UNC
SCHOOL OF GOVERNMENT
THE UNIVERSITY
of NORTH CAROLINA
at CHAPEL HILL

Prosecution and Law Enforcement Access to Information about Electronic Communications

Jeffrey B. Welty

Introduction

Law enforcement officers and prosecutors frequently wish to access information about a suspect's electronic communications, such as phone calls, text messages, and e-mails. Of course, such information may be stored on the suspect's computer, cellular phone, or other electronic device, and officers are sometimes able to search those devices, whether pursuant to a search warrant or under an exception to the warrant requirement. However, this bulletin focuses on information possessed by service providers, access to which is governed more by statutory law than by Fourth Amendment principles.

How an officer or prosecutor can obtain such information depends on the specific type of information sought and whether the information includes the content of a suspect's electronic communications or is limited to so-called envelope information—addressing and other non-content information related to electronic communications, such as the time and duration of a communication. The procedure that the officer or prosecutor must follow, and the showing that he or she must make, also depends on whether he or she seeks access to information about the suspect's past communications (historical information) or ongoing, real-time access to the suspect's current and future communications.

The appendix contains a chart that summarizes the basic rules for different types of information; the text below analyzes each type of information in detail.

Jeffrey B. Welty is a School of Government faculty member specializing in criminal law and procedure. He may be reached at 919.843.8474 or welty@sog.unc.edu.

Phone Records

What Are They?

Wired and wireless telephone service providers collect large amounts of information about each of their phone lines and accounts. This information includes the identity of the subscriber, data concerning the use of his or her line or account, payment information, and so forth. Available information about the use of the line typically includes a record of each telephone number that has been dialed from the phone, the time at which each number was dialed, and the duration of each call. Phone records may also include information about incoming calls. However, phone records do *not* include information about the content of calls.

Status under the Federal Constitution

Because a subscriber voluntarily discloses dialed and received call information to his or her service provider, the subscriber has no reasonable expectation of privacy in the information. The United States Supreme Court has held that the use of a pen register or a trap and trace device[1] is not a search under the Fourth Amendment. Smith v. Maryland, 442 U.S. 735 (1979). It follows that it is also not a Fourth Amendment search for law enforcement to obtain an individual's phone records.

Relevant Federal Statutes

Although nothing in the Fourth Amendment prevents law enforcement officers from requesting an individual's phone records or prevents a phone company from complying voluntarily with such a request, federal statutory law limits the disclosure of such records to officers. These federal restrictions apply to all service providers in the United States, and state prosecutors and officers, just like federal prosecutors and officers, must follow the procedures proscribed in the statutes for obtaining access to phone records.

Under 18 U.S.C. § 2702(c), service providers may not disclose subscriber records to governmental entities, such as officers and prosecutors, absent specific lawful authority. The principal source of such authority is 18 U.S.C. § 2703. Under 18 U.S.C. § 2703(c)(2), a governmental entity may obtain basic records about a phone line, including a subscriber's name, his or her address, and records of calls placed and received, using a subpoena (either administrative,[2] grand jury, or trial).[3] Under 18 U.S.C. § 2703(c)(1), such an entity may obtain not only the foregoing basic information but *any* "record or other information pertaining to a subscriber to or customer" *except* "the contents of communications" through a federal or state search warrant or a court order (or,

1. Readers unfamiliar with these devices can find a description of them under the heading "Pen Registers and Trap and Trace Devices," below.

2. Many federal agencies have administrative subpoena powers. In North Carolina, the State Bureau of Investigation (SBI) may issue administrative subpoenas for certain phone records under N.C. Gen. Stat. (hereinafter G.S.) § 15A-298 if the records are "material to an active criminal investigation" being conducted by the SBI.

3. These basic records include a subscriber's name and address, the means and source of payment on the account, and "local and long distance telephone connection records [and] records of session times and durations." 18 U.S.C. § 2703(c)(2)(C). Whether noncontent information regarding voicemail, for example, the fact that A left B a voicemail at a particular time, falls within the subpoena-for-basic-information provision is debatable: Was there a "telephone connection" when A left B the voicemail, even though B did not answer the phone? No cases answer this question, suggesting that it is of limited significance in practice.

of course, with the consent of the subscriber).[4] The requirements for a court order are set forth in 18 U.S.C. § 2703(d), which requires the applicant to present "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought[] are relevant and material to an ongoing criminal investigation." Because this standard is lower than the probable cause required for a search warrant, law enforcement officers and prosecutors may prefer to seek a court order rather than a warrant.

Relevant State Statutes

North Carolina's General Statutes do not address the procedure by which law enforcement officers may obtain phone records, except that North Carolina General Statutes (hereinafter G.S.) 15A-298 gives the State Bureau of Investigation (SBI) administrative subpoena authority as discussed in note 2. Thus the federal statutes discussed above provide the relevant legal framework.

Practice and Procedure

North Carolina officers and prosecutors must comply with the requirements of the relevant federal statutes. These statutes apply to all "governmental entities," not just to *federal* governmental entities. Fortunately, compliance is not difficult. If a criminal case is pending, a prosecutor may simply subpoena basic phone records. If no criminal case is pending, or if more than the basic information available by subpoena is needed, usually the easiest way to procure phone records is to seek a court order.[5]

As to which entity should seek the order, the federal statutes only discuss the procedure by which a "governmental entity" may obtain phone records. The statutes do not define the term "governmental entity," and it is likely that both prosecutors' offices and law enforcement agencies qualify as governmental entities. Thus either an officer or a prosecutor may properly seek a court order, though in some districts, local practice may require the involvement of a prosecutor. The