BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

Sixth Circuit Finds Stored Communications Act Unconstitutional, Providing Further Momentum for ECPA Reform, Possible Supreme Court Review

By Amy E. Worlton and Megan L. Brown

Amy E. Worlton, a partner in Wiley Rein LLP's Privacy Practice in Washington, advises a broad range of U.S. and foreign companies and institutions on privacy, security, economic sanctions, telecommunications, internet and e-commerce issues. Worlton can be reached at 202.719.7458 or aworlton@wileyrein.com.

Megan L. Brown, a partner in Wiley Rein's Litigation and Appellate Practices, has significant experience representing clients in litigation and appellate matters in state and federal courts across the country and before various federal agencies. Brown can be reached at 202.719.7579 or mbrown@wileyrein.com.

A recent decision by the United States Court of Appeals for the Sixth Circuit invalidating part of the Stored Communications Act (SCA) casts doubt on law enforcement's ability to access e-mail communications without a warrant, and renews questions about updating the Electronic Communications Privacy Act (ECPA). This decision is likely to be reviewed by the *en banc* Sixth Circuit, and may eventually present the U.S. Supreme Court with questions about the constitutionality of the SCA. As such, it is an important case for law enforcement, service providers and privacy advocates interested in the particular issues presented and ECPA reform generally.

In *United States v. Warshak*, 2010 WL 5071766 (Dec. 14, 2010) (9 PVLR 1731, 12/20/10), the Sixth Circuit ruled that the Fourth Amendment to the federal Constitution prevents law enforcement from obtaining stored e-mail communications without a warrant based on a showing of probable cause. Accordingly, the court held that the provision of the SCA, 18 U.S.C. §§ 2701 *et seq.*, a part of the ECPA, that permits warrantless government access to certain stored e-mails, is unconstitutional. The decision may influence the way in which electronic communications service providers-such as Internet Service Providers (ISPs) and social networking sites-handle their obligations to government investigators under the SCA. More fundamentally, the decision serves as yet another indication of the need for clarification of the ECPA.

ECPA Reform Is Under Consideration

The *Warshak* panel opinion is but the latest manifestation of the frustrations voiced by several courts and

commentators with the SCA and the ECPA, which many feel cannot comfortably govern modern technologies that sit uncomfortably with critical statutory categories. As one Court of Appeals observed almost a decade ago, ''the [SCA] was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communication . . . . Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results.'' *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002). And a panel of the First Circuit noted, ''[i]t may well be that the protections of the Wiretap Act have been eviscerated as technology advances.'' *U.S. v. Councilman*, 373 F.3d 197, 203 (1st Cir. 2004) (3 PVLR 784, 7/5/04), opinion vacated on rehearing en banc, 418 F.3d 67 (1st Cir. 2005). Several courts have remarked on the rapidly changing technology landscape, consumers' expectations of privacy in now-pervasive technologies and the seeming inadequacy of the existing legal regime. ''[T]he statutory framework governing online communication is almost a quarter century old and has not been amended to keep pace with changes in technology since that time.'' *Crispin v. Christian Audigier, Inc.*, 717 F. Supp.2d 965, 972 (C.D.Cal. 2010).

This arguably poor fit between evolving technology and a complicated statutory framework generates legal uncertainty as to the proper status and treatment of certain communications. Against this backdrop of uncertainty, service providers need clarity about their obligations and immunities, but the plain text provides little comfort and there are few occasions for judicial clarification. The typical vehicles for guidance come through efforts by criminal defendants to exclude evidence or overturn convictions. Such endeavors often shed little light on the implications for private parties trying to navigate the complex and murky requirements and prohibitions in the SCA and related statutes.

The ECPA was enacted in 1986, and provides standards for law enforcement access to electronic communications and associated data. It struck a balance between privacy protections for emerging technologies and the needs of law enforcement. But, many argue that because technologies have advanced dramatically since 1986, the ECPA has been outpaced and is outmoded. Various proposed amendments to the ECPA presently are under consideration. Some privacy advocates, major companies and think tanks have formed a policy coalition to advance what they see as needed reforms to the ECPA. *See http://www.digitaldueprocess.org.* Hearings on ECPA were held in late September 2010. *See* Hearing on the Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Act Before the S. Comm. on the Judiciary, 111th Cong. (Sept. 22, 2010); Hearing on ECPA Reform and the Revolution in Cloud Computing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary, 111th Cong. (Sept. 23, 2010).

