The Stored Communications Act and Private E-Mail Communications

The Government's Unconstitutional Policy of Seizing Private E-Mails Without a Warrant or Notice

BY ROBERT M. GOLDSTEIN AND MARTIN G. WEINBERG

Electronic mail ("e-mail") has quickly become the preferred medium of written communication in the United States of America. E-mail has literally transformed the manner in which American society communicates, and members of society clearly have a vital interest in preserving the privacy of the contents of their e-mails.[1] Certainly, an individual possesses a strong and reasonable expectation of privacy in the contents of his or her e-mail messages — whether traveling on the electronic highway or stored within an Internet Service Provider ("ISP") server — and these modern day "closed containers" are entitled to the full protections of the Fourth Amendment, just as the Supreme Court has clearly held in the context of first-class mail and packages.[2]

The government believes otherwise, however, and through employment of the **Stored Communications Act, codified at 18 U.S.C.** § 2701 *et seq.* ("Act" or "SCA"), it has effectuated a policy that allows it to seize and read a citizen's e-mails without comporting with the dictates of the Fourth Amendment, *i.e.*, without demonstrating probable cause that the seized e-mails are somehow connected to criminal activity, and without securing a judicially issued warrant. Moreover, through the Act, the government accomplishes a wholesale seizure of its targets' e-mails, without any limitation on the subject matter of the e-mails or the participants to the communication, and thereby gains access to a citizen's most private communications (privileged e-mails to a spouse or attorney, or a private message to oneself as a reminder for upcoming events or as motivation to reach goals) in flagrant disregard of the Fourth Amendment's particularity requirements. The government has also inserted into its SCA Applications and Proposed Orders its own definition of *electronic storage*, a key term within the Act. This definition — flatly rejected by the Ninth Circuit — allows the government to seize a significantly larger universe of e-mails than it would otherwise be entitled to obtain.

In *Warshak v. United States*, a target of a government investigation filed a civil suit and sought injunctive relief, asserting that the government's use of the Act violated his Fourth Amendment rights to the extent that it allowed the government to seize and search his e-mails without establishing probable cause, without a judicially issued search warrant, and without any particularity.[3] In granting Steven Warshak a preliminary injunction, the Honorable Susan J. Dlott, in a case of first impression, concluded that Warshak had "shown a substantial likelihood of success on the merits of his Fourth Amendment claim," and preliminarily held that particular sections of the Act violate the Fourth Amendment "to the extent

that they collectively authorize the *ex parte* issuance of search and seizure orders without a warrant and on less than a showing of probable cause."[4]

The government appealed and, on June 18, 2007, the Sixth Circuit Court of Appeals, in an opinion authored by the Honorable Boyce F. Martin Jr., affirmed the district court's decision, asserting, *inter alia*, it has "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."[5] "It goes without saying," the court observed, "that like the telephone earlier in our history, e-mail is an ever-increasing mode of private communication, and protecting shared communications through this medium is as important to Fourth Amendment principles today as protecting telephone conversations has been in the past."[6]

The Sixth Circuit held the government cannot lawfully secure the content of an individual's e-mails unless: (1) it first "obtains a search warrant under the Fourth Amendment, based on probable cause and in compliance with the particularity requirement," (2) it provides notice to the account holder in seeking an SCA order, according him the same judicial review he would be allowed were he to be subpoenaed, or (3) the government can show specific, articulable facts demonstrating that an ISP or other entity has complete access to the e-mails in question ("such as where the government can show that auditing, monitoring, or inspection are expressly provided for in the terms of service") and that the ISP actually relies on and utilizes this access in the normal course of business, sufficient to establish that the user has waived his expectation of privacy with respect to that entity.[7]

This article will discuss the relevant statutory sections, how and why the government's use of the Act violates the Fourth Amendment and contradicts the Supreme Court's well-seasoned "closed container" jurisprudence, and why the government's arguments to the contrary are not persuasive. We will utilize the facts and arguments presented in *Warshak* for contextual flavor, as well as a paradigm to demonstrate the government's narrow view of the Fourth Amendment and its expansive use of the SCA.

The Act, E-Mail and the Fourth Amendment

For the government to compel an ISP to provide the contents of a wire or electronic communication in "electronic storage" for 180 days or less, it must obtain a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation (or equivalent state warrant).[8] For e-mail communications in electronic storage for 181 days or more, however, the Act allows the government to compel disclosure of these private e-mail communications by an administrative or grand jury subpoena,[9] or court order if the government "offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication are relevant and material to an ongoing investigation."[10] Of course, as discussed in detail *infra*, it appears that the government unilaterally inserts into its Applications and Proposed Orders its own definition of *electronic storage*, which allows the government to seize and read any e-mail that has been opened or accessed by the ISP customer, whether it has been in one's virtual mailbox for one day or 181 days.

