under the Fourth Amendment's general reasonableness standard. The panel then invoked a "Fourth Amendment caveat" to this rule when it stated that a target who can demonstrate that he has a reasonable expectation of privacy in the records sought by subpoena can dispute that subpoena's issuance on Fourth Amendment grounds. Whether stated as a caveat or as a second step, the reasonable expectation of privacy analysis is crucial to evaluating the Fourth Amendment regulation of compelled access to stored e-mails. Because that analysis in turn requires consideration of the third party argument, we discuss that argument next. As we will argue, and as the Warshak panel properly recognized, the government's broad reading of the third party rule seeks to extend precedents well beyond their holdings.

B. The Third Party Argument

In addition to its argument that all compelled disclosures merit only reasonableness review, the government has also argued that users lack any expectation of privacy in those stored e-mails that reside on their ISPs' servers. Under the government's logic, a subscriber reveals e-mail communications to her ISP merely by allowing the ISP to store them and she thereby assumes the risk that the ISP might choose or even be compelled to disclose those records to the government.

The government's argument relies on an overbroad reading of the Supreme Court's decision in the Miller case just discussed. The government derives from Miller's language a third party rule that posits that a user forfeits any expectation of privacy in information that may be obtained from a third party. The following quote contains the pertinent language from Miller:

The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be

105 Warshak, 490 F3d at 468–69.
106 See Government Proof Brief at *38 (cited in note 77) (arguing that “the government may compel a third party to disclose anything that the third party can access”).
used only for a limited purpose and the confidence placed in the third party will not be betrayed.  

Although courts could view this language as inviting the government’s broad third party rule, they should decline the invitation for several reasons. First, Miller falls into a line of cases concerning “business records” and “corporate records” before them. Stored e-mails look nothing like business or corporate records, but rather entail private communications. Although Miller may push the scope of the “business records” category to its limits, nothing in Miller suggests that the category is all-encompassing—that one lacks an expectation of privacy in anything in the hands of a third party. Moreover, by their nature, storage lockers and letters and packages in the hands of third parties are much more analogous to e-mails stored with ISPs than are the business records at issue in Miller.  

Second, reading Miller’s “assumption of risk” approach broadly creates undue tension with Katz. Even the narrower reading of it meshes poorly with the actual facts of Miller and fits the stored e-mail context even worse. In Miller, the Court viewed bank customers as having made the voluntary choice to reveal their documents to the banks when they could not easily function in modern society without a bank account. It is odd to view a bank customer’s use of a bank as analogous to misplacing trust in a confidant, as the Court did in using the assumption of risk approach in Miller. Because the assumption of risk analysis in Miller was such a stretch, there is no reason to extend it further to apply in the context of stored e-mails. That is especially so because those in analogous relationships that better match users’ relationships with their ISPs do not assume the risk of warrantless compelled disclosure.  

In Part III C, we will address whether the ISP’s relationship with its customer amounts to a constitutional privacy waiver.  

107 Miller, 425 US at 443 (emphasis added).  
108 See Part II.  
109 See Miller, 425 US at 451 (1976) (Brennan dissenting) (stating that “the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account”), quoting Burrows v Superior Court, 529 P2d 590, 596 (Cal 1975); Wayne LaFave et al, Criminal Procedure § 3.2(j) (Thomson 4th ed 2004). See also Smith v Maryland, 442 US 735, 750 (1979) (Marshall dissenting) ("[U]nless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance.").  
110 See Bellia, 72 Geo Wash L Rev at 1402 (cited in note 20).
But as an initial matter, courts should reject the idea that those whose e-mails may be accessed by their ISPs have assumed the risk that the government will access those e-mails without a warrant. Even if a bank customer were to assume the risk her bank will voluntarily disclose her documents, which, again, are not her communications, that does not mean that she assumes the different risk that the government will compel the bank to disclose those documents without first obtaining a warrant.

As for the third party argument, it should be clear that courts must chart new ground to determine the constitutional status of stored e-mail. Subpoena law, which has addressed business records in the hands of third parties, has not yet addressed a fundamentally new phenomenon: storage by third parties of another's private communications. Though it might seem an easy way to resolve the question, to use a broad third party rule from Miller is to read much more into the case than it deserves and to misapprehend the nature of stored e-mail.

1. Stored e-mails are neither "corporate" nor "business" records.

The Supreme Court and lower courts have historically treated business and corporate records as less deserving of privacy than confidential communications, and the latter is what one finds in stored e-mail. For example, the Miller Court began its Fourth Amendment analysis by observing that "[w]e must examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents." The Court then clearly indicated that the documents at issue did not constitute confidential communications, for which, impliedly, a different analysis would be appropriate. As the Court discussed:

Even if we direct our attention to the original checks and deposit slips, rather than to the microfilm copies actually viewed and obtained by means of the subpoena, we perceive no legitimate 'expectation of privacy' in their contents. The checks are not confidential communications but


112 Whether some stored e-mail may more properly be considered as a record of a transaction and therefore not a private communication is an important issue that is beyond the scope of this Article.

113 425 US at 442 (emphasis added).
negotiable instruments to be used in commercial transac-

tions.114

The Court's distinction between "confidential communica-
tions" on the one hand and "negotiable instruments" used in
"commercial transactions" on the other reflects precedent cases
in which the Court withheld robust Fourth Amendment protec-
tion from the compelled disclosure of corporate records.

Starting in the 1906 case of Hale v Henkel,115 the Court held
that neither the Fourth Amendment nor the Fifth Amendment
barred the government's access to corporate records.116 The
Court distinguished between the rights of the corporation, as "a
creature of the state," and the rights of a citizen, who "owes no
duty to the State . . . to divulge his business" and who has "im-

munity . . . from arrest or seizure except under a warrant of the
law."117 Similarly, in Oklahoma Press Publishing Co v Walling,
when the government targeted a corporation and sought its re-
cords, the Court analogized the federal government's investiga-
tive powers over corporations to the "visitorial" power of the in-
corporating state.118

The Court in Oklahoma Press distilled prior case law as fol-
lows: "[I]n so far as [earlier cases] apply merely to the produc-
tion of corporate records and papers in response to a subpoena or or-
der authorized by law and safeguarded by judicial sanction," those cases establish that "the Fourth [Amendment], if applica-
ble, at the most guards against abuse only by way of too much
indefiniteness or breadth . . . if also the inquiry is one the de-
manding agency is authorized by law to make and the materials
specified are relevant."119 In subsequent cases involving subpoe-
nas to compel production of a corporation's records, the Court
continued to distinguish between corporate records and private

114 Id.
115 201 US 43 (1906), overruled in part, Murphy v Waterfront Commissioner of NY

116 The Court thus repudiated the prior case of Boyd v United States, 116 US 616
(1886), in which the Court had held that the Fourth Amendment (and the Fifth) barred
the government from compelling the owners of goods to produce relevant invoices. Id at
638.
117 Hale, 201 US at 74.
118 327 US at 204.
119 Id at 208 (emphasis added). The Court explained that Congress can authorize
access to corporate records by administrative subpoena in part because, when a corpora-
tion's activities affect interstate commerce, Congress possesses a wide investigative

power over it, "analogous to the visitorial power of the incorporating state." Id at 204 &
nn 31–32.
documents, suggesting that the latter were immune from compulsory process.\footnote{Christopher Slobogin, Subpoenas and Privacy, 54 DePaul L Rev 805, 816–17 (2005); Bellia, 72 Geo Wash L Rev at 1397–99 (cited in note 20); 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).}