It presently is unclear what reforms, if any, are likely to be enacted. But the *Warshak* decision will continue the ongoing debate over appropriate changes to the ECPA.

The Sixth Circuit's Decision: A Recap

In *Warshak*, the Sixth Circuit was reviewing the criminal convictions of Steven Warshak and others that arose from the fraudulent sale of supplements to consumers, which, the Court of Appeals reported, once grossed $250 million annually. Warshak was convicted on numerous counts, including mail fraud, bank fraud, money laundering and conspiracy, among others. He had been sentenced to 25 years of imprisonment and ordered to forfeit over $500 million.

Warshak raised numerous arguments on appeal, as to which the court reported 14 holdings. Although Warshak prevailed on some points, his conviction was largely upheld. The contention receiving first (and the most) attention in Judge Boggs' opinion related to the government's having obtained from an ISP, by subpoena, some 27,000 of Warshak's e-mails without his knowledge or permission.

Access to Stored Email Must be Based on Probable Cause

Warshak asserted that his e-mails had been accessed improperly by federal government investigators, despite the issuance of a subpoena under Section 2703(b) of the SCA. Reaching a decision foreshadowed by earlier Sixth Court rulings in the same case (*Warshak v. U.S.*, 490 F.3d 455 (6th Cir. 2007), vacated by *Warshak v. U.S.*, 532 F.3d 521 (6th Cir. 2008) (*en banc*)), the panel agreed with the defendant that an SCA subpoena was insufficient. Judge Boggs wrote:

> [A] subscriber enjoys a reasonable expectation of privacy in the contents of emails 'that are stored with, or sent or received through, a commercial ISP'. . . . The government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause.
>
> Therefore, because they did not obtain a warrant, the government agents violated the Fourth Amendment when they obtained the contents of [the defendant's] e-mails. Moreover, to the extent that the SCA purports to permit the government to obtain such e-mails warrantlessly, the SCA is unconstitutional.

Service providers governed by the SCA, particularly those with operations in the Sixth Circuit (Michigan, Ohio, Kentucky and Tennessee), should consider how the Sixth Circuit's opinion affects their compliance protocols. Service providers are expected to comply with properly issued government demands for assistance. *See, e.g.*, 18 U.S.C. 2703(c). To facilitate that cooperation, the SCA grants service providers immunity from lawsuits where they have complied in good faith with orders issued under statute, such as the subpoena issued in *Warshak*. See 18 U.S.C. § 2703(e).

The Sixth Circuit's analysis, which indicates that certain disclosures may be unconstitutional notwithstanding a facially valid subpoena, does not address service providers' immunity under Section 2703(e) or Section 2707(e). It does analyze the government agents' good-faith reliance on the unconstitutional SCA subpoena provision as a sufficient reason for affirming the trial court's refusal to exclude the evidence secured using that SCA subpoena. Indeed, the panel's conclusion that the agents acted in good-faith makes its resolution of the Fourth Amendment question all the more noteworthy. As the panel explained, ''[t]he doctrine of good-faith reliance should not be a perpetual shield against

  PVLR ISSN 1538-3423

the consequences of constitutional violations. In other words, if the exclusionary rule is to have any bite, courts must, from time to time, decide whether statutorily sanctioned conduct oversteps constitutional boundaries.'' Judge Boggs went on to note, ''Of course, after today's decision, the good-faith calculus has changed, and a reasonable officer may no longer assume that the Constitution permits warrantless searches of private emails.''

Though the panel did not address service providers' potential liability, the decision could affect their immunity by calling into question the legality of a subpoena on which that immunity is predicated. Because statutory immunity could thus be compromised, providers may need to consider whether revisions to their law enforcement assistance protocols are necessary or appropriate.

Prospective Data Retention Questioned in a Concurrence

Another aspect of this case is noteworthy for companies that may receive law enforcement assistance requests. In a separate concurrence, Judge Keith went out of his way to express unease about the use by the government of preservation requests to secure the retention of e-mails on a going-forward basis (an issue that Warshak did not appeal). By way of background, Section 2703(f) requires that a provider of wire or electronic communication services ''upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.'' 18 U.S.C. § 2703(f). In the *Warshak* case, the government served a request on the service provider to preserve the defendant's e-mails *in the future*. Those e-mails would not otherwise have been preserved by the ISP. The government later subpoenaed those e-mails under Section 2703(b).