To the extent the Act allows the government to compel disclosure of private e-mail communications without a warrant, it violates well-established Supreme Court "closed container" jurisprudence. As early as 1878, the Supreme Court determined that the contents of "[l]etters and sealed packages … in the mail are as fully guarded from examination and inspection … as if they were retained by the parties forwarding them in their own domiciles."[11] As long as a package is "closed against inspection," the Fourth Amendment protects its contents "wherever they may be," and the police must obtain a warrant to search it just "as is required when papers are subjected to search in one's own household." [12]Indeed, the Supreme Court has long recognized that individuals do not surrender their expectations of privacy in closed containers when they send them by mail or common carrier, and that "[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."[13]

E-mails stored on an ISP's server are simply another, albeit modern, form of a closed container. The contents of an e-mail are not visible to the naked eye; rather, there are several intrusive searches that axiomatically precede one's ability to view the contents of an e-mail stored on an ISP's server.

First, an individual seeking to view the contents of an e-mail must gain access to that portion of the ISP's server that houses the subscriber's e-mail, a process that typically encompasses a screen name and a password. Even after one gains access to a subscriber's virtual mailbox, the contents of those e-mails remain closed against inspection, much like the contents of a first-class letter remain shielded when one peers into a mailbox at the top of a driveway. To view the contents of the e-mail, an individual must take another intrusive physical act — he or she must unseal the e-mail. To do so, one double-clicks on the e-mail through the use of a computer mouse or perhaps using the "open" function of the computer. Either way, the closed nature of the e-mail conceals its contents from plain view until somebody opens or unseals it. This is no different from the physical act of unsealing a closed first-class envelope, unsealing a closed package, unlocking a closed footlocker, opening a closed filing cabinet, or opening a closed storage facility. From a doctrinal perspective, these incontrovertible facts compel a finding that an e-mail is a closed package and, as such, no constitutional difference exists between unsealing a first-class letter and double-clicking an e-mail, and both closed containers are entitled to the same constitutional protection.

Certainly, in creating a relationship with an ISP, the subscriber does not relinquish a reasonable expectation of privacy in any unopened or opened-and-then-closed-again e-mail communication stored on the ISP's server. Keeping a closed e-mail on the server of an ISP does not relinquish one's interest in the e-mail, or the reasonable expectation of privacy therein. Indeed, in the case of e-mail, the subscriber maintains more control over the e-mail letter than in any other traditional third party carrier context. In the latter scenarios, the sender or receiver of a closed letter or package actually relinquishes control of the container. He or she cannot immediately repossess the letter or package; it is in the physical possession of the postal carrier or common carrier outside the dominion and control of the sender or recipient. In the e-mail context, however, the owner of the e-mail can repossess a read-and-then-closed e-mail at any moment, without any notice or permission from the ISP. The owner of the e-mail can delete it from the mailbox, or do whatever he or she wants to do with the e-mail. It is, for all purposes, in that

person's possession, dominion, and control at all times. Consequently, if there is any difference, the privacy interests should be greater in the context of e-mail than in the traditional carrier paradigm — an argument the district court in *Warshak* found persuasive.[14]

In *Warshak*, to defend its use of the Act, the government unpersuasively argued that an individual loses any reasonable expectation of privacy in the content of e-mails because some (but not all) ISP contracts permit the *ISP* to review e-mail content for limited, particularized reasons. That the ISP might theoretically have access to one's e-mails does not affect the constitutional inquiry surrounding the *government's* search or seizure of these closed containers. It is well settled that while common carriers or other private parties do not violate the Fourth Amendment if they search the packages of others, whether or not they have authority to do so, since the amendment protects only against unreasonable governmental action,[15] if government agents themselves are to open containers that are sent by mail or private carrier, or order a private carrier to open a closed container, the private carrier therefore becomes a government agent and the government must comply with the Fourth Amendment.[16] Moreover, while the seizure of a container might not necessarily compromise the interest in preserving the privacy of its contents, it may only be opened pursuant to either a search warrant[17] or one of the well-delineated exceptions to the warrant requirement. The bottom line is that "unless the container is such that its contents may be said to be in plain view, those contents are fully protected by the Fourth Amendment."[18]

As such, the government's general reliance upon ISP service agreements or terms of service is unavailing. That Yahoo! or other ISPs inform their account holders that they may access and disclose "content" for certain limited purposes, including complying with legal process, does not control the constitutional propriety of governmental searches of e-mails stored by ISPs. The terms of service are, at most, contractual agreements between private parties which cannot and do not confer any rights on the government. Whatever the provisions of the terms of service, the government must still conduct itself in accordance with the law. If the Fourth Amendment requires a warrant, an announcement to subscribers by Yahoo! or another ISP that it will access "content" to comply with legal process other than a warrant is irrelevant. As the district court ruled in granting Warshak's preliminary injunction:

> This screening for illegal content, even assuming it happens as a matter of course, does not appear to the court to destroy the analogy between the contents of e-mail accounts and the contents of sealed packages or letters. The Supreme Court has held that once agents for a private carrier have opened and viewed the contents of a suspicious package without any government prompting, the government may re-examine those exposed contents without violating the Fourth Amendment's warrant requirements. *Jacobsen*, 466 U.S. at 115-116. However, it has also rejected the proposition that government authorities may rely on broad private searches to circumvent their Fourth Amendment obligations. *See, e.g., Jacobsen*, 466 U.S. at 117-18. By analogy, it would seem that even if an ISP's discovery that a subscriber e-mail contained child pornographic content gave the government sufficient grounds to seize and view that e-mail without a warrant, it would not necessarily follow that the government could routinely seize and view the contents of entire e-mail accounts not known to contain any illegal material.[19]

Likewise, the Sixth Circuit rejected the government's argument that Warshak waived any expectation of privacy because the terms of service provided limited access to e-mails. The court held that "mere accessibility is not enough to waive an expectation of privacy," noting that the terms of service cited by the government "provide for access only in limited circumstances, rather than wholesale inspection, auditing, or monitoring" of e-mails.[20] "Because the ISP's right to access e-mails under these user agreements is reserved for extraordinary circumstances, … it is similarly insufficient to undermine a user's expectation of privacy."[21]

Indeed, in *Warshak*, the government provided no reasons to believe that ISPs routinely *read* the contents of their customers' e-mails, as opposed to screening via computer programs without human intervention or actual comprehension of the content. The Sixth Circuit therefore appropriately observed that the government's argument that ISPs are developing technology to scan user images for child pornography and viruses has no bearing on an individual's expectation of privacy. Technological review, rather than manual, human review, "would not disclose the content of the e-mail to any person at the ISP or elsewhere, aside from the recipient," and "the reasonable expectation of privacy of an e-mail user goes to the *content* of the e-mail message."[22] Therefore, the Sixth Circuit held, the "fact that a computer scans millions of e-mails for signs of pornography or a virus does not invade an individual's content-based privacy interest in the e-mails and has little bearing on his expectation of privacy in the content."[23]

The rejections by the district court and Sixth Circuit of the government's reliance upon terms of service agreements are well grounded in law and fact. The mere fact that a third party has a theoretical right of access to the closed containers of another in their possession for specific and limited purposes does not give *the government* the right to obtain the contents of the containers without either a warrant or an exception to the warrant requirement.

It is well established that an individual manifests a subjective expectation of privacy that society views as objectively reasonable when he or she places contents into a closed container, even when he or she places that closed container in the possession of a private third party, such as within a friend's apartment, a leased house, a rented storage facility, or a third party common carrier.[24] As the Sixth Circuit observed, ISP screening processes are analogous to the post office screening packages for evidence of drugs or explosives, which does not expose the content of written documents enclosed in the packages.[25] "The fact that such screening occurs as a general matter does not diminish the well-established reasonable expectation of privacy that users of the mail maintain in the packages they send."[26]

In fact, while perhaps fact specific, the subscriber's relationship to the ISP typically adds to the reasonable expectation of privacy in the contents of closed e-mails contained on the ISP's server. Like an individual who rents a storage space at a local storage facility, an ISP subscriber contracts to secure a section of the ISP's storage facility (i.e., its server), sometimes incurring a fee in connection with the process. Indeed, in the *Warshak* case, the orders compelled pro-

duction of "contents of wire or electronic communications … that were placed or stored in directories or files *owned or controlled by the [subscriber's] accounts.*" (emphasis added). The very language of the orders sought and secured by the government acknowledged that the subscriber has an ownership or controlling interest in the directories or files in which the closed e-mails were stored.

Additionally, the subscriber's "storage space" within the ISP server is locked and inaccessible to the public at large, like the individual who places a lock on his storage space. While a physical storage space or a physical filing cabinet is protected by combination or key locks, the rented portion of the ISP's server is protected by a screen name and a password, precluding access to its contents by any member of the public. Moreover, like the owner of a physical storage facility, or a bailee who takes possession of another person's private documents, the ISP is not permitted to access the private mail contained on the server except under very limited circumstances. ISPs are not permitted or expected to simply open and review private e-mail at their whim and discretion.