After Katz, courts continued to deny Fourth Amendment claims regarding records kept by businesses, but they did so by finding no expectation of privacy in those records. For example, in Couch v United States,\footnote{409 US 322 (1973).} the Supreme Court rejected a taxpayer's Fourth Amendment objection to enforcement of a summons requiring her accountant to produce records that Couch had provided for use in her tax returns.\footnote{Id at 323–24, 325 n 6. The Court also rejected a Fifth Amendment claim. Id at 325, 331. We return to a discussion to the relevance of Fifth Amendment doctrine in these cases in Part III B 3.} When the accountant refused to produce the records and the IRS sought judicial enforcement of the summons, Couch intervened to assert that her Fifth Amendment privilege against self-incrimination barred the government from compelling the accountant to produce the records.\footnote{Id at 325, 331.} The Court addressed the Fourth Amendment claim only briefly, due to the dominance of Fifth Amendment issues, but concluded nonetheless that "the necessary expectation of privacy" under Katz "to launch a valid Fourth Amendment claim does not exist."\footnote{Couch, 409 US at 336 n 19.} The Court reasoned that "there can be little expectation of privacy where records are handed to an accountant, knowing that mandatory disclosure of much of the information therein is required in an income tax return."\footnote{Id at 335.}

Couch became the foundation for a series of cases involving records turned over to third parties for the third parties to perform particular tasks with such records—with all of the cases rejecting claims that an individual can retain an expectation of privacy in the records. Miller and Couch thus expanded the category of records subject to warrantless compelled disclosure beyond records about the corporation. The documents sought in Miller and Couch concerned the bank depositor and the taxpayer whose records were stored with the targets of the subpoenas, while in the prior cases the corporation was the target of the investigation and received the subpoena. However, even in Miller, the Court's focus on the character of the records at issue was
unmistakable: they were "not confidential communications"; they were records "exposed ... in the ordinary course of business" or "business records of the banks." "

To justify using the Miller case to resolve the stored-records question, then, a court must regard stored e-mails as close enough to the bank's business records at issue in Miller as to warrant the same treatment. We have already made the most crucial argument opposed to that conclusion: stored e-mails are more properly considered confidential communications than the records of a business. In light of that, limiting the judicial oversight attendant to the disclosure of stored e-mails raises concerns not only under the Fourth Amendment but also the First Amendment. We return to the special nature of stored e-mails as records of communications rather than the non-communications records of a business in Part III C.

Meanwhile, another reason not to analogize stored e-mails to business records is that there are much better analogies. In particular, analogies to a third party's carriage or storage of physical property better capture the role a third party ISP plays when it stores e-mail.

Cases involving a third party's carriage or storage of physical property clearly provide that the government must obtain a warrant before investigating the items it seeks. 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." The same general rule applies to luggage carried by private transportation compa-

126 Miller, 425 US at 442 (emphasis added).
127 Id at 440, 442.
128 See Daniel J. Solove, The First Amendment as Criminal Procedure, 82 NYU L Rev 112 (2007); Mulligan, 72 Geo Wash L Rev at 1587 (cited in note 120). See also In re United States, 534 F Supp 2d 585, 612 (W D Penn 2008) (discussing the "associational interests implicated" by government access to stored electronic records disclosing cell-phone users' movements); id at 591 n 21 (noting the link between Fourth Amendment protection and First Amendment associational interests and citing Katz). We will address further where to draw the line between an ISP's business records and stored e-mails in Part III C.
129 One exception is the case of United States v Palmer, 536 F2d 1278 (9th Cir 1976), which the government cited in its Warshak brief. See Government Proof Brief at *45 (cited in note 77). For an argument distinguishing Palmer, see Bellia, 72 Geo Wash L Rev at 1410–11 (cited in note 20).
130 Jacobsen, 466 US at 114. See also Ex parte Jackson, 96 US 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.").
nies. Similarly, when someone maintains personal property on a third party’s premises, she retains an expectation of privacy in the property, even though the third party may have the right to access the premises for some purposes. While third parties in such cases may retain extensive rights of access to the property under both contract and common law in order to provide their service or protect their property, the property carried, transported, or stored has never been treated as were the business records in Miller. Moreover, and as we next address, the notion that the property owner “assumes the risk” that government agents will compel the third party to turn the property over is entirely absent from case law dealing with personal property.

2. Assumption of risk.

As the broad language from the Miller case illustrates, the Supreme Court combined both the corporate records cases and the assumption of risk cases to decide Miller. One of us has argued elsewhere that the Supreme Court could have decided the Miller case without getting into the “assumption of risk” analysis. But it did rely on the customer’s assumption of risk, and the government has made that an integral part of its broad third party rule, under which e-mail users assume the risk that their ISPs will disclose their stored e-mails merely by virtue of the government’s ability to obtain the stored e-mails from the ISPs.

a) Conflicts with Katz. The strongest version of the assumption of risk argument is that a third party’s technical ability to gain access to communications, without more, eliminates a user’s

---

131 See Bond v United States, 529 US 334, 338–39 (2000) (holding that petitioner bus passenger had a reasonable expectation of privacy in his carry-on bag and that agent’s warrantless physical manipulation of the bag violated petitioner’s reasonable expectation of privacy).

132 See, for example, Stoner v California, 376 US 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 US 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 F2d 1131, 1133–35 (9th Cir 1988) (implicitly recognizing reasonable expectation of privacy in rented storage unit). But see cases discussed in note 184 (describing how benefits of third party relationship persist only while the relationship itself persists and has not been substantially violated by the first party).

133 Bellia, 72 Geo Wash L Rev at 1397–1402 (cited in note 20). See also Miller, 425 US at 442 (finding that “the lack of any legitimate expectation of privacy concerning the information kept in bank records was assumed by Congress in enacting the Bank Secrecy Act, the expressed purpose of which is to require records to be maintained because they have a high degree of usefulness in criminal tax, and regulatory investigations and proceedings”) (citation omitted).
reasonable expectation of privacy in them. *Katz* itself forecloses that argument. *Katz* involved communications carried over a telephone line by a communications carrier that had the technical ability to monitor the communications, and yet the Court concluded that agents' use of a listening device to overhear the target's end of a conversation invaded the target's privacy.\(^{134}\)

The only way to reconcile *Miller* with *Katz*—which *Miller* purport to apply rather than to overrule—is to recognize that communications are not "revealed" to a third party merely because that third party has the technical ability to gain access to them.\(^{135}\)

\(b\) Assumption of what risk? In *Miller*, the Supreme Court never claimed that mere accessibility of Miller's records to the bank precluded Miller's reasonable expectation of privacy claim. Instead, the Court reasoned that Miller's disclosure of his bank records to the bank precluded him from raising that claim. As the Court noted:

\[\text{the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.}\]\(^{136}\)

What may not be entirely clear from the above quote is that *Miller*'s reliance on the assumption of risk cases implied three findings about Miller that the facts of the case do not support. Those are: 1) that Miller had voluntarily revealed his banking information to the bank, 2) that the bank was therefore a party to his communications, and 3) that when one assumes the risk that a party to one's communication will voluntarily reveal the communication to the government, one also assumes the risk that the government will *compel* that party to disclose the communication. As we next discuss, those findings are difficult to support in the context of bank records and make even less sense when applied to the context of stored e-mails.

In the precedent cases from which the *Miller* Court drew, the Supreme Court had held that the Fourth Amendment does

---

\(^{134}\) *Katz*, 389 US at 353.

\(^{135}\) See Freiwald, 2007 Stan Tech L Rev 3 (cited in note 60) (rejecting argument that "fact-of-interceptibility" determines constitutional privacy).

\(^{136}\) *Miller*, 425 US at 443.
not preclude a government informant from testifying about a conversation to which he was a party. In *Hoffa v United States*, the Court denied a defendant's motion to suppress the testimony of a witness who had been present for several conversations in which the defendant had made incriminating statements. The Court held that "no interest legitimately protected by the Fourth Amendment is involved" because the Fourth Amendment does not protect "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."  

