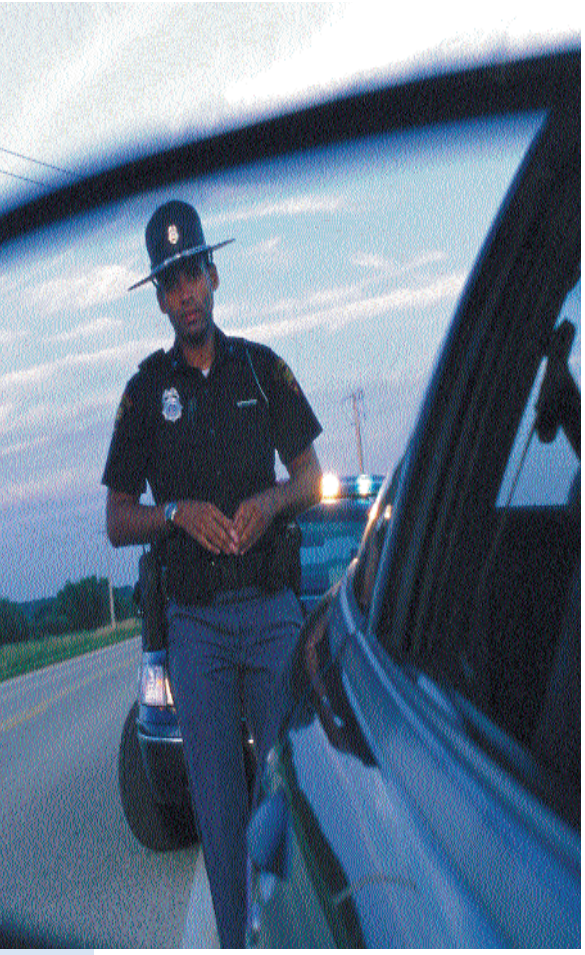

Search & Seizure Commentary

BY MARTIN G. WEINBERG AND ROBERT M. GOLDSTEIN

Warshak 4 Years Later

The DOJ Continues to Fight The *Warshak* Court Requirement Of a Warrant (Not a Subpoena) To Search and Seize Emails

In *United States v. Warshak*,[1] the Sixth Circuit held that the government's *warrantless* seizure of Steven Warshak's emails, while held in storage by his Internet Service Provider ("ISP"), violated the Fourth Amendment. The government argued, unsuccessfully, that the Stored Communications Act facially permits the seizure of a citizen's emails from an ISP through subpoena or court order (*i.e.*, without a warrant) if the emails are more than 180 days old or if they are in "remote" storage, which the government defined, without statutory authority, as including all emails downloaded and opened by the receiver.[2] According to the *New York Times*, however, the government continues to construe the Act as permitting it "to read email and cloud-stored data over six months old without a search warrant," a position that "is under attack from technology companies, trade associations and lobbying groups, which are pressing Congress to tighten privacy protections."[3] While the Department of Justice presumably honors the *Warshak* decision within the Sixth Circuit, the reported use of subpoenas or orders, rather than warrants, in all other jurisdictions raises significant privacy concerns. While "Silicon Valley giants like Facebook, Twitter and Google say they will no longer hand over their customers' data without a search warrant," a position that likely derives from the *Warshak* decision, it appears that "smaller Web hosting and cloud computing companies may be outmuscled by law enforcement officials," because they either do not know their rights or do not have the resources to fight the government (or, perhaps, both).[4]

The Sixth Circuit is not alone in applying the Fourth Amendment to modern technological advances. In the highly publicized matter of *Klayman v. Obama, et al.*,[5] Judge Leon ruled a substantial likelihood existed that he will eventually hold that the government's warrantless bulk collection and analysis of telephony data pursuant to Section 215 of the Patriot Act violates the Fourth Amendment.[6] Neither *Warshak* nor *Klayman* should be surprising if one considers the fundamental question that underpins the relevant Fourth Amendment inquiry: whether *society* is prepared to recognize as "reasonable" a citizen's "subjective expectation" of privacy in the technological communicative tools of modern society.[7] Just as an 18th century American citizen did not reasonably expect that his letters would be opened and searched by the then-nascent government, today's American does not reasonably expect that his every email can be seized and read, indiscriminately, by the government, with no independent scrutiny by a detached, neutral magistrate that probable cause exists to believe the citizen has engaged in criminal wrongdoing, and that the emails at issue — often many thousands of emails authored over many years on many subjects — would be seized without any attempt to conform to the particularization imperatives of the Fourth Amendment. Likewise, a citizen does not reasonably expect her government to indiscriminately collect, retain and analyze all of her telephone data, without detached judicial review.[8]