There Are Limits to the Reach of Subpoenas

In defending the Act, the government improperly relied upon the line of cases wherein individuals knowingly expose communications to a third party, which are then conveyed to law enforcement authorities pursuant to subpoenas, most notably *United States v. Miller*.[27] In *Miller*, the Court held that a bank customer could not challenge on Fourth Amendment grounds the admission into evidence of financial records obtained by the government from his bank pursuant to allegedly defective subpoenas, despite the fact that he was given no notice of the subpoenas.[28] The Court ruled that no Fourth Amendment interests of the depositor were implicated because the depositor knowingly exposed those documents to the bank's employees in the ordinary course of business, and that "checks are not confidential communications but negotiable instruments to be used in commercial transactions."[29] As such, the Court ruled that the case was governed by the general rule that the issuance of a subpoena to a third party to obtain the records of that party does not violate the rights of a defendant.[30]

In the context of e-mail messages stored on an ISP server — whether they have been previously opened by the addressee or not — the messages remain closed to the public and to the ISP (except, perhaps, for limited, defined, extraordinary circumstances). Most importantly, they have not been provided to the ISP for their exposure, review, or consumption. Unlike the checks at issue in *Miller*, e-mail communications are closed containers and, even if an ISP contract provides limited circumstances in which they may be viewed by the ISP, subscribers have an objectively reasonable expectation that those e-mails will remain absolutely private and concealed subject to those very limited circumstances.

While the Supreme Court specifically noted that the documents at issue in *Miller* were "not confidential communications,"[31] e-mails obviously are confidential communications. Moreover, the checks at issue in *Miller* or the documents at issue in analogous cases do not involve closed containers. As argued *supra*, e-mail messages –whether stored in an individual's computer or in an ISP's server — are closed containers. Because e-mails are not openly exposed to employees of an ISP, it becomes crystal clear why e-mail is constitutionally different than tax records sent to an accountant (for the purpose of reviewing), and constitutionally equivalent to a closed container stored in one's home or in a remote storage facility.

Notwithstanding the government's protestations to the contrary, there should be limits to what the government may accomplish through the mechanism of grand jury and administrative subpoenas. No one, for example, would contend that the government could search a suitcase in the custody of an airline or a footlocker shipped via a third-party carrier simply because it obtained possession of the item through a subpoena. Nor could the government permissibly seize and search a briefcase by issuing a subpoena to the restaurant where it had been checked while its owner dined. Nor could the government subpoena the U.S. Postal Service to seize and search first class mail on the way to a target of an investigation. The government cannot search a computer's files simply because it obtained possession of the computer pursuant to a subpoena,[32] nor can the government search unopened mail without a warrant, even if it obtained the mail pursuant to a subpoena.[33]

In *Warshak*, the Sixth Circuit rejected the government's argument that secret court orders issued under the SCA are not searches, but rather compelled disclosures akin to subpoenas. Noting that subpoenas — even ones issued to third parties — are analyzed only under the Fourth Amendment's general reasonableness standard rather than a probable cause analysis, the Sixth Circuit noted that "[o]ne primary reason for this distinction is that, unlike 'the immediacy and intrusiveness of a search and seizure conducted pursuant to a warrant[,]' the reasonableness of an administrative subpoena's command can be contested in federal court before being enforced."[34] The court then observed that prior circuit precedent "makes explicit, however, a necessary Fourth Amendment caveat to the rule regarding third-party subpoenas: The party challenging the subpoena has 'standing to dispute [its] issuance on Fourth Amendment grounds' if he can 'demonstrate that he had a legitimate expectation of privacy attaching to the records obtained.'"[35]

While the government could arguably issue a subpoena to a third party to whom a person has knowingly disclosed the content of his records — i.e., the recipient of one's e-mail message, "because he maintains no expectation of privacy in the disclosure vis-a-vis that individual, and assumes the risk of that person disclosing (or being compelled to disclose) the shared information to the authorities," the Sixth Circuit held that if "the e-mail user does maintain a reasonable expectation of privacy in the content of the e-mails with respect to the ISP, then the Fourth Amendment's probable cause standard controls the e-mail seizure."[36] Because the Sixth Circuit ruled that an ISP user does maintain privacy in the content of his or her e-mails stored on an ISP server, it held that the Fourth Amendment's probable cause standard controls the seizure of e-mail absent prior notice to the user enabling judicial review of the government's action.

Absence of Particularization

The *ex parte* § 2703(d) orders and § 2703(b) subpoenas authorized by the Act and utilized by the government in *Warshak* present one additional grave concern — the complete and utter absence of the particularity required to prevent the exploratory rummaging through a citizen's private papers and effects that was such anathema to the Framers that they erected in the Fourth Amendment a prohibition against gen-

eral warrants.[37] At least in the context of administrative subpoenas, they are necessarily limited to the subject matter of the specific investigation that the agency is authorized by law to undertake and in pursuit of which it has been specifically authorized by Congress to issue administrative subpoenas, and the items sought must be relevant to that investigation. An administrative subpoena will be accompanied by a specific list of responsive documents, which may be challenged as irrelevant or overbroad. In *Warshak*, in exceedingly sharp contrast, the *ex parte* § 2703(d) orders and § 2703(b) subpoenas routinely compelled the production of *all* of the target's e-mails regardless of how far removed their content was from the subject matter of the government's investigation. Such a process obviously leaves the government in unchallenged possession of that content, free to read every word the target has written and every word that has been written to him, regardless of how intensely private and personal the content, and regardless of whether any of the communications are privileged attorney-client or spousal communications.