After *Katz*, the Supreme Court made clear that its assumption of risk analysis had survived that decision. In *United States v White*, for example, the Court approved the warrantless use of an electronic listening device by a government informant. A plurality of the *White* Court distinguished *Katz* as follows:

*Katz* involved no revelation to the Government by a party to conversations with the defendant nor did the Court indicate in any way that a defendant has a justifiable and constitutionally protected expectation that a person with whom he is conversing will not then or later reveal the conversation to the police.

The *Miller* Court tackled assumption-of-risk analysis onto its application of subpoena doctrine. In doing so, the Court implied that the bank with whom Miller transacted could be analogized to the parties to communications in the precedent cases. In developing that point, the Supreme Court focused on the fact that Miller had voluntarily transacted with the bank, and that

---

138 Id at 294–95.
139 Id at 302. See also *Lopez v United States*, 373 US 427, 437–38 (1963) (holding that evidence derived from conversation surreptitiously recorded by a government agent was admissible, even though government had not sought prior judicial authorization for use of the recording device); *Osborn*, 385 US at 327 (finding tape recording made by government informant admissible on the ground that "[w]e . . . deal here not with surreptitious surveillance of a private conversation by an outsider, but . . . with the use by one party of a device to make an accurate record of a conversation about which that party later testified") (citation omitted).
140 401 US 745 (1971) (plurality opinion).
141 Id at 746–47.
142 Id at 749. See also *United States v Caceres*, 440 US 741, 750–52 (1979) (following *White*).
143 The Court never suggested, however, that assumption-of-risk analysis determines what constitutes a business record or that assumption-of-risk analysis governs all interactions with third parties.
the records produced thereby were the bank's records, used by it in the ordinary course of its business.

Scholars and jurists have questioned whether Miller should be seen to have "voluntarily" disclosed his records to the bank.\textsuperscript{144} If one is to "assume" a risk, then certainly there must be a moment in time when one makes a choice to take that risk and thereby to forgo a less risky choice. Yet, one could not conduct banking without creating records, and one could not easily engage in modern society without banking.\textsuperscript{145} Whether or not the Supreme Court got it wrong in \textit{Miller}, it would stretch \textit{Hoffa}, \textit{White}, and similar precedents beyond all recognition to consider that an e-mail user voluntarily discloses her e-mails and related records to her ISP, and thereby assumes the risk of disclosure to the government.

Two obvious exceptions present themselves. First, if the ISP is itself a party to the e-mail, for example when it is the actual addressee of that e-mail, then it should be considered a party to the communication. In that case, just as one party to a conversation assumes the risk that the other party will reveal that communication, an e-mail user should not be able to raise a Fourth Amendment complaint about the ISP's voluntary disclosures of those e-mails sent to it. Second, to the extent that the ISP is disclosing records of its own business and to the extent that those records do not concern the customer's own communications, disclosure will not implicate the customer's reasonable expectations of privacy.\textsuperscript{146}

For an ISP to reveal to the government those e-mails to which it is not a party would go well beyond \textit{Miller} and completely out of range of the original assumption-of-risk cases. We take up the issue of what these parameters mean in the specific context of an ISP-user relationship in the next part. For now, suffice it to say that the precedents, including \textit{Miller}, do not support a finding that users assume the risk of disclosure by their ISPs, unless the ISP itself was an actual party to the communications disclosed.

\textsuperscript{144} See, for example, Mulligan, 72 Geo Wash L Rev at 1580 n 179 (cited in note 120).

\textsuperscript{145} See sources cited in note 109. See also Freiwald, 2007 Stan Tech L Rev 3 at ¶ 41 (cited in note 60).

\textsuperscript{146} We take up the line between communication records and non-communication records in Part III C.
3. A clean slate.

We have just argued that *Miller* does not directly apply to the case of stored e-mail and that there is good reason not to extend it to do so. One could argue that the business records cases have trended towards a rule that deprives stored e-mail of the protections of the warrant requirement. While we recognize that argument has some support in the cases, although mostly in dicta, we argue that the business records cases should not be extended to e-mail stored on an ISP. The absence of precedent establishing robust Fourth Amendment protection for information in the hands of third parties may be attributed to several facts that have no bearing on resolution of the constitutional question.

First, the Fourth Amendment aspects of subpoenas were long underdeveloped in part because, until the latter part of the 20th century, the Fifth Amendment provided fairly robust protection in the case of first-party subpoenas. Because the Supreme Court viewed the compelled production of private documents from a person to implicate the privilege against self-incrimination, broad Fourth Amendment protection was unnecessary. Robust Fifth Amendment protection survived until the case of *Fisher v United States* in 1976.

Second, although it is true that the application of Fourth Amendment and Fifth Amendment doctrine to third party subpoenas never created a sphere of privacy matching that which

---

147 See Slobogin, 54 DePaul L Rev (cited in note 120) (tracing evolution of Fourth Amendment and Fifth Amendment doctrine in subpoena law).

148 Nevertheless, in cases dealing with corporate records, the Supreme Court consistently distinguished between corporate records and private documents, suggesting that the latter were immune from compulsory process. See sources cited in note 120.

149 425 US 391 (1976). In *Fisher*, the Court evaluated Fifth Amendment challenges to the IRS's use of summonses demanding that taxpayers' attorneys produce documents prepared by the taxpayers' accountants. Because of the attorney-client privilege, the Court analyzed whether the privilege against self-incrimination would have protected the documents in the taxpayers' hands. Id at 403–05. Rather than inquiring whether the records in question were private records—the analysis that prior subpoena cases contemplated—the Court considered whether the contents of the documents had been created with government compulsion. The Court reasoned that because a subpoena itself does not force the creation of the documents the government seeks, any self-incrimination that occurs by virtue of the documents' disclosure is not "compelled." The Court acknowledged that the act of producing documents in response to the subpoena may itself sometimes result in compulsory testimonial incrimination. Id at 410. The Court thus shifted the focus of the Fifth amendment away from the *nature of the documents* to the *act of production*. See Slobogin, 54 DePaul L Rev 805 at 821–22 (cited in note 120) (discussing subsequent cases); Robert P. Mosteller, *Simplifying Subpoena Law: Taking the Fifth Amendment Seriously*, 73 Va L Rev 1, 6–11 (1987) (describing the *Fisher* act-of-production framework).
applied until the latter part of the twentieth century to first-party subpoenas,\textsuperscript{150} that fact is less relevant than it seems. Before\textit{Katz}, a property concept of the Fourth Amendment prevailed, under which Fourth Amendment protection of documents held by a third party (and in which the third party had a property interest) was highly unlikely. Since\textit{Katz}, that property-based conception no longer controls, and courts have recognized that privacy interests exist independently of property interests.\textsuperscript{151}

Finally, both before the Court's decision in\textit{Katz} in 1967 and between that decision and the Court's decision in\textit{Fisher} in 1976, the absence of Fourth Amendment protection mattered the most—indeed, perhaps mattered only—in cases involving third parties. But cases involving third parties were comparatively few in this time period, no doubt because there were far fewer third party record holders during that time period than there are now.\textsuperscript{152} As other scholars have recognized, the breadth of third party doctrine becomes increasingly problematic as the quantity of third party records vastly expands.\textsuperscript{153} One reason that courts should not sanction the government's attempt to export subpoena law to stored e-mail is that the dramatic increase in e-mail storage capacity similarly creates scenarios that the authors of the subpoena precedents never anticipated.\textsuperscript{154} Instead, as we next argue, courts should recognize that stored e-mail and its related attributes should be protected by a warrant requirement in the vast majority of cases.

C. Internet Service Providers and Reasonable Expectations of Privacy

The government claims that even if compelled disclosure of information in the hands of third parties could sometimes impli-

\textsuperscript{150} Outside of the attorney-client privilege context, the Court has recognized that the Fifth Amendment does not prohibit use of a subpoena to compel a third party to produce documents that are later used against the target. See, for example,\textit{Johnson v United States}, 228 US 457, 458 (1913) ("A party is privileged from producing evidence but not from its production.").