In both *Warshak* and *Klayman*, each court wisely rejected the government's reliance upon *Smith v. Maryland*[9] and *United States v. Miller*,[10] two cases decided in the 1970s, well before anyone could remotely predict the "vital role" email and cellphones have come to play in modern society.[11] Societal expectations undeniably change over time. As Judge Leon observed in rejecting the government's reliance upon *Smith*, "the evolutions in the government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies" have "become so thoroughly unlike those considered by the Supreme Court 34 years ago that a precedent like *Smith*" no longer controls the inquiry, for the *Smith* Court could never imagine "how the citizens of 2013 would interact with their phones," nor "the almost-Orwellian technology that enables the government to store and analyze the phone metadata of every telephone user in the United States. …"[12] Or, as Judge Martin mused in concluding his dissent in a predecessor decision in the Warshak litigation (where a divided *en banc* court ordered Warshak's declaratory judgment civil suit dismissed on standing grounds), "[i]f I were to tell James Otis and John Adams that a citizen's private correspondence is now potentially subject to

Editor's Note: The authors, Martin G. Weinberg and Robert M. Goldstein, served as counsel for the defendant in *United States v. Warshak*. This piece updates their March 2011 article published in *The Champion*.

ex parte and unannounced searches by the government without a warrant supported by probable cause, what would they say? Probably nothing, they would be left speechless."[13]

The Supreme Court has previously acknowledged that a new Fourth Amendment analysis, and result, may be warranted given the passage of time. In 1928, in *Olmstead v. United States*,[14] where law enforcement officers intercepted messages by inserting "small wires" along "ordinary telephone wires" from the defendants' residences and an office, "without trespass upon any property of the defendants," the Court held that the "wire tapping [t]here disclosed did not amount to a search or seizure within the meaning of the Fourth Amendment."[15] Thirty-nine years later, in *United States v. Katz*,[16] where the Court held unlawful a government agent obtaining "the petitioner's end of telephone conversations" by attaching "an electronic listening and recording device to the outside of the public telephone booth" used by the defendant, the Court observed "that the underpinnings of *Olmstead* [ ] have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling."

Today, cellphones and email accounts house as much, if not more, private information as the homes or commercial warehouses that were central to the formative concerns of colonial ancestors that led to the framing of the Fourth Amendment.[17] For example, as Judge Leon observed, today's society shares "an entirely different relationship with phones than they did 34 years ago," and the "rapid and monumental shift towards a cellphone-centric culture means that the metadata from each person's phone 'reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.'"[18] The same observation holds true for emails as well. This "monumental shift" renders the holdings of *Miller* and *Smith* inapposite. Indeed, in *Warshak*, the Sixth Circuit noted that *Miller* involved "simple business records, as opposed to the potentially unlimited variety of 'confidential communications' at issue" with email.

The analyses employed and conclusions reached, by both the Sixth Circuit in *Warshak* and Judge Leon in *Klayman*, are highly persuasive. Indeed, the Department of Justice was acutely aware of the issues raised in the *Warshak* appeal, having participated in the appellate process along with the local U.S. Attorney's Office, yet no appeal was pursued. One could reasonably infer the government feared an appeal could potentially result in a nationwide application of the *Warshak* principles — *i.e.*, the full application of the Fourth Amendment's Warrant Clause to the practice of subpoenaing or otherwise acquiring the content of one's emails from an ISP (often accompanied by a corollary order prohibiting the ISP from notifying the customer of the subpoena or warrantless seizure). The *New York Times* article, discussed above, indicates that strategy is paying dividends, at least with smaller companies without the knowledge or resources to contest the government's subpoenas. To this date, there is no legislation codifying the *Warshak* decision (despite efforts in the Senate Judiciary), and there has been no change of the DOJ manual.[19] The import of the *Warshak* decision to, and its impact upon, the government's view of its national security powers is undeniable; indeed, the *Warshak* decision has made its way into the assigned course book for the National Security Law class at Harvard Law School, and has been the subject of numerous law review articles and legal blog discussions about the intersection of the Fourth Amendment and electronic and Internet seizures.[20]