In *Warshak*, the Sixth Circuit noted that whether the government seized e-mail pursuant to a warrant supported by probable cause or compelled disclosure pursuant to a subpoena, it is not "necessarily entitled to every e-mail stored with the ISP, many of which are likely to be entirely unrelated to its specific investigation."[38] If the e-mails are seized pursuant to a warrant, the court noted, the Fourth Amendment's particularity requirement would necessitate that the scope of the search somehow be designed to target e-mails that could reasonably be believed to have some connection to the alleged crime being investigated. "Similarly, where a subpoena or an SCA order compels the disclosure of e-mails, the demand must be reasonable in scope and relevance. In either instance, a district court should consider whether the search could be narrowed by parameters such as the sender, recipient, date, relevant attachments, or keywords."[39]

The Government's Unilateral Modification of the 'Electronic Storage' Definition

Pursuant to the first sentence of § 2703(a), a governmental entity may require the disclosure by an ISP of the contents of a wire or electronic communication that is in *electronic storage* for 180 days or less, *only* pursuant to a judicially authorized warrant.[40] *Electronic storage* is defined in 18 U.S.C. § 2510(17) as: "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication."

In *Warshak*, the government sought and received orders issued to the ISPs advising that "unopened incoming communications less than 181 days old" were included within the definition of electronic storage and therefore were not within the purview of the order, but also commanded that "*[c]ommunications not in "electronic storage" include any e-mail communications received by the specified accounts that the owner or user of the account has already accessed, viewed, or downloaded.*" The consequences of the government's unilateral definition of *electronic storage* is that any and every e-mail communication opened by an account holder but then kept in his e-mail folder for backup purposes or later viewing (or for any other reason) would be produced to the government, whether or not it was less than 181 days old.

In essence, by excluding from the definition of electronic storage "any e-mail communications received by the specified accounts that the owner or user of the account has already accessed, viewed, or downloaded," regardless of whether those e-mail communications are more than or less than 180 days old, the Orders sought and secured by the government in the *Warshak* matter eviscerated the spirit and language of § 2703(a), which requires a search warrant for any e-mails in electronic storage for 180 days or less. While the definitional language included within the Orders reflects the Department of Justice's interpretation of the SCA as contained in their internal manual, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," it is an interpretation that was squarely rejected by the Ninth Circuit in the fairly recent case of *Theofel v. Farey-Jones*,[41] and frankly, is an interpretation that firmly undercuts the intent of Congress in enacting the SCA.

Theofel concerned a commercial litigation dispute amongst private parties, during which Farey-Jones sought access to his adversary's e-mail by serving an ISP (NetGate) with a subpoena pursuant to the Federal Rules of Civil Procedure.[42] NetGate eventually provided Farey-Jones with a "free sample" of 339 e-mail messages and the plaintiffs eventually filed a separate action against Farey-Jones, claiming that the defendant's subpoena violated the Stored Communications Act and various other laws.[43] Among other things, the defendants argued that e-mails that remain on an ISP's server after delivery no longer fall within the definition of electronic storage contained in 18 U.S.C. § 2510(17).[44] The United States, as *amicus curiae*, joined the defendant's argument, asserting the legal rationale that underlies the language in the orders secured by the government in *Warshak*: E-mails that are downloaded, accessed or viewed are no longer in "electronic storage." [45]

The Ninth Circuit concluded that "[t]here is no dispute that messages remaining on [an ISP's] server after delivery are stored 'by an electronic communication service' within the meaning of 18 U.S.C. § 2510(17)(B)."[46] Then the only issue, according to the Ninth Circuit, "is whether the messages are stored 'for purposes of backup protection.'"[47] Noting that an "obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again — if, for example, the message is accidentally erased from the user's own computer," the Ninth Circuit concluded that the ISP copy of the message functions as a "backup" for the user.[48] The Ninth Circuit rejected the contention that "backup protection" includes only temporary backup storage pending delivery, and not any form of "post-transmission storage." [49]

The Ninth Circuit did "not lightly conclude that the government's reading is erroneous," but it held that "prior access is irrelevant to whether the messages at issue were in electronic storage" and, ultimately, that the plaintiffs' e-mails were in electronic storage regardless of whether they had been previously delivered.[50] Hence, according to the Ninth Circuit, e-mail communications accessed by the user but stored on an ISP server for 180 days or less for backup purposes cannot be seized by the government without a warrant, as required by 18 U.S.C. § 2703(a).