\textsuperscript{151} See\textit{Katz}, 389 US at 351 (rejecting argument that the Fourth Amendment applies only in "constitutionally protected areas"; concluding that "the Fourth Amendment protects people, not places").

\textsuperscript{152} Daniel J. Solove,\textit{ The Digital Person} 13–21 (NYU 2004) (providing history of development of public-sector and private-sector databases); Mulligan, 72 Geo Wash L Rev at 1585 (cited in note 120).

\textsuperscript{153} See Christopher Slobogin,\textit{ Transaction Surveillance by the Government}, 75 Miss L J 139, 167–69 (2005); Solove,\textit{ The Digital Person} at 201–02, 207–08 (cited in note 152).

\textsuperscript{154} See Bellia, 75 U Chi L Rev 137 (cited in note 20).
cate the warrant requirement, the typical subscriber-ISP relationship defeats any expectation of privacy that otherwise might exist in stored electronic communications. When the government focuses on the ISP's technical ability to access the contents of communications or the ISP's reservation of the right to accede to lawful access, its claims clearly conflict with established Fourth Amendment law. Arguments concerning the ISP's reservation of a right to access the contents of users' communications for various reasons and its actual screening of the contents of e-mail for viruses, spam, and child pornography merit more discussion. But as we argue next, neither precedents nor the principles of the Fourth Amendment support the breadth of the government's claim that when a user accedes to an ISP relationship with these parameters, she forfeits any claim to an expectation of privacy in her stored communications.

1. Evaluating the government's claims.

a) Technical ability to access communications. As we discussed earlier, the ISP's mere technical ability to access the contents of communications cannot affect the customer's expectation of privacy. If it did, Katz would have been wrongly decided, for the telephone company had the technical ability to access the contents of the communications at issue in that case. Similarly, the U.S. Postal Service or a common carrier has the technical ability to gain access to the contents of a sealed letter or package, and courts have never held that that fact alone eliminates the customer's expectation of privacy. Courts have always required something more.

b) Reserved rights to comply with legal process. We can also set aside another of the government's claims: that a service pro-

---

155 Government Proof Brief at *34 (cited in note 77). The government's argument may be even broader than the claim that ISPs reserve the right to access the contents of communications—that service providers have an unfettered right to access the contents of all stored communications on their computer systems, regardless of the terms of service. See id at *47–48. The government bases this conclusion on the fact that the SCA exempts a service provider from the SCA's prohibition on unlawful access to communications services. Here, the government confuses immunity from statutory liability for unauthorized access under a single statute, the SCA, with blanket immunity for unauthorized access under any other possible state or federal cause of action, such as a state breach of contract claim for access inconsistent with the terms of the service agreement. The SCA simply lacks this broad preemptive effect.

156 Id at *49 ("[I]n practice, service providers routinely screen the content of their users' e-mail. In particular, they check the content of stored e-mail for viruses, spam, and, increasingly, child pornography.").

157 See note 130 and accompanying text.
vider's statement in its terms of service that the provider will comply with legal process itself eliminates the user's Fourth Amendment claim. E-mail users must be entitled to presume that agents will present appropriate legal process to obtain stored e-mails, not that they will present inadequate legal process. What process is appropriate of course depends on what the Fourth Amendment requires and was the very matter in dispute in *Warshak*. That question, which is one of constitutional law and not contract law, must be answered independently of the provider's commitment to cooperate with the government. Otherwise the government could extinguish an expectation of privacy simply by choosing to use a form of legal process that is unavailable when an expectation of privacy exists. Moreover, it would be anomalous to view the ISP customer as having reason to expect that its ISP will flout the law, let alone assuming the risk of that. Certainly courts should, as a normative matter, credit e-mails users' reasonable expectations that their service providers will respect constitutional rights.

c) Other reserved rights of access and actual screening practices. The ISP's reservation of a right to access the contents of users' communications and actual ISP practices present more complicated questions. Recall *Miller's* language that one who "reveals" information to a third party loses any expectation of privacy in it. Does a subscriber "reveal" her communications to an ISP by agreeing to circumstances under which an ISP can access the contents of the communications? Does she "reveal" her communications if the ISP actually screens their contents?

In arguing that the answers to these last two questions are both "yes," the government again stretches precedents well beyond their reach. Without clear precedents, the question becomes one of constitutional interpretation. We argue that Fourth Amendment principles require a much narrower view of the cir-

---

158 See Government Proof Brief at *34–35 (cited in note 77) ("[B]ecause [a customer] consents to Yahoo! disclosing her e-mail in response to legal process, compelled disclosure of e-mail from a Yahoo! account does not violate the Fourth Amendment.").

159 Relatedly, customers of AT&T have brought a class action against the telecommunications giant for disclosing both telephone calls and e-mails to the National Security Administration in violation of both statutory and constitutional law. See *Hepting v AT&T*, 439 F Supp 2d 974 (N D Cal 2006).

160 Freiwald, 2007 Stan Tech L Rev 3 at ¶¶ 29–34 (cited in note 60) (arguing that courts must make a normative judgment about what kind of society we want to live in and how executive branch surveillance practices fit in). See also *White*, 401 US at 786 (Harlan dissenting) ("Our expectations, and the risks we assume, are in large part reflections of laws that translate into rules the customs and values of the past and present.").
cumstances under which a user waives a reasonable expectation of privacy, and a more analytically precise consideration of the consequences of such waivers.

As we have discussed throughout, a key question concerns how to analogize stored e-mails. Under the least protective approach urged by the government, one could view them as analogous to the banking records at issue in *Miller*, and as to which the Supreme Court found no reasonable expectation of privacy. As we argued above, however, the *Miller* court considered only such documents as checks, deposit slips, and account statements as the records of the bank.161 As the *Warshak* panel recognized, some information that ISPs retain about their users, for example subscriber information, may fit comfortably within the rubric of the *Miller* decision.162 As to that information, and because the ISP has an independent business interest in it, the customer does not likely have a reasonable expectation of privacy.163 If the ISP chose to turn over that information to the government, or even were compelled to do so, then the e-mail user would not likely have a claim. Knowledge that records a business keeps of its operations may be subject to subpoena is likely widespread enough that a court should not recognize as reasonable an ISP customer's claim that it expected such records to be protected by the warrant requirement.

A crucial question remains: what counts as a record of the ISP's business and what does not? At the time it drafted the ECPA in 1986, Congress did not fully consider this issue. Congress determined that communications stored for more than 180 days could be obtained without a warrant, but it is unclear whether that conclusion rested on the view that such communications were abandoned or on a view that the communications constituted records of the provider's business. During the hearings on ECPA, the DOJ argued that communications left on the

---

161 See Part III B.
162 See *Warshak*, 490 F3d at 471 ("Compelled disclosure of subscriber information and related records through the ISP might not undermine the e-mail subscriber's Fourth Amendment interest . . . [because] subscriber information and related records are records of the service provider as well, and may likely be accessed by ISP employees in the normal course of their employment.").
163 See, for example, *Guest v Leis*, 255 F3d 325, 335–36 (6th Cir 2001) (internet bulletin board users lost reasonable expectation of privacy in subscriber information including subscribers' names, addresses, birthdates, and passwords communicated to bulletin board system operator); *United States v Kennedy*, 81 F Supp 2d 1103, 1110 (D Kan 2000) (rejecting a privacy interest in subscriber information submitted to ISP); *United States v Hambrick*, 55 F Supp 2d 504, 508–09 (W D Va 1999) (defendant destroyed privacy interest in subscriber information by conveying it to ISP).
provider's system for more than 180 days should not be subject to a warrant requirement, and the House Report accompanying ECPA acknowledged that a communication kept beyond 180 days "is closer to a regular business record maintained by a third party and, therefore, deserving of a lesser standard of protection." The report recognized, however, that providers typically did not retain messages for longer than a few months and that warrant-level protection in fact applied to a communication long past the time a subscriber could reasonably expect to retrieve it from a provider. There is no evidence that Congress recognized that communications would eventually be stored for more than 180 days as a matter of routine. Similarly, Congress's determination that remotely stored files could be obtained without a warrant apparently rested in part on the view that such files would constitute business records of the entities engaging the provider's services, not records of the provider's business.