The *Warshak* and *Klayman* decisions portend future rulings by the Supreme Court, should these issues ultimately wind their way to the top court, particularly if one considers Justice Sotomayor's observation, in her concurring opinion in *United States v. Jones*, that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[21]

On June 25, 2014, the U.S. Supreme Court, in a 9-0 decision, *Riley v. California*,[22] conclusively determined that warrantless cellphone searches incident to arrest were, absent exigent circumstances, prohibited by the Fourth Amendment. The Court distinguished cellphones from other properties that had traditionally been subject to seizure in relation to an arrest because of their immense storage capacity and the breadth of information they contain, noting that a cellphone discloses the "sum of an individual's private life"[23] which, if subject to warrantless search, would compromise the "privacies of life."[24] The Court's unanimous holding that warrantless searches of cellphones incident to arrest are not reasonable is a hopeful sign that the justices are open to similarly protecting the content of emails by requiring a warrant before they are accessed.

While "GPS monitoring generates a precise, comprehensive record of a person's public movements," which reflects "a wealth of detail about her familial, political, professional, religious and sexual associations,"[25] the government's collection, storage and examination of every call placed by an individual, or every email written or sent, with perhaps no end to that collection, creates a more detailed and far more comprehensive record of that person's associations and beliefs. Collection and indefinite retention, combined with sophisticated computer analytical tools available to government agents, undoubtedly provide the government with the ability to erect a detailed roadmap of a citizen's life, which is likely the reason the program has become an effective tool for the government. Yet in the end, it seems elemental that society would view an expectation of privacy in these materials as reasonable.

Open-ended seizures of emails or unlimited collection and analysis of cellphone records are akin to a General Search. Unlike wiretapping, there is no minimization. Unlike a warrant, there is no attempt to comport with the Particularization Clause of the Fourth Amendment. The government practice of obtaining emails from ISPs — often years of stored emails — and/or collecting and analyzing cellphone records constitutes a massive invasion of privacy and must be subject to the ordinary limits that prevent the use of general warrants.[26] Finally, it should be noted that upholding as reasonable society's expectation of privacy in these communicative tools does not unduly frustrate the government's ability to effectively secure society. There are other avenues available to the government. For example, the government can secure a warrant from a detached and neutral magistrate. Or, when "special needs" exist beyond routine law enforcement, the government could advocate there exists an exception to the Fourth Amendment warrant requirement, such as the area of national security.[27]

Notes

1. 631 F.3d 266 (6th Cir. 2010).

2. *See* 18 U.S.C. § 2703(a)-(f).

3. Elena Schneider, *Technology Companies Are Pressing Congress to Bolster Privacy Protections*, N.Y. Times, May 26, 2014, *available at* http://www.nytimes.com/2014/05/27/us/technology-firms-press-con-

gress-to-tighten-privacy-law.html?_r=0 (last viewed June 1, 2014).

4. *Id*.

5. 957 F. Supp. 2d 1 (D.D.C., Dec. 16, 2013).

6. In *ACLU v. Clapper*, 959 F. Supp. 2d 724 (S.D.N.Y., Dec. 27, 2013), Judge Pauley reached a contrary conclusion. Congress is currently drafting legislation that may, if passed, moderate but not eliminate the invasions concomitant to this policy.

7. *See, e.g., Warshak*, 631 F.3d at 285 (the "Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish"), citing *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (noting that evolving technology must not be permitted to "erode the privacy guaranteed by the Fourth Amendment); *Warshak*, 631 F.3d at 284 ("societal" question was "of grave import and enduring consequence, given the prominent role that email has assumed in modern communication").

