Office of Chief Counsel
Internal Revenue Service
memorandum

Number: **201141017**
Release Date: 10/14/2011

CC:PA:07
POSTS-110431-11

UILC: 7602.03-00

date: July 08, 2011

to: Associate Area Counsel (Newark, Group 1)
(Small Business/Self-Employed)

from: William V. Spatz,
Senior Counsel, Branch 6
(Procedure & Administration)

---

subject: Summons Inquiry Regarding the Stored Communications Act
(18 U.S.C. §§ 2701-2711)

This Chief Counsel Advice responds to your request for assistance. This advice may not be used or cited as precedent.

ISSUES

1. Should the Service's administrative summons seeking from an Internet service provider (ISP) the contents of a customer's e-mails that are less than 180 days old,-- i.e., the summons requests all e-mails from a specified date through the date of the ISP's compliance with the summons – be withdrawn as inconsistent with the Stored Communications Act (18 U.S.C. §§ 2701-2711)?

2. Would it be sensible under the circumstances – in which the ISP is headquartered in the Ninth Circuit and the revenue officer is interested primarily in obtaining very recent leads to the taxpayer's potential assets from the contents of the e-mails at issue – for the Service to reissue a modified administrative summons on the ISP for the contents of the customer's e-mails that are more than 180 days old, i.e., from a specified date until another specified date that is more than 180 days before the issue date of the new summons?

3. May the revenue officer issue a modified administrative summons to the ISP for the non-content information for electronic communications services specified in 18 U.S.C.

§ 2703(c)(2) for the customer (e.g., name, address, length and type of service, and means of payment), as referred to in IRM Exhibit 5.20.4-10 (rev. 7-20-2010)?

CONCLUSIONS

1. Yes, the summons the Service issued to the ISP should be withdrawn for violating the SCA. In particular, the summons requests from a provider of electronic communication services (the ISP) the contents of electronic communications (including all e-mails) for an ISP customer that have been in electronic storage by the ISP for the 180 days preceding the Service's issuance of the administrative summons and prospectively, after the date of issuance until the date the ISP complies with the summons, in violation of 18 U.S.C. § 2703(a). This section of the SCA provides, in pertinent part, that a governmental entity may require an ISP or other provider of electronic communications services to disclose the contents of an electronic communication the ISP has maintained in electronic storage for 180 days or less, only pursuant to a warrant issued under the procedures described in the Federal Rules of Criminal Procedure by a court of competent jurisdiction. The procedures described in Federal Rule of Criminal Procedure 41 for a warrant to seek electronically stored information were not followed by the revenue officer in this case; further, the revenue officer would not be eligible to seek a warrant for the civil (as opposed to criminal) tax law provisions he is engaged in seeking to enforce in this case.

2. No, as a practical matter it would not be sensible for the revenue officer in this case to reissue a modified administrative summons to the ISP, seeking only the contents of the ISP customer's e-mails from a date certain until another specified date that is more than 180 days before the issue date of the new summons. The SCA, 18 U.S.C. § 2703(a)-(b), does permit a governmental entity to require an ISP to produce the contents of an ISP customer's electronic communications that have been in electronic storage for more than 180 days in response to an administrative subpoena (including an IRS summons). In such cases, the governmental entity must either provide prior notice of the administrative subpoena to the customer, or the governmental entity may provide the customer with "delayed notice" of the subpoena if the conditions and procedures described in 18 U.S.C. § 2705 for such delayed notice to the customer are followed, including a required written certification by a supervisory official. In a recent case, the Sixth Circuit opined that the SCA provisions which allow a governmental entity to require an ISP to produce the contents of a customer's e-mails which are more than 180 days old without a properly authorized warrant, upon a showing of probable cause, violated the Fourth Amendment (as an unreasonable search and seizure) and were unconstitutional. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010), reh'g and reh'g en banc denied, 2011 U.S. App. LEXIS 5007 (6th Cir. March 7, 2011).[1] The ISP in