In other words, although the SCA treats electronic communications stored more than 180 days, or files stored on behalf of an entity that outsources processing and storage tasks, as more like the business records at issue in Miller than like the contents of safe deposit boxes, that treatment does not reflect a congressional determination that the communications or files themselves become the records of the provider's business. Even if it did, more than twenty years later, and with modern practices, including some web-based systems that encourage users to retain their e-mails forever, that view should no longer hold.

165 Id ("Most—if not all—electronic communications systems (such as electronic mail systems), however, only keep copies of messages for a few months. To the extent that the record is kept beyond that point it is closer to a regular business record maintained by a third party and, therefore, deserving of a different standard of protection.").
166 See Mulligan, 72 Geo Wash L Rev at 1572–76 (cited in note 120).
168 See Freiwald, 56 Ala L Rev at 49–50 (cited in note 2) (reviewing the legislative history).
169 See, for example, Gmail Help Center, Should I archive or delete?, available at <http://mail.google.com/support/bin/answer.py?answer=32608&topic=13286> (last visited Apr 11, 2008) (informing Gmail service users that they may keep their e-mails indefinitely and recommending that users do so by archiving their messages).
In our view, the records of an ISP should include only static information about a user that does not vary as communications contents and associated attributes do. When the government acquires subscriber information, for example, it does not obtain information that covers a period of time, and therefore it engages in investigative activity that is more like requesting the ISP's paper records of its business than conducting electronic surveillance. Any inquiry into information about communications that changes over time should be seen as surveillance-type activity, and therefore not an inquiry into business records.

Because the question of the constitutional protection of stored e-mail remains unresolved, the question of where the line should be drawn around protecting stored e-mail remains unresolved as well. We would resolve it by grouping both communications contents and their associated attributes into a single category in which users retain a reasonable expectation of privacy, and we reject the distinction offered by some courts between communications contents and non-contents information. First, we regard those cases as overreading the Supreme Court's decision in *Smith v Maryland*, which, in 1979, withheld constitutional protection from the telephone numbers detected by a mechanical recording device. *Smith* did not address the vastly richer information available about modern communications, such as the identities of the parties, the duration of their communications, and all of the information associated with web-based communications and use. Second, we agree with those courts which have rejected the contents/non-contents dividing line and which have extended constitutional protection, often as a matter of state constitutional law, to all communication attributes.
short, we view only static, non-communication records to be unprotected by the warrant requirement.

Besides static, non-communication records, a second category of information also proves problematic for e-mail users under constitutional precedents. As we have also discussed, those communications as to which the ISP is a party fall within the line of cases concerning confidants. Those precedents, and modern equivalents involving electronic bulletin boards\textsuperscript{175} and chat rooms,\textsuperscript{176} establish that when an e-mail user intentionally sends an e-mail (or other electronic communication) to another, she assumes the risk that the intended recipient will disclose that communication to the government.\textsuperscript{177} The Warshak panel also clearly carved out this scenario as one in which the user's expectation of privacy would not be reasonable.\textsuperscript{178} To be clear, these are cases in which the ISP, as recipient of an intended communication, acts as a "second party" rather than a third party to a communication between two others.

Before we move on to the cases in which the ISP acts as a third party, however, we would argue that courts should be careful when they consider the implications of disclosure to a second party ISP. Cases have held that those who communicate with another have no claim when that other party voluntarily discloses the communication to another.\textsuperscript{179} That voluntary disclosure is within the set of risks that the first party assumes. And they have held that the first party lacks standing to contest the manner in which the second party is made to hand over the communication in those cases in which the government must compel the second party to disclose.\textsuperscript{180} But the cases do not say that the second party, here the ISP, lacks its own standing to assert a Fourth Amendment right of privacy in the communication—in other words to refuse to disclose the communication without a warrant. And they do not establish that the first party user should expect, or assume, that the government will violate

\begin{itemize}
  \item \textsuperscript{175} Leis, 255 F3d at 330.
  \item \textsuperscript{176} United States v Charbonneau, 979 F Supp 1177, 1184–85 (S D Ohio 1997); State v Evers, 815 A2d 432, 439–40 (NJ 2003).
  \item \textsuperscript{177} See Charbonneau, 979 F Supp at 1184–85 (relying in part on Hoffa in concluding that chat room user lacked expectation of privacy in messages, where undercover agents were participants in chat room).
  \item \textsuperscript{178} See Warshak, 490 F3d at 470–71.
  \item \textsuperscript{179} See Part III B 2.
  \item \textsuperscript{180} See Miller, 425 US at 445 (concluding that target “possessed no Fourth Amendment interest that could be vindicated by a challenge to the subpoenas.”).  
\end{itemize}
the rights of the second party ISP by compelling disclosure without obtaining a warrant if the second party does assert its own Fourth Amendment claims.

It should be easy to understand why this scenario has not yet presented itself to a court. The question of the ISP's rights would arise only if the government compelled the ISP to disclose its actual communications with a customer and the ISP asserted its own Fourth Amendment claim. The customer's reasonable expectation of privacy in that scenario would be an issue only if the customer were somehow able to overcome her lack of Fourth Amendment standing. Nonetheless, careful consideration of this scenario, and of the precedents that govern, indicates a useful rule for actual third party cases: a user does not forfeit her Fourth Amendment rights merely because there is another party to the communication. Katz, for one, and the entire electronic surveillance statutory structure, rest on the recognition that two-party communications may be private and that the parties to them may expect the government to follow the dictates of the Fourth Amendment in obtaining access to them.

With that in mind, we now turn to the cases in which the government seeks neither communications to which the ISP is a party, nor static, non-communication records of the ISP's business, in which it retains an independent interest and which do not implicate the user's reasonable expectations of privacy. In other words, does a user's granting of access to an ISP to her communications with others lead the user to forfeit an expectation of privacy vis-à-vis that ISP, and if so, what does that mean for government access?

We first return to the proper analogy for the information at issue. These are neither static, non-communication business records nor communications to which the ISP is an actual party, but rather communications and attributes created when the target communicates with others, and to which the ISP obtains some access. As we have discussed, we view the best analogy for this scenario as the cases in which a third party carries, transports, or stores property for another. In those cases, as in the stored e-mail case, the customer grants access to the ISP because it is essential to the customer's interests. Someone cannot send a letter or package without engaging an intermediary—the postal service or package service—to do the actual transporting. But one does not engage the third party because one wants the intermediary to have access; that access is a required means of effectuating the customer's interests. The same can be said of the
user of a storage locker, a rental property, or a safe deposit box. The customer's interest in making use of the service necessitates the involvement of the third party. Of course, the same may be said of the ISP customer; she engages with the ISP out of the desire to use its intermediary services.

In all cases, the third party intermediaries retain rights of access to protect their own property and to provide their own services. As we have discussed, in all the analogous cases, the law has clearly required that the government procure a warrant before demanding access to those items carried, transported, or stored. That is because the law has recognized that permitting access to an intermediary who needs such access to provide his service or protect his property has no bearing on one's reasonable expectations of privacy vis-à-vis the government. The same must apply for users of ISPs. The contrary notion that users forfeit all expectations of privacy by virtue of permitting access to ISPs to protect their business and property is both counter-intuitive and in conflict with Fourth Amendment law. To be clear, users may lack a reasonable expectation of privacy with regard to those third party intermediaries who discover information in the course of exercising their rightful access to the users' packages, storage lockers, rental properties, or stored e-mail accounts.

