wiley

NEWSLETTER

Sixth Circuit Holds Probable Cause Warrant Required for Private Email

January 2011

In *United States v. Warshak*, 2010 WL 5071766 (Dec. 14, 2010), the U.S. Court of Appeals for the Sixth Circuit ruled that the Fourth Amendment prevents law enforcement from obtaining stored email communications without a warrant issued based on a showing of probable cause. Accordingly, the court held to be unconstitutional, the provision of the Stored Communications Act (SCA), 18 U.S.C. § § 2701 *et seq.*, a part of the Electronic Communications Privacy Act (ECPA), that permits warrantless government access to certain stored emails. The Sixth Circuit decision has several notable elements that may affect 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. It serves as yet another indication of the need for clarifying amendments to the ECPA.

In this decision, the Sixth Circuit reviewed the criminal convictions of Steven Warshak and others that arose from a highly successful business based on 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 emails without his knowledge or permission.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Probable Cause Needed to Access Email

Warshak contended that his emails 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] emails. Moreover, to the extent that the SCA purports to permit the government to obtain such emails 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). 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 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 any 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

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 emails 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 emails *in the future*. Those emails would not otherwise have been preserved by the ISP. The government later subpoenaed those emails 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.

ECPA Reform Needed

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). 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).

There are few occasions for judicial clarification on matters of this sort, and the typical vehicles for guidance-efforts by criminal defendants to exclude evidence or overturn convictions-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. If the legal system is to provide certainty about the rights and obligations of electronic communications service providers, law enforcement and individuals, revisions to the ECPA appear necessary. Various proposed amendments to the ECPA presently are under consideration, and the *Warshak* decision likely will stimulate such deliberations.