6999 Library

The State of South Carolina
OFFICE OF THE ATTORNEY GENERAL

CHARLIE CONDON
ATTORNEY GENERAL

September 22, 2000

Daniel R. Yeargin, Assistant Chief
Department of Public Safety
Winthrop University
2 Crawford Building
Rock Hill, South Carolina 29733

RE: Informal Opinion

Dear Assistant Chief Yeargin,

By your letter of May 5, 2000, you have requested an opinion of the Attorney General's Office. Specifically you wish to know the proper mechanisms for obtaining information from Internet providers necessary pertinent to an ongoing criminal investigation.

By way of background you provide the following: At Winthrop University police are occasionally asked to investigate e-mail harassment and death threats. In the past, the police have been told by the Internet providers that in order to release subscriber information, the police would need to obtain a subpoena. If the police sought the actual contents of the e-mail messages, they would need to obtain a search warrant. You have written our office for clarification because in a prior opinion of this office, dated February 10, 2000, we opined that generally a search warrant is the proper investigative tool to obtain information before any charges have been brought against a suspect. You now question how police can acquire subscriber account information from Internet providers before an arrest has been made.

As a preliminary note, the information you received from the Internet providers regarding procedures based on the level of information sought is generally correct, but requires more explanation because the applicable statute is, in practicality, complicated. The governing federal statute is the Electronic Communications Privacy Act, codified in part at 18 U.S.C.A. §2703. The statute offers a tiered approach to obtaining information depending on the level of intrusiveness into the subscriber's account. Because of the length of the statute, I have reproduced only the relevant portions below:

REMBERT C. DENNIS BUILDING • POST OFFICE BOX 11549 • COLUMBIA, S.C. 29211-1549 • TELEPHONE: 803-734-3970 • FACSIMILE: 803-253-6283

Request Form

(a) Contents of electronic communications in electronic storage.--A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) Contents of electronic communications in a remote computing service.--(1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection--

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity--

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

. . .

(c) Records concerning electronic communication service or remote computing service.--**(1)(A) Except as provided in subparagraph (B), a provider of** electronic communication service or remote computing service may disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to any person other than a governmental entity.

(B) A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b)

of this section) to a governmental entity only when the governmental entity--

(i) obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant;

(ii) obtains a court order for such disclosure under subsection (d) of this section;

(iii) has the consent of the subscriber or customer to such disclosure; or

(iv) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title).

(C) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity, and length of service of a subscriber to or customer of such service and the types of services the subscriber or customer utilized, when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under subparagraph (B).

(2) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) Requirements for court order.--A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction described in section 3127(2)(A) and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. ...

• • •

In the above statute, subsection (a) discusses the disclosure of the contents of electronic communications of less than 180 days and requires the government to get a federal or state warrant. Subsection (b) addresses the contents of communications older than 180 days and requires the government to obtain a federal or state warrant, if the subscriber is not notified. If the subscriber does have prior notice, the government must have a federal or state administrative subpoena, a

federal or state grand jury or trial subpoena, or a U.S. district court order.[1] In your letter, you mentioned that you rarely seek the contents of the communications, so subsections (a) and (b) are not relevant to your inquiry. Instead, the focus of your inquiry rests on subsection (c), which provides for the disclosure of subscriber information (not contents). Subsection (c)(1)(A) allows disclosure to persons other than governmental entities. Subsection (c)(1)(B) allows the government to have information pertaining to a subscriber when the government: (i) gets a federal or state search warrant; (ii) gets a U.S. district court order;[2] (iii)gets consent of the subscriber; or (iv) submits a formal request relevant to an investigation for telemarketing fraud. Subsection (c)(1)(C) adds a federal or state administrative subpoena, a federal or state grand jury subpoena, and a federal or state trial subpoena as options to the four outlined in (c)(1)(B) when the government seeks information such as the identity, address, and billing records of a subscriber.

Although in summary the statute seems complicated, the difficulties worsen in its application to the facts. I will try to be as succinct as possible. In your situation, the University police require subscriber information for an investigation of e-mail harassment or threats. You have indicated the police do not need the contents of the messages, but I assume the police do want account information such as the name, address, and billing records of the subscriber who is the focus of the investigation. This puts investigators squarely within the purview of subsection (c)(1)(C). Again, the options available to the police are:

(1) federal or state administrative subpoena
(2) federal or state grand jury subpoena
(3) federal or state trial subpoena
(4) federal or state warrant
(5) U.S. district court order[3]
(6) consent of the subscriber
(7) written request pursuant to a telemarketing fraud investigation

---

[1] Or United States Magistrate or Court of Appeals order. A "court order" under 2703 (d) is defined as a court of competent jurisdiction described in 3127(2)(A). Unfortunately, 3127(2)(A) is defined as "a district court of the United States (including a magistrate of such a court) or a United States Court of Appeals." Undoubtedly, the drafters of 2703 (d) intended to include 3127 (2)(B) as well, which is "a court of general criminal jurisdiction of a State authorized by the law of that State to enters orders authorizing the use of a pen register or a trap and trace device." The omission of the state court was likely only a scrivener's error, but we are nonetheless faced with the statute as worded.

[2] *Id.*

[3] *Id.*

Unfortunately, although several alternatives appear to be available to police to obtain this information, many of the options have their limitations, particularly in the context of an investigation of e-mail harassment or threats. For the sake of clarity, the options to which I refer in the following paragraphs are those seven options listed above, derived from 18 U.S.C.A. § 2703(c)(1)(C).