181 See notes 130–32 and accompanying text.
182 See, for example, Stoner, 376 US at 489 ("It is important to bear in mind that it was the petitioner's constitutional right which was at stake here, and not the night clerk's nor the hotel's. It was a right, therefore, which only the petitioner could waive by word or deed, either directly or through an agent. It is true that the night clerk clearly and unambiguously consented to the search. But there is nothing in the record to indicate that the police had any basis whatsoever to believe that the night clerk had been authorized by the petitioner to permit the police to search the petitioner's room.").
183 See id at 489–90 (finding defendant to have retained Fourth Amendment claim against warrantless search despite hotel clerk's consent and rights of access); Chapman, 365 US at 616–18 (holding that home owner's putative right to enter rental premises to view waste did not give it permission to authorize law enforcement warrantless search for evidence of a crime).
184 In addition, a customer who fails to pay or to remove property at the end of a definite term, or who violates the agreement with the third party may have so altered the relationship with the third party as to have forfeited his right to rely on the fact that the intermediary will not turn over that property to the government. See, for example, United States v Poulsen, 41 F3d 1330, 1336–37 (9th Cir 1994) (holding that 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); United States v Rahme, 813 F2d 31, 34–35 (2d Cir 1987) (holding that 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). The case of United States v Young, 360 F3d 1302 (11th Cir 2003), would seem to go further. There the court held that a warrantless search was constitutional because the defendant failed to adhere to Fed-Ex's clear contractual requirement
That implies that if the third party chooses to disclose the information so discovered to the government without requiring a warrant, the user cannot complain. When the user assumed the risk that the intermediary would discover incriminating information or property in the course of its business, she also assumed the risk that the intermediary would choose to turn that information over to the government. If the user mistakenly trusted the intermediary to protect its incriminating information, there is no reason for the Fourth Amendment to protect that misplaced trust. Importantly, however, permitting the third party access to one’s property or communications does not mean that one accedes to unlawful acquisition by the government. In those cases when the relationship with the third party is intact and when the third party chooses not to disclose information to the government but instead resists, the government must proceed to get a warrant. There is no reason to construe the user’s assumption of the risk that the intermediary will discover incriminating information in the course of its proper access as the assumption of the risk that the government will compel the ISP that resists to produce that information without following the proper procedures.

While thus far we have been discussing ISPs that provide services to the public, we should note that our analysis extends as well to private ISPs, such as employers and educational institutions who provide e-mail to employees and other constituents. Because of the nature of the employment or educational environment, private ISPs likely enjoy greater access to users of their e-mail systems. That, in turn, means that they will likely not to ship cash, and Fed-Ex retained the right to search all packages without limit. In its discussion, however, the court did not say that consent to search alone would be sufficient, and it noted that the precedents required both violation of contract terms and that the search was not instigated by the government. Id at 1305–08.

See note 139 and accompanying text. See also White, 401 US at 749 (holding that a defendant has no “justifiable and constitutionally protected expectation that a person with whom he is conversing will not then or later reveal the conversation to the police”). Whether this rule should apply in the ISP context is beyond the scope of this Article, but certainly not beyond question.

See, for example, United States v Barry, 673 F2d 912, 915–18 (6th Cir 1982) (distinguishing between cases in which the carrier originated the disclosure to the government and those in which the carrier was asked, and therefore acted as an agent of the government).

The argument for this is the same for the argument that granting an ISP the right to respond to lawful access cannot be the same thing as granting the ISP the right to respond to access that violates the constitution. See Part III C 1 b.

Employees’ e-mails may provide an indication, for example, of how employees treat the company’s customers, of whether employees are sharing proprietary information with
have more opportunity to uncover incriminating information. Just as with public ISPs, however, such private ISPs may not be compelled to turn over information so uncovered without the proper procedure of a warrant.\(^{189}\) Unless the information they discover is a static, non-communication record of their business, or a communication to which the ISP itself is a party, the stored e-mail's sender or recipient enjoys the protections of the warrant requirement.

Finally, there are at least two ways in which the government may wrongfully try to compel disclosure by an ISP, public or private. One is to issue a subpoena or related court order for information that the ISP has discovered in the course of its own rightful access to the communications of its users. Another is to use a subpoena or related court order to compel an ISP to disclose a greater amount of information on the grounds that it could have discovered the information itself in the course of its exercise of its lawful access. The second scenario, which more closely resembles the government's actions in the Warshak investigation, is no more defensible than the first.\(^{190}\) When the ISP proceeds in response to a court order or subpoena, or even at the request of the government, it acts as an agent of the government and the scope of its private access to its users' e-mails should play no role in the constitutional analysis.\(^{191}\)

2. Summary.

We have argued that the government may compel disclosure of information from an ISP without obtaining a probable-cause warrant only when it seeks the ISP's static, non-communication records of its business or information pertaining to the ISP's own outsiders, and of whether employees are properly using their time in the office.

\(^{189}\) In this context, consider *O'Connor v Ortega*, 480 US 709, 721–23 (1987) (plurality opinion) (recognizing, in a case involving a government employer, the need to distinguish between searches for work-related purposes and searches for evidence of criminal misconduct, and subjecting only the former to a reasonableness requirement).

\(^{190}\) See, for example, *Stoner*, 376 US at 489–90 (holding that a warrant was needed because agents asked hotel clerk for entry to defendant's room); *Chapman*, 365 US at 616–18 (holding that agents needed a warrant when they asked property owner's permission to enter renter's house with the purpose of investigating crime).

\(^{191}\) See *Long*, 64 MJ at 65 (in context of search of e-mails by military employer, distinguishing a prior case in which "incriminating e-mail evidence was found inadvertently by personnel performing routine systems maintenance" and concluding that "evidence seized in this case was [seized] as a part of a search for law enforcement purposes"). For other cases distinguishing private searches from government searches, see, for example, *United States v Jarrett*, 338 F3d 339 (4th Cir 2003); *United States v Steiger*, 318 F3d 1039, 1045–46 (11th Cir 2003); *United States v Runyan*, 275 F3d 449, 456 (5th Cir 2001).
communications. For access to all other information, though the ISP may choose to disclose the information to which it has access without violating a user's reasonable expectation of privacy, it may not be compelled to do so unless the government first obtains a warrant based on probable cause.\textsuperscript{192} The provider's technical ability to access communications and the provider's announcement that it will comply with legal process are clearly irrelevant. The provider's rights to protect its own property and to prevent misuse of its services limit the conditions under which the user may allege that the provider has violated his privacy rights, but do nothing to reduce the government's obligation under the Fourth Amendment to acquire a warrant before it either demands access to what the ISP has discovered or demands that the ISP conduct a new search in aid of the government's own investigative mission.

D. Comparison of the Warshak Panel's Approach

1. Reasonable expectations of privacy in ISP relationships.

In the course of its decision, the Warshak panel described three possible scenarios under which users may in fact waive their reasonable expectations of privacy in those e-mails they store with third party ISPs.\textsuperscript{193} Our analysis arrives at roughly the same conclusion as to the first scenario but differs as to the second and third.

In the first scenario, a third party may disclose those e-mails to which it is a party.\textsuperscript{194} We agree that such a conclusion follows from the Hoffa/White line of cases, but emphasize again that a third party's right to disclose e-mails does not equate to the government's right to compel such disclosure without a warrant. It is axiomatic that a government agent cannot open a sealed letter without a warrant while it is being carried by the United States Postal service, while the letter's ultimate recipient is free to disclose it to the government without restriction.\textsuperscript{195}

\textsuperscript{192} See Part IV B for our discussion of whether a wiretap order may be required instead.