[1] The Sixth Circuit went on to hold that the Government relied in "good faith" in Warshak upon the provisions at issue of the SCA – allowing the Government to obtain the contents of the e-mails at issue via a subpoena or via a court order requiring a reasonable showing of relevance and materiality to an ongoing criminal investigation (rather than "probable cause") – so the court declined to apply the "exclusionary rule" to the evidence the Government obtained via the subpoena and court order under SCA procedures. Warshak, at 288-292. Consequently, the petitions for rehearing en banc that were filed

the present case is headquartered within the Ninth Circuit, rather than the Sixth Circuit, but the ISP has advised Counsel that it does not intend to comply voluntarily with the summons. The Ninth Circuit has not yet addressed the constitutionality of the provision of the SCA that the Sixth Circuit opined was unconstitutional, but the Ninth Circuit has previously opined that the contents of certain electronic messages were protected by the Fourth Amendment, and it has discussed possible constitutional distinctions between the contents of electronic communications and the non-content information associated with a customer's use of electronic communications. In short, we do not believe there is any reasonable possibility that the Service will be able to obtain the contents of this customer's e-mails that are more than 180 days old through a modified summons upon this ISP without protracted litigation, if at all. Moreover, the revenue officer has indicated that he is primarily interested in this case in the opportunity to look for the most recent potential collection leads in the customer's e-mails. The most recent e-mails the SCA permits the Service to seek via an administrative summons would surely contain only "stale" leads by the time any protracted litigation with the ISP (and any intervenors and likely amici)[2] could practically be concluded.

3. Yes, the current controversy concerning the constitutionality under the Fourth Amendment of the SCA permitting governmental entities to obtain the "content" of more than 180-day old customer e-mails and other electronic communications from an ISP by means short of a court-approved warrant, upon a showing of "probable cause," should not affect the Service's ability to continue to use an administrative summons to obtain from an ISP the non-content records concerning a customer's electronic communication services, which are described in 18 U.S.C. § 2703(c)(2). A model summons attachment that requests this non-content information from an ISP was contained in the July 2010 version of IRM Exhibit 5.20.4.-10, which is currently being republished in IRM chapter 25.5.2. The Ninth Circuit and other courts have recognized that a warrant is not required by the Constitution for a government entity to require an electronic communications provider to produce a customer's non-content information regarding an electronic communication. See United States v. Forrester, 512 F.3d 500, 509-513 (9th Cir.), cert. denied sub. nom., 129 S.Ct. 249 (2008) (the Government's use of a court-approved computer surveillance analogue to a pen register for telephone calls, disclosing the "to" and "from" addresses for a customer's e-mail messages, was not a "search" for Fourth Amendment purposes); United States v. Bynum, 604 F.3d 161, 164 (4th Cir.), cert. denied, 130 S.Ct. 3442 (2010) (a customer's subscriber information provided to an ISP is not protected by a Fourth Amendment privacy expectation); In re § 2703(d) Order, 2011 U.S. Dist. LEXIS 25322 (E.D. Va. March 11, 2011) (the Wikileaks Twitter Order case). Pursuant to 18 U.S.C. § 2703(c)(2)(F), the Service may continue to use an administrative summons upon an ISP (with no "notice" to the affected customer) to request, inter alia, the "means and source of payment" for the ISP's

---

with the Sixth Circuit in January 2011 were filed only by defendants Warshak and his mother; the United States did not file a petition for rehearing of the Sixth Circuit's 2010 decision in Warshak.

[2] The Electronic Frontier Foundation, a privacy advocacy group, participated in an amicus role at some stages of the Warshak case, and has done so in other cases involving these SCA issues.

electronic communication services to the customer, "including any credit card or bank account number." Through follow-up requests based on this ISP customer payment information, if sought in a new summons, the revenue officer may indirectly obtain some of the potential collection asset leads he is interested in pursuing further in this case.