Let us dispose of the obvious first. The harassment case clearly does not involve telemarketing fraud, so option (7) is inapplicable. It is highly unlikely that the subscriber will give consent, so option (6) is also unavailable. A federal or state trial subpoena, option (3), is inapplicable here because no case is pending. If no charges have been brought, nor arrests made, the jurisdiction of the trial court has not yet attached. Practically, the solicitor would be unable to provide the name of the court (with appropriate jurisdiction) or the title of the action if the case is still being investigated. See S. C. R. CRIM. P. 13.

Two other options are possible, but unlikely. Under option (2), an investigative subpoena, the kind of subpoena sought in this instance, could be sought from a federal or state grand jury, but the proceeding must be a grand jury investigation. In South Carolina, the State Grand Jury investigates narcotics and controlled substances, obscenity, public corruption, and crimes involving the election laws. See S.C. CODE ANN. § 14-7-1630. The State Grand Jury derives its investigative subpoena power expressly from the General Assembly. See S.C. CODE ANN. § 14-7-1680. Furthermore, assuming a liberal interpretation of "State grand jury" also includes local grand juries, local grand juries have only the subpoena powers authorized by the South Carolina Rules of Civil Procedure and §§ 19-9-10 through 19-9-130 . See S.C. CODE ANN. § 14-7-1550. There is no comparable statute granting express authority to local grand juries to issue subpoenas for investigative purposes. As such, local grand juries are probably without authority to issue subpoenas until a case is pending. Similarly, for a federal grand jury to issue a subpoena, the investigation must be pursuant to a federal grand jury proceeding.

As option (1) indicates, the officer could also seek a federal or state administrative subpoena to obtain the information. Typically administrative subpoenas are expressly authorized by statute, such as S.C. CODE ANN. § 44-53-480, which empowers the State Law Enforcement Division to issue administrative subpoenas and warrants in its investigation of illicit traffic in controlled substances. See also S.C. CODE ANN. § 20-7-9575 (authorizing the Department of Social Services to issue administrative subpoenas in enforcement of child support orders). Federal statutes provide the basis for the issue of a federal administrative subpoena. See e.g. 18 U.S.C.A. 3486 (the Attorney General may issue subpoenas when investigating child exploitation). Although the law enforcement officer investigating the e-mail harassment would not have the authority to issue administrative subpoenas, a separate state or federal agency may have been authorized to do so under color of a state or federal statute. As a practical matter, the law enforcement officer's best course of action would be to contact the State Law Enforcement Division (SLED) or the Federal Bureau of Investigation (FBI) for their assistance in determining the appropriate contacts to obtain an administrative subpoena.

Finally, the officer may attempt to obtain the information through the order of a United States District Court, Magistrate, or Court of Appeals. The federal court must have some basis for jurisdiction to issue such an order, however. In this instance, the officer could contact the United States Attorney General's Office for assistance.

At the conclusion of this analysis you may question what, practically, the police officer should do to obtain subscriber information when no charges have been brought and no case is pending. The option not discussed above, the search warrant, may in some instances be the officer's easiest course of action. We are advised that some internet providers, particularly the most well known, have designated law enforcement contacts available to process requests for account information. For example, the South Carolina police officer contacts the designated officer in Virginia, where the office of the provider is physically located. The S.C. officer forwards his affidavits supporting a warrant to the officer in Virginia. The Virginia officer takes the documents to a judge with appropriate jurisdiction locally to issue the warrant. The warrant is served on the provider, has proper jurisdiction despite the out of state request, and adequately protects the subscriber's rights to privacy. Of course, this option is not available when there is less than probable cause to support a warrant. This option also presents problems when the Internet provider is lesser known and their agents are difficult to locate. Again, SLED or the FBI may provide some assistance in locating providers.

In sum, the Electronic Communications Privacy Act's tiered approach does provide guidelines for Internet providers and governmental entities in obtaining information about subscribers under color of federal law. Although the statute appears to provide some clarity to the alternatives available, the practical limitations of each option can be quite complicated. In the circumstances you describe, in which the information is needed in the investigative stage of the process, the options are much more restricted. A search warrant, a grand jury subpoena, or an administrative subpoena may be feasible options in some instances, but the police officer will likely need outside assistance to acquire the appropriate authority, either from state or federal law enforcement or from the U.S. Attorney's Office.

As a final note, at least two cases have addressed the consequences of an improperly issued subpoena. See United States v. Hambrick, No. 99-4793, 2000 WL 1062039, (4th Cir. Aug. 3, 2000); Tucker v. Waddell, 83 F.3d 688 (4th Cir. 1996). In Hambrick the Fourth Circuit found that the Electronic Communications Privacy Act did not provide for the remedy of suppression of evidence obtained from an improperly issued subpoena. In Tucker the Fourth Circuit also held that "the language of § 2703(c) does not prohibit any governmental conduct, and thus a governmental entity may not violate that subsection by simply accessing information improperly. See 83 F.3d at 692. In light of these cases, we cannot opine that failure to follow the guidelines of 18 U.S.C.A. § 2703 (c) in obtaining a subpoena will necessarily result in either suppression of evidence or a civil suit against the government. We would caution, however, that flagrant disregard for the statute could have ethical implications for the entity issuing the subpoena.

This letter is an informal opinion only. It has been written by a designated Senior Assistant Attorney General and represents the position of the undersigned attorney as to the specific question asked. It has not, however, been personally scrutinized by the Attorney General nor officially published in the manner of a formal opinion.

With kind regards, I remain

Very truly yours,

Robert D. Cook
Assistant Deputy Attorney General