\textsuperscript{193} The ISP is a third party in that the sender of the e-mail is the first party and the recipient is the second party.

\textsuperscript{194} Warshak, 490 F3d at 475. As discussed above, the ISP is actually the second party to the communication. See text accompanying notes 178–80.

\textsuperscript{195} Compare Ex parte Jackson, 96 US at 733 (holding that letters and packages sent through the mail guarded by same protection from government search and seizure as though they were retained by the sender and recipient in their homes) with White, 401
In the second scenario, the panel recognized that ISPs may disclose to law enforcement agents those attributes of communications to which they retain access in the ordinary course of their business. While it is unclear exactly to which attributes the panel was referring, the panel made clear that the contents of e-mails could not be so disclosed. To the extent that the panel was discussing the static, non-communication records of the ISP, such as the "subscriber information" to which it referred explicitly, we feel compelled to agree, based on *Miller*. But we disagree with the panel's approach to the extent that it is meant to apply to the other communication attributes to which ISPs have access. We view those other communications attributes, along with their associated communications, to be protected against compelled disclosure by the warrant requirement.

In the panel's third scenario, ISPs may disclose those e-mails to which their agreements with users grant them "total access." While the panel recognized the conceptual question as whether "the challenger has . . . maintained an expectation of privacy with respect to the individual being compelled to make the disclosure," we believe that it misapprehended the implications of ISP access. As we have just discussed, when stored e-mail users lose a reasonable expectation of privacy in information to which the ISP has proper access, they lose the right to complain about the ISP's voluntary disclosure of that information. But they do not assume the risk that the government will compel the ISP, without a warrant, to turn over information, whether or not the ISP actually obtained access to that information in the course of its business.

2. Raising Fourth Amendment claims.

Our disagreement with some of the *Warshak* panel's findings leads us to specify exactly how we believe a court should respond when presented with a question as to the Fourth Amendment status of stored e-mail. Our approach, while quite

---

196 *Warshak*, 490 F3d at 473–74.
197 Id at 471.
198 Id at 475.
199 Id at 469 (casting the "critical question" as whether "an e-mail user maintains a reasonable expectation of privacy in his e-mails vis-à-vis the party who is subject to compelled disclosure—in this instance, the ISPs.").
similar to the procedure outlined by the Warshak panel, differs in a few important respects.

The Warshak panel indicated that the government could obtain a warrant to compel an ISP to disclose the e-mails it stores for its users. We agree with that approach for all information other than the static, non-communication records of the ISP's business, though we consider, in the next part, whether it would make more sense for a court to demand an order that meets the Fourth Amendment requirements for electronic surveillance set forth in Berger.\textsuperscript{200}

The panel also indicated that the government could bypass the need for a warrant and proceed under a subpoena when it establishes to a reviewing court's satisfaction that the ISP has extinguished its user's expectation of privacy in her communications by (a) explicitly reserving the right to monitor (b) the contents of communications and (c) exercising that right in the ordinary course of its business.\textsuperscript{201}

We do not agree that such a showing would entitle the government to proceed by subpoena or equivalent court order. As discussed, the nature of the ISP's access to its users' communications is relevant to the users' potential privacy or contract claims against the ISP. That access may also imply that the user lacks a Fourth Amendment claim when an ISP, pursuant to lawful access, obtains incriminating information and chooses to disclose it to the government. But ISP access does not mean that the government may either compel the ISP to disclose non-static communications information it has found or ask the ISP to gather information without first obtaining a warrant based on probable cause.

Besides being more in keeping with the principles of the Fourth Amendment and the precedents, our approach dramatically reduces the need for a detailed, fact-based inquiry. The question for a reviewing court is whether the ISP acted independently of the government in turning over the pertinent information. If not, a warrant, at least, is clearly required. If so, further inquiry into the nature of the ISP's privacy violation would be necessary only to evaluate the user's claims against the ISP. Since it should be relatively straightforward to determine whether the ISP volunteered the information at issue or the gov-

\textsuperscript{200} 388 US at 55–60 (discussing the heightened need for particularity and other safeguards in the context of electronic surveillance).

\textsuperscript{201} Warshak, 490 F3d at 473–74.
ernment compelled disclosure, there will be little need for individual hearings. In addition, to the extent the SCA permits compelled disclosure without a prior warrant, it is clearly unconstitutional.

Finally, the panel indicated that the government may avoid obtaining a prior warrant or making the showing above if it instead provides the target with notice and an opportunity to be heard. During that hearing, the target must be entitled to raise the claim that warrantless compelled disclosure of her e-mails and related attributes would violate her Fourth Amendment rights. It is difficult to imagine why the government would shoulder any lesser burden, unless one accepted the argument that compelled disclosure merits only reasonableness review (independent of the target’s reasonable expectation of privacy), which is a view we have refuted.

IV. CONSTITUTIONAL PROTECTION AND GOVERNMENT PROCEDURES

A. Unifying the SCA’s Procedural Hurdles

As we discussed in Part I A, the DOJ has proffered a confusing set of statutory interpretations that have construed the SCA to impose minimal procedural burdens on government investigators. As we discussed, under the DOJ’s scheme, the procedural hurdles for access to stored e-mails vary based on how long the e-mails have been stored, whether they have been downloaded or accessed, and with what type of service provider they reside.

Recall that the DOJ views a significant category of stored e-mails as lacking any of the protections of SCA and regards a tiny category of stored e-mails as entitled to the protections of the warrant requirement. In particular, the DOJ claims the right to acquire any opened, accessed, or downloaded e-mails stored on corporate or university computers without adhering to the SCA in any way. It says it may acquire those e-mails that have

---

202 See note 85 (providing conflicting statements of the Warshak panel) and note 52 (providing district court language that is consistent with our argument).
203 See Orin Kerr, Warshak and Fourth Amendment Standards for Orders to Compel, available at <http://volokh.com/archives/archive_2007_06_24-2007_06_30.shtml#1182840096> (last visited Apr 11, 2008) (interpreting panel decision to suggest that “the Fourth Amendment requires probable cause or notice, but the presence of notice drops the required legal threshold down to reasonableness” but criticizing that suggestion).
204 See Part III A.
205 DOJ Search Manual at 89 (cited in note 19) (describing how the “ECPA no longer
been opened or otherwise accessed on an ISP that provides service to the public using a subpoena or related court order pursuant to § 2703(d). Only those e-mails that are neither drafts nor copies of sent e-mails, and that have been residing 180 days or less without being opened, accessed, or downloaded, require a probable cause warrant to acquire.\textsuperscript{206} In addition to imposing only minimal constraints on government agents before they obtain stored e-mails, the SCA provides no statutory exclusionary remedy\textsuperscript{207} and offers limited civil remedies\textsuperscript{208} to victims of those investigations that fail to satisfy the minimal protections it imposes.

The recognition that the Fourth Amendment regulates government access to stored e-mails and their attributes implies a much simpler scheme, and one that provides much higher procedural hurdles and significant remedies. As discussed above, Fourth Amendment questions arise only when the government requests disclosure instead of the ISP volunteering it. Then, the focus must be on distinguishing between static, non-communication records of the ISP, to which the subpoena standard applies, and everything else. For everything else, the government must acquire a warrant based on probable cause, at least. Failure to adhere to that constitutional minimum necessitates the availability of a suppression remedy as to all evidence acquired from the ISP or derived from that evidence.\textsuperscript{209} The Fourth Amendment analysis does not depend on how long the information has been stored because the analysis concerns whether the government's inquiry covers a period of time and not when that period of time occurred.\textsuperscript{210} Similarly, there is no con-

\textsuperscript{206} Id at 95–99. Even for those, the DOJ claims that it does not need to give notice to the target, although the Federal Rules of Criminal Procedure require such notice. The DOJ manual claims that the "search warrant obviates the need to give notice to the subscriber," but for that proposition it cites only a provision of the statute that does not in fact apply to the category of communications discussed in the text. See id at 98 (citing 18 USC § 2703(b)(1)(A)).