The Ninth Circuit's decision in *Theofel* comports with the underlying purpose of the Electronic Communications Privacy Act of 1986 ("ECPA"), which included a broad definition of *electronic storage* to enlarge pri-

vacy protections for stored data.[51] Congress added the Stored Communications Act to the ECPA to halt potential intrusions on individual privacy, not with an intent to limit or curtail individual privacy.[52] "While drafting the ECPA's amendments to the Wiretap Act, Congress … recognized that, with the rise of remote computing operations and large databanks of stored electronic communications, threats to individual privacy extended well beyond the bounds of the Wiretap Act's prohibition against the 'interception' of communications", and so Congress added Title II to the ECPA.[53]

The government's interpretation of *electronic storage* essentially guts the warrant requirement of § 2703(a). Under the government's view of the statute, the only e-mails protected by the 180-day warrant requirement of § 2703(a) are those e-mails that reach a subscriber's mailbox, but are left untouched and unread for 180 days. In reality, this hardly, if ever, occurs. If the government's view is accepted, a subscriber would have Title III protection for an e-mail up to the point it is moved from the ISP server to his or her mailbox,[54] a subscriber would have § 2703(a) warrant protection only until he or she opens or accesses the e-mail, and from that point on, whether or not 180 days expire, the subscriber will have no more protection of his or her *content* e-mail than individuals have in their telephone numbers under the pen register provisions or account information, all of which is knowingly exposed to thousands of employees of various companies.[55] In short, the government's interpretation of *electronic storage* significantly curtails an individual's privacy interests in his or her stored communications, which cuts directly against the intent of Congress in enacting the SCA.

Delayed Notice Meant No Notice

Finally, there is grave concern that the United States abuses its authority to delay notice to the target of its investigations. Pursuant to the Act, where a court order is sought pursuant to § 2703(d), the government can delay notice to an aggrieved citizen for an initial 90-day period "if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result, i.e., endangering life or safety of an individual, flight from prosecution, destruction or tampering with evidence, intimidation of potential witnesses, or "otherwise seriously jeopardizing an investigation or unduly delaying trial."[56] Where the government seeks an administrative subpoena pursuant to § 2703(b), it can delay notice for an initial period of 90 days "upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have" the same adverse results.[57] Extensions of the delay of notification can be provided by the court, up to 90 days each, only upon application or by certification by a governmental entity, and only after making the necessary determinations.[58]

In the *Warshak* matter, the government never voluntarily provided Warshak with notice of the orders and subpoenas and it never bothered to comply with the terms of § 2705. Instead, attorneys for Warshak discovered on their own the likelihood of these investigatory techniques and demanded notice from the government. The very next day, the government provided notice that Warshak's e-mails had been seized pursuant to the SCA. As the district court observed in granting Warshak's request for a preliminary injunction:

> [I]t is not entirely clear whether the United States and the magistrate judge adhered to the letter of the delayed-notice provisions in keeping Warshak's NuVox and Yahoo orders under seal for a year and nine months, respectively. … There is no evidence of the[] periodic determinations [that continued sealing is necessary] in the docket for this case, or the magistrate's dockets for the NuVox and Yahoo seizures (obtained in hard copy by the court). Rather, it appears that the magistrate judge simply ordered the orders and the United States' applications for those orders "sealed until otherwise ordered by the court," and that they remained sealed for many multiples of 90 days until the United States moved, in late May 2006, for them to be unsealed.[59]

The lesson of the *Warshak* matter is that counsel should be vigilant — both preindictment and postindictment — in demanding notice from the government whether it has employed the SCA to unconstitutionally seize and search a client's e-mail communications.

Protecting Closed Containers

That the SCA authorizes the use of subpoenas and orders to obtain e-mails without a warrant is not in dispute; it plainly does. That the government actively employs the SCA to effect wholesale seizures of the e-mails of citizens is not in dispute. In *Warshak*, the government asserted that it has been utilizing the Act in similar fashion for 20 years. The issue is what the *Constitution* requires. Ultimately, it is the province of the courts to determine whether ISP-stored e-mails should be regarded, for purposes of the Fourth Amendment, as closed containers that cannot be searched absent a warrant issued upon probable cause.

The "balance" struck by Congress when e-mail and the Internet were still relatively new and used by few people is not automatically the "balance" which should be drawn when, as now, e-mail has evolved into the communication method of choice for millions of Americans.[60] And, ultimately, it is not a question of balance at all, but of what the Fourth Amendment requires in the context of seizure and search of the content of private ISP-stored e-mails. Like a sealed or resealed first-class letter, a closed filing cabinet, a sealed or resealed federal express package, or a closed unit within a storage facility, an e-mail stored on an ISP's server is a closed container in which an individual has a strong reasonable expectation of privacy, as the district court and Sixth Circuit concluded in the *Warshak* matter. Consequently, in accord with more than a century of Supreme Court jurisprudence, a closed e-mail stored within an ISP server should be afforded all of the Fourth Amendment protections conferred upon first-class mail and other closed containers.