8. Judge Leon's analytical structure mirrors that employed in the *Warshak* decision. He framed the issue confronted by the court as follows: "whether plaintiffs have a reasonable expectation of privacy that is violated when the government indiscriminately collects their telephony metadata along with the metadata of hundreds of millions of other citizens without any particularized suspicion of wrongdoing, retains all of that metadata for five years, and then queries, analyzes, and investigates that data without prior judicial approval of the investigative targets." *Klayman*, 957 F. Supp. 2d at 30.

9. 442 U.S. 735 (1979).

10. 425 U.S. 435 (1976).

11. *Katz*, 389 U.S. at 352 (suggesting that the Constitution must be read to account for "the vital role that the public telephone has come to play in private communication").

12. As noted *supra*, in *ACLU v. Clapper*, Judge Pauley reached a contrary conclusion, finding *Smith* controlling, and observing that *Smith's* "bedrock holding is that an individual has no legitimate expectation of privacy in information provided to third parties." *Clapper*, 959 F. Supp. 2d at 749.

13. *Warshak v. United States*, 532 F.3d 521, 538 (6th Cir. 2008).

14. 277 U.S. 438 (1928).

15. *Olmstead*, 277 U.S. at 456-57, 464, 466.

16. 389 U.S. 347 (1967).

17. *Warshak* 631 F.3d at 284 ("'account' is an apt word for the conglomeration of stored messages that comprises an email account, as it provides an account of its owner's life").

18. *Klayman*, 957 F. Supp. 2d at 36, *quoting Jones*, 132 S. Ct. at 955.

19. Absent legislation or uniform acceptance of *Warshak*, there is also the risk that the government serves subpoenas, warns the ISP not to disclose, and then uses the information for investigation only, thus avoiding the risks of post-*Warshak* litigation.

20. *See* Stephen Dycus, Arthur L. Berney, William C. Banks & Peter Raven-Hansen, National Security Law, Chapter 23 (5th ed. 2011).

21. *United States v. Jones*, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

22. *Riley v. California*, 134 S. Ct. 2473 (2014).

23. *Id. at 2489.*

24. *Id.* at 2495.

25. *Jones*, 132 S. Ct. at 955.

26. *See, e.g., Matter of the Search of Information Associated with [redacted]@ mac.comthat is Stored at Premises Controlled by Apple, Inc.*, — F. Supp. 2d —, 2014 WL 945563 (D.D.C., March 7, 2014) ("Despite this court's repeated prior warnings about the use of formulaic language and overbroad requests that — if granted — would violate the Fourth Amendment, this court is once again asked by the government to issue a facially overbroad search and seizure warrant.") (rejecting application for a search and seizure warrant pursuant to Rule 41 and 18 U.S.C. § 2703(a), (b) and (c) to disclose certain records and contents of electronic communications relating to an Apple email address because it failed to clearly specify which emails it sought to seize and because it sought authorization to seize emails for which it had not established probable cause to seize); *Matter of Search of Information Associated with [Redacted]@ mac.com that is Stored at* , — F. Supp. 2d —, 2014 WL 1377793 (D.D.C., April 07, 2014) (again rejecting application).

27. *See, e.g., In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1011 For. Intel. Surv. Rev. (August 22, 2008) ("The question, then, is whether the reasoning of the special needs cases applies by analogy to justify a foreign intelligence exception to the warrant requirement for surveillance undertaken for national security purposes and directed at a foreign power or an agent of a foreign power reasonably believed to be located outside the United States. Applying principles derived from the special needs cases, we conclude that this type of foreign intelligence surveillance possesses characteristics that qualify it for such an exception."). ■

About the Authors

Martin G. Weinberg is co-chair of NACDL's Lawyers Assistance Strike Force. 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 1000
Boston, MA 02116
617-227-3700
Fax 617-338-9538
E-MAIL owlmgw@att.net

Robert M. Goldstein has successfully defended clients in a broad range of government investigations and prosecutions, including health care fraud, public corruption, financial fraud, tax matters, and export control violations.

Robert M. Goldstein
20 Park Plaza, Suite 1000
Boston, MA 02116
617-742-9015
Fax 617-742-9016
E-MAIL rmg@goldstein-lawfirm.com