\textsuperscript{207} See 18 USC § 2708 (2000) (limiting remedies to those provided by statute and not providing suppression remedy for stored records, no matter how acquired).

\textsuperscript{208} The USA PATRIOT Act raised the civil recovery from $1,000 to $10,000 but precluded attorneys' fees awards and limited recovery to cases in which victims establish "willful" violations. See 18 USC § 2712 (2000 & Supp IV 2004).

\textsuperscript{209} See, for example, State v Reid, 2008 WL 1774969, *10–11 (NJ 2008) (granting a suppression remedy for subscriber information obtained without meeting constitutional requisites); Commonwealth v Melilli, 521 Pa 405 (1989) (granting suppression remedy for evidence gathered by pen register without a warrant).

\textsuperscript{210} Freiwald, 2007 Stan Tech L Rev 3 at ¶¶ 74–75 (cited in note 60) (making the dis-
stitutional basis for reducing the procedural hurdles imposed on demands for e-mails because they are stored on systems that do not provide e-mail to the public. As we discussed above, employers likely engage in monitoring practices that afford their employees a lower expectation of privacy vis-à-vis their employers in their stored information than users of public systems. But that means only that the employer or university will have access to more information that it may choose to disclose to the government without violating the user’s rights. But whatever the scope of the private ISP’s access to users’ stored communications, that has no bearing on the government’s ability to compel disclosure. Therefore, whenever the government seeks an ISP’s communication records instead of its static, non-communication, records the government must acquire a warrant, no matter what the ISP’s status.

Finally, warrant-level protection for stored e-mail should persist whether or not an e-mail has been opened, accessed, or downloaded. It is hard to imagine why the act of reading or preparing to read an e-mail, which is the entire point of communicating by e-mail, should somehow deprive a user of his reasonable expectation of privacy in the electronic communication. As discussed, the government’s distinctions on this basis derive from a strained reading of out-of-date statutory provisions, and neither reflect nor should impact the Fourth Amendment status of stored e-mail.

In conclusion, Fourth Amendment protection for stored e-mail does not hinge on arcane terms embedded in the SCA nor the DOJ’s tortured interpretations of those terms. The Warshak panel recognized this by failing to use any of the categories just described in its analysis. constitutional protection for stored e-mail brings much needed simplicity to the scheme of electronic communications privacy. It also requires much more protection than the DOJ interprets the SCA to provide. To the extent that the SCA provides less than a warrant requirement as the procedural hurdle to access stored e-mail and attributes not considered to be a static, non-communication record of the ISP, it must be struck down.

211 The Warshak panel’s injunction said nothing about the duration of the constitutional protection or whether the e-mail had been opened, downloaded, or otherwise accessed. Warshak, 490 F3d at 475. It also noted that its analysis applied to e-mails stored on private ISPs as well as public. See id at 473.
B. Procedural Requirements: Wiretap Order or Warrant?

As we briefly noted in the introduction, the procedural hurdles imposed on government agents who seek a wiretap to intercept telephone conversations are more burdensome than those imposed on agents who seek a traditional search warrant to search a home. Courts have granted targets of electronic surveillance technologies the highest level of Fourth Amendment protection by imposing significantly more stringent restraints on government agents than that imposed by the warrant requirement. In *Berger*, the Supreme Court found the Fourth Amendment to require that agents use wiretapping and eavesdropping as a last resort, strictly limit the duration of their investigations, and minimize the collection of non-incriminating communications.\(^{212}\) An important procedural question that follows from treating the government's acquisition of stored e-mail as a Fourth Amendment search is: should the protections afforded wiretapping apply or should a traditional probable-cause warrant apply?

We have already made what we view as the best argument for applying the same heightened protection accorded to telephone calls to stored e-mail surveillance.\(^{213}\) As the *Warshak* panel recognized, e-mail is the modern day analog of a telephone conversation. Accordingly, the compelled disclosure of stored e-mail accounts has the potential to be as hidden, continuous, indiscriminate, and intrusive as wiretapping and video surveillance.\(^{214}\) At the same time, Congress has distinguished between information in electronic storage and information acquired in real time, and has accorded the former less protection.\(^{215}\) The question is whether that distinction, made as a matter of policy in 1986, holds up as a matter of constitutional law today.

In fact, there are good arguments for holding the compelled disclosure of stored e-mail to a simple probable cause-based warrant.\(^{216}\) There are several ways in which, depending on the nature of the investigation, the compelled disclosure of stored e-mail and its attributes could actually be less hidden, continuous,

\(^{212}\) *Berger*, 388 US at 58–60.

\(^{213}\) See note 60 and accompanying text.

\(^{214}\) See Freiwald, 2007 Stan Tech L Rev 3 at ¶¶ 61–72 (cited in note 60); Freiwald, 56 Ala L Rev at 81 (cited in note 2).

\(^{215}\) See note 2.

\(^{216}\) See, for example, Solove, 72 Geo Wash L Rev at 1298–1303 (cited in note 74) (advocating a warrant for online surveillance).
indiscriminate, and intrusive. First of all, if the target is given prior notice of the disclosure order, and the chance to contest it before it is executed, then the investigative tool would no longer be hidden. To the extent agents must meet the particularity requirement and compel disclosure only of those stored e-mails for which they have probable cause, the indiscriminate and intrusive nature of the surveillance may be reduced if the ISP produces only those e-mails and related attributes that are particularly specified. Similarly, if agents substantially limit the period over which the e-mails and attributes they seek were sent and received, and particularly if they limit their inquiry to one moment in time, then the investigation would seem less continuous than wiretapping. In fact, as we have argued, one may analogize stored e-mail searches to a search for first class letters, which are regulated by the warrant requirement but not by the heightened wiretap requirements. Second, one can analogize such searches to the searches of stored containers, as the *Warshak* panel did. Those are also subject only to a warrant based on probable cause.

All in all, if a simple search warrant is used along with procedures that minimize the problematic qualities of stored e-mail surveillance, it is possible that process would suffice to meet constitutional requirements. However, if the government seeks stored e-mail or its attributes covering a period of time, and if the breadth of the request makes it indiscriminate, stored e-mail surveillance could merit the application of a wiretap court order. Stored e-mail surveillance can be significantly more intrusive than a traditional wiretap. Depending on whether, and, if so, when, the target receives notice and an opportunity to be heard, stored e-mail surveillance may be equally as hidden.

Whether a wiretap order or a traditional search warrant is required, targets of improper investigations must have the benefit of a suppression remedy. That requirement is, of course, mandated by constitutional doctrine. In addition, the incentive to bring a constitutional challenge, which accompanies the exclusionary rule, will mean more cases and more opportunities to refine the doctrine as necessary to reflect new circumstances and, undoubtedly, new technologies.

---

218 The numerous challenges to wiretapping investigations have helped to define the constitutionally permissible parameters of that practice.
CONCLUSION

E-mail users generally retain a reasonable expectation of privacy in the e-mails and related attributes stored on their ISPs' computers. Fourth Amendment precedents support that conclusion. The DOJ's arguments to the contrary rely on misunderstandings of the precedents and ultimately on normative arguments that are unpersuasive. Once courts recognize a reasonable expectation of privacy in stored e-mail, as the Warshak panel did in the Sixth Circuit, they will bring the constitutional protection of modern electronic communications in line with analogous traditional media. According warrant-level protection for stored e-mail requires courts to construe the SCA's warrant requirement to apply to virtually all stored e-mail or to invalidate the SCA to the extent that such a construction is impossible. Either way, it provides both a dramatic simplification in the statutory law and meaningful judicial oversight of modern surveillance practices.