Notes

1. Recently available statistics indicate that 68 percent of North America utilizes the Internet. The information about usage data, *World Internet Usage Statistics and Population Statistics*, is available at www.internetworldstats.com/stats.htm.

2. *See Ex Parte Jackson*, 96 U.S. 727, 733 (1878); *United States v. Van Leeuwen*, 397 U.S. 249, 251 (1970); *United States v. Jacobsen*, 466 U.S. 109 (1984).

3. The civil action *Warshak v. United States* (Civil No. 06-357), a case from the U.S.

District Court for the Southern District of Ohio, evolved out of a federal criminal investigation of the president and owner of Berkeley Premium Nutraceuticals Inc. Steven Warshak is represented by Martin G. Weinberg and Robert M. Goldstein, who along with Kimberly Homan authored the briefs that resulted in the opinions discussed in this article. Weinberg presented oral argument in both the district court and the U.S. Court of Appeals for the Sixth Circuit.

4. *See Warshak v. United States* (Civil No. 06-357, S.D. Ohio), Preliminary Injunction Order (Doc. No. 21), at 11, 18 ("Preliminary Injunction Order" herein).

5. *Warshak v. United States*, ____ F.3d ____, 2007 WL 1730094, at *13 (6th Cir., June 18, 2007).

6. *Warshak v. United States*, ____ F.3d ____, 2007 WL 1730094, at *13.

7. *Id.* at *13, 15.

8. 18 U.S.C. § 2703(a).

9. *See* 18 U.S.C. § 2703(a), (b)(1)(B)(i).

10. *See* 18 U.S.C. § 2703(a), (b)(1)(B)(ii), and (d).

11. *Ex Parte Jackson*, 96 U.S. 727, 733 (1878).

12. Id. *Accord, United States v. Van Leeuwen*, 397 U.S. 249 (1970).

13. *United States v. Jacobsen*, 466 U.S. 109, 114 (1984), citing *United States v. Chadwick,* 433 U.S. 1, 10 (1977); *United States v. Ross,* 456 U.S. 798, 809-812 (1982); *Robbins v. California,* 453 U.S. 420, 426 (1981) (plurality opinion); *Arkansas v. Sanders,* 442 U.S. 753, 762 (1979).

14. Preliminary Injunction Order at 9-10.

15. *See Jacobsen*, 466 U.S. at 113-114; *Walter v. United States*, 447 U.S. 649, 662 (1980).

16. *See Jacobsen,* 466 U.S. at 113-114; *see also Van Leeuwen*, 397 U.S. at 250-53 (upholding detention of mail while search warrant could be obtained).

17. *See Smith v. Ohio,* 494 U.S. 541 (1990); *United States v. Place,* 462 U.S. 696, 701 (1983); *Arkansas v. Sanders,* 442 U.S. 753 (1979); *United States v. Van Leeuwen,* 397 U.S. 249 (1970).

18. *Robbins,* 453 U.S. at 427.

19. Preliminary Injunction Order at 10, n.10.

20. *Warshak v. United States*, ____ F.3d ____, 2007 WL 1730094, at *13.

21. *Id.*

22. *Warshak v. United States*, ____ F.3d ____, 2007 WL 1730094, at *14 (emphasis in original).

23. *Id.*

24. *See, e.g., United States v. James*, 353 F.3d 606, 614 (8th Cir. 2003) (deciding an issue of consent, the court noted that Eighth Circuit law and law of other circuits indicates that one does not cede dominion over an item to another just by putting it in the possession of another; for example, a lessee does not have authority to consent to a search of the lessor's financial records stored at the leased house merely on account of the lessor-lessee relationship); *United States v. Dowler*, 940 F.2d 1539 (10th Cir.1991) (unpublished decision) (before leaving state, appellant placed documents in boxes, file cabinet and briefcases, which were then stored by apartment manager at request of appellant's agent; held that appellant manifested an expectation that the documents would remain private and free from inspection, and that appellant's expectation of privacy and protection from a wrongful search and seizure continued into the creation of the bailment by the apartment manager and her agent); *United States v. Fultz,* 146 F.3d 1102 (9th Cir.1998) (defendant who lived "on and off" with his friend and stored many of his belongings in closed boxes in friend's garage had a reasonable expectation of privacy in his belongings, even though those belongings were kept in a place that was *not* exclusively controlled by him).

25. *Warshak v. United States*, ____ F.3d ____, 2007 WL 1730094, at *14.

26. *Id.*

27. 425 U.S. 435, 443 (1976).

28. *Id.* at 441-443. *See also Donaldson v. United States,* 400 U.S. 517, 522 (1971) (Internal Revenue summons directed to third party does not trench upon any interests protected by the Fourth Amendment).

29. *Id.* at 442.

30. *Id.* at *443.*

31. *Id.* at 442.

32. *See United States v. Capital Triumph Group*, 211 F.R.D. 31 (D. Conn. 2002) (government obtained laptop through grand jury subpoena but obtained warrant before searching it); *see also Davis v. Gracey*, 111 F.3d 1472, 1483 (10th Cir. 1997) (assuming, without deciding, that additional warrant would be required to access the content of e-mails in bulletin board on seized computers).

33. *See United States v. Barr*, 605 F.Supp. 114 (S.D.N.Y. 1985) (government obtained unopened mail through grand jury subpoena but obtained search warrant before opening it). *See also Wilson v. Moreau*, 440 F.Supp.2d 81, 108 (D.R.I. 2006) (police could not search library patron's private e-mail account, which he accessed through public library computers, without either a warrant or valid consent).

34. *Warshak v. United States*, ____ F.3d ____, 2007 WL 1730094, at *8.

35. *Id.*

36. *Id.* at *9.

37. *See United States v. Upham,* 168 F.3d 532, 535 (1st Cir. 1999).

38. *Id.* at *n.8.

39. *Id.*

40. 18 U.S.C. § 2703(a).

41. 359 F.3d 1066 (9th Cir. 2004).

42. *Id.* at 1071.

43. *Id.* at 1071-72.

44. *Id.* at 1075.

45. *Id.* at 1075-77.

46. *Id.* at 1075.

47. *Id.,* quoting 18 U.S.C. § 2510(17)(B).

48. 359 F.3d at 1075. The Ninth Circuit's conclusions are supported by the 1986 study of privacy implications of electronic surveillance conducted by the Congressional Office of Technology Assessment in connection with the intent of Congress to amend the electronic surveillance statutes. The report, known as the OTA Report, concluded that e-mail messages retained on the service provider's computers after transmission are primarily retained for "billing purposes and as a convenience in case the customer loses the message." *See United States v. Councilman*, 418 F.3d 67, 76, 77 (1st Cir. 2005).

49. 359 F.3d at 1075. *See also Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623, 635-36 (E.D. Pa. 2001), holding such a view "as contrary to the plain language of the Act."

50. 359 F.3d at 1077.

51. *See United States v. Councilman,* 418 F.3d 67, 76 (1st Cir. 2005) (finding that "the purpose of the broad definition of electronic storage was to enlarge privacy protections for stored data under the Wiretap Act, not to exclude e-mail messages stored during transmission from those strong protections.").

52. *Councilman,* 418 F.3d at 80-81.

53. *Id.*

54. *Id.* at 76-77.

55. *Cf. Smith v. Maryland,* 442 U.S. 735 (1979) (holding that the installation and use of a pen register does not constitute a Fourth Amendment search because a caller has no reasonable expectation of privacy in the numbers dialed from his or her phone).

56. 18 U.S.C. § 2705(a)(1)(A).

57. 18 U.S.C. § 2705(a)(1)(B).

58. 18 U.S.C. § 2705(a)(4).

59. Preliminary Injunction Order at 17, n.18.

60. In addition, the "balance" struck by Congress makes no sense. Congress extended the full protection of the warrant clause of the Fourth Amendment to e-mails in electronic storage for 180 days or less, but permitted the government to obtain e-mails in electronic storage for 181 days or more through subpoena or court order. Why Congress drew such an arbitrary demarcation is not revealed. An e-mail message that is one year old is no less worthy of

Fourth Amendment protection than is a message that is a day old. Permitting the seizure of an e-mail that is 181 days old via § 2703 orders or subpoenas, but requiring a warrant based on probable cause for one that is 179 days old, is a distinction without constitutional foundation or principle.

About the Authors

Martin G. Weinberg, a nationally prominent criminal defense lawyer whose offices are in Boston, Mass., is currently counsel for Steve Warshak in the civil and criminal proceedings referenced in this article. He is co-chair of NACDL's Lawyers Assistance Strike Force, and has represented accused defendants in over twenty federal district courts and eight federal courts of appeals. In the U.S. Supreme Court, he successfully argued *United States v. Chadwick*, a landmark Fourth Amendment case.

Martin G. Weinberg
20 Park Plaza, Suite 905
Boston, MA 02116
617-227 3700
Fax 617-338 9538
E-MAIL owlmcb@att.net

Robert M. Goldstein is co-counsel for Steve Warshak in the civil and criminal proceedings referenced in this article. Over the course of his career, he has successfully defended clients in a broad range of government investigations and prosecutions, including health care fraud, public corruption, financial fraud, tax matters, export control violations, and environmental matters. He was selected by his peers as a 2007 Massachusetts Super Lawyers "Rising Star" in the area of white collar criminal defense.

Robert M. Goldstein
20 Park Plaza, Suite 903
Boston MA 02116
617-742-9015
Fax 617-742-9016
E-MAIL rmg@goldstein-lawfirm.com