BACKGROUND

The Service is seeking to collect more than a quarter million dollars assessed against an apparent shell entity taxpayer which received large tax refunds, arising from improperly claimed tax credits. The revenue officer is seeking to identify sources from which collection may be made, including from the assets of a suspected alter ego of the taxpayer. To learn more about the suspected alter ego's finances, specifically to whom and where the suspected alter ego may have transferred funds, the revenue officer served a summons upon an ISP headquartered within the Ninth Circuit. The summons requests the contents of the suspected alter ego's electronic messages and other communications for a period exceeding two years, through the date of the ISP's compliance with the summons. The revenue officer indicates is particularly interested in receiving the most recent e-mails, those the suspected alter ego sent or received within the last 180 days before the ISP complies with the summons. In response to the summons, the ISP first sent the revenue officer a letter, informing him of some of the relevant SCA limitations contained in 18 U.S.C. §§ 2703(a)-(b) and 2705. In a subsequent conversation, a representative of the ISP informed Counsel that the ISP would not voluntarily comply with the summons, in large part due to the recent Warshak decision by the Sixth Circuit. You requested our advice on how to proceed with respect to the summons.

ADDITIONAL DISCUSSION

Steven Warshak, an owner/operator of small businesses, was convicted in 2008 for fraud and money laundering in connection with the false marketing of Enzyte. His criminal conduct involved a series of advertisements on television and the Internet. It also included his practice of enrolling persons who responded to the advertisements in auto-ship programs for Enzyte without their consent, and his practice of misrepresenting his businesses' chargeback records for unsatisfied customers to various merchant banks that had agreed to process the credit card payments received by the Warshak businesses. In 2004, the Government first formally requested that one of Warshak's ISPs prospectively preserve the contents of any e-mails to and from Warshak's e-mail account to prevent them from being automatically deleted (via Post Office Protocol) from the ISP's server after Warshak downloaded the messages. Next, in 2005 the Government issued a subpoena to the ISP, pursuant to 18 U.S.C. § 2703(b)(1)(B)(i), requiring the ISP to turn over the content of some of the e-mails that it had begun preserving the previous year. Several months later in 2005, the Government obtained a further ex parte court order, pursuant to 18 U.S.C. § 2703(b)(1)(B)(ii), requiring the ISP to surrender the contents of additional e-mails preserved from Warshak's account. In all, the Government compelled the ISP to reveal the contents of approximately 27,000

e-mails. Warshak did not receive notice of either the subpoena or the order until more than a year later. Warshak, at 283.

The Sixth Circuit began with the proposition that a Fourth Amendment "search" occurs when the Government infringes upon "an expectation of privacy that society is prepared to consider reasonable." The court said this standard breaks down further into two discrete inquiries, first whether the target of the investigation has manifested a subjective expectation of privacy in the object of the challenged search, and second whether society is willing to recognize that expectation as reasonable. The Sixth Circuit found that Warshak plainly manifested a subjective expectation that his e-mails would be shielded from outside scrutiny. The court found that answering whether society was willing to recognize an expectation of privacy in the contents of e-mails as reasonable was of great importance because of "the prominent role that email has assumed in modern communication" and because "the Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish." The Sixth Circuit looked first for guidance to the case of Katz v. United States, 389 U.S. 347 (1967), where Government agents had affixed an electronic listening device to the exterior of a public phone booth and had used the device to intercept and record several phone conversations. In Katz, the Supreme Court found that this electronic interception of the contents of a conversation constituted a "search" under the Fourth Amendment, notwithstanding the fact that the telephone company (a third party) had the capacity to monitor and record the calls for its own business reasons. The Sixth Circuit further observed that the contents of letters receive similar Fourth Amendment protection, despite the fact that sealed letters are handed over to perhaps dozens of mail carriers, any one of whom could tear open the envelopes that separate the private words from the world outside. Warshak, at 284-5.