Judge Keith expressed skepticism about the government's use of the Section 2703(f) preservation request prospectively, opining that such use appears to evade the heightened legal requirements for the *prospective* gathering of information, as set forth in the Pen Register Statute and Wiretap Act. He wrote that, in the ordinary course:

> The provider would have destroyed Warshak's old emails but for the government's request that they maintain all current and prospective emails for almost a year without Warshak's knowledge. In practice, the government used the statute as a means to monitor Warshak after the investigation started without his knowledge and without a warrant. Such a practice is no more than back-door wiretapping. I doubt that such actions, if contested directly in court, would withstand the muster of the Fourth Amendment.

In his view, ''their policy likely exceeded the parameters of § 2703(f)'' and such ''a policy whereby the government requests emails prospectively without a warrant deeply concerns me.'' His concern partly reflected that the use of § 2703(f) prospectively is rejected by the Department of Justice's computer-surveillance manual, as well as by several federal district court decisions. Service providers should be aware of this view and carefully consider requests that seem to be prospective in nature.

The Panel Opinion Is Likely to Be Subject to *En Banc* Proceedings, and Could Be Headed to the Supreme Court

Both sides in *Warshak* sought additional time in which to file petitions for *en banc* rehearing, which were due Jan. 27. *En banc* proceedings seem likely in this case. The *en banc* Sixth Circuit has already had a heated battle over Warshak's claims that the government improperly accessed his e-mails. In 2008, a sharply divided *en banc* court reviewed and vacated a preliminary injunction obtained by Warshak preventing the government from obtaining his e-mails. *See Warshak v. U.S.*, 532 F.3d 521 (6th Cir. 2008). In the earlier proceeding, Warshak, while still a suspect, had learned of the government's request for his e-mails and sought declaratory and injunctive relief against the United States, alleging that the government's compelled disclosures of his e-mails without a warrant violated the Fourth Amendment and the SCA. The United States District Court for the Southern District of Ohio had granted his request and enjoined the government from using § 2703(d) to seize the contents of ''any personal email account [ ]'' belonging to Warshak or ''any resident of the Southern District of Ohio'' without ''prior notice and an opportunity to be heard.'' *Id.* at 523. A panel of the Sixth Circuit had largely affirmed that injunction in 2007, *see Warshak v. U.S.*, 490 F.3d 455 (6th Cir. 2007), but the *en banc* Sixth Circuit vacated that decision, concluding that the issue was not ripe for adjudication and noting the sweeping and improper breadth of the District Court's injunction.

Five judges dissented in a separate opinion notable for its heated tone. ''Apparently taking a page from the Supreme Court, today the majority dismisses this case by concluding that it is not ripe for adjudication. Why do today what can be done tomorrow? I dissent because I not only believe this case is ripe for review, but because the majority gives unwarranted deferential treatment to the government.'' *Id.* at 534. The dissenters lamented that this case

> is but another step in the ongoing degradation of civil rights in the courts of this country. . . . History tells us that it is not the fact that a constitutional right is at issue that portends the outcome of a case, but rather what specific right we are talking about. If it is free speech, freedom of religion, or the right to bear arms, we are quick to strike down laws that curtail those freedoms. But if we are discussing the Fourth Amendment's right to be free from unreasonable searches and seizures, heaven forbid that we should intrude on the government's investigatory province and actually require it to abide by the mandates of the Bill of Rights.

Id. at 538.

It seems likely that the *en banc* Court remains interested in this case, and petitions filed by the government and Warshak will be closely examined, both by the Court of Appeals and by those interested in ECPA reform. Given the Sixth Circuit's history with Warshak's claims and the importance of these issues to law enforcement agencies and service providers, a petition for rehearing stands a good chance of being granted. And, depending on the outcome at the Court of Appeals, the Supreme Court could well be asked to evaluate Warshak's claims concerning the constitutionality of the SCA. As a result, this case will be closely followed by practitioners, service providers and privacy advocates to see how it informs the debate over ECPA reform.