In further support of the proposition that the contents of e-mails deserve the same societal protection from a warrantless search as the contents of traditional paper mail or a telephone conversation, the Sixth Circuit cited to portions of the Ninth Circuit's 2008 Forrester decision, which had found the non-content portions of e-mail messages (e.g., the senders and receivers) were unprotected by the Fourth Amendment, and different in character from the "contents" of the e-mails (which had not been obtained without a warrant in that case). Warshak, at 286; Forrester, at 509-10 (importantly, the Supreme Court in the pen register case of Smith v. Maryland, 442 U.S. 735 (1979), distinguished pen registers from more intrusive surveillance techniques on the ground that pen registers do not acquire the "contents" of communications, but rather only the addressing information associated with phone calls). The Sixth Circuit also relied upon findings from a Ninth Circuit case that was reversed by the Supreme Court. Significantly, the Supreme Court did not adopt those findings; instead, it chose to assume them arguendo or comment on without deciding their merits. Warshak, at 286; City of Ontario v. Quon, 130 S.Ct. 2619, 2629-30 (2010), rev'g, Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008) (explicitly assuming only arguendo that Quon had a reasonable expectation of privacy in the text messages sent on the pager provided to him by the city, and observing that the "judiciary risks error by elaborating

too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear").

In Warshak, at 288-9, the Sixth Circuit ultimately held and announced the intended application of its decision as follows:

> 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 Warshak's emails. Moreover, to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional. … However, we disagree that the SCA is so conspicuously unconstitutional as to preclude good-faith reliance. …. it was not plain or obvious that the SCA was unconstitutional, and it was therefore reasonable for the government to rely upon the SCA in seeking to obtain the contents of Warshak's emails. ... 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 e-mails.

Since Warshak was decided, commentators and Government officials have observed that "the decision is only binding within the four states comprising the Sixth Circuit." Commentator Casey Perry opined that "it remains unclear how the rest of the nation will treat the Warshak decision," and "the good faith exception would continue to exist in each circuit until a similar case is heard and decided."[3] And in his April 6, 2011 testimony before the Senate Judiciary Committee, Cameron F. Kerry, General Counsel, U.S. Department of Commerce, stated:

> Warshak is the law only in the Sixth Circuit, and the U.S. government is determining whether to seek Supreme Court review [and] [u]ntil such time as the Court squarely addresses the issue, the law as to what protection the Fourth Amendment affords to the messages and other customer content transmitted and stored electronically will be unsettled. [4]

At the same hearing before the Senate Judiciary Committee, Associate Deputy Attorney General James A. Baker cautioned legislators to consider carefully whether the existing SCA or the Sixth Circuit's Warshak opinion strikes the correct balance about the privacy interests that society is willing to recognize as reasonable, explaining:

---

[3] U.S. v. Warshak: Will Fourth Amendment Protection be Delivered to Your Inbox?, 12 N.C. J.L. & Tech. 345, 365-6 (2011).

[4] The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age: Before the Sen. Judiciary Comm., Apr. 6, 2011, available at http://judiciary.senate.gov/hearings/hearing.cfm?id=e655f9e2809e5476862f735da16a199e, page 10 (Testimony of Cameron F. Kerry, General Counsel, U.S. Dept. of Commerce).

First, current law allows for the acquisition of certain stored communications using a subpoena where the account holder receives prior notice. This procedure is similar to that for paper records. If a person stores documents in her home, the government may use a subpoena to compel production of those documents. Congress should consider carefully whether it is appropriate to afford a higher evidentiary standard for compelled production of electronically-stored records than paper records.

Second, it is important to note that not all federal agencies have authority to obtain search warrants. For example, the Securities and Exchange Commission (SEC) and Federal Trade Commission (FTC) conduct investigations in which they need access to information stored as the content of email. Although those entities have authority to issue subpoenas, they lack the ability to obtain search warrants. Raising the standard for obtaining stored email or other stored communications to a search warrant could substantially impair their investigations.

Third, Congress should recognize the collateral consequences to criminal law enforcement and the national security of the United States if ECPA were to provide only one means – a probable cause warrant – for compelling disclosure of all stored content. For example, in order to obtain a search warrant for a particular email account, law enforcement has to establish probable cause to believe that evidence will be found in that particular account. In some cases, this link can be hard to establish. In one recent case, for example, law enforcement officers knew that a child exploitation subject had used one account to send and receive child pornography, and officers discovered that he had another email account, but they lacked evidence about his use of the second account.

Thus, Congress should consider carefully the adverse impact on criminal as well as national security investigations if a probable cause warrant were the only means to obtain such stored communications.

Please call me if you have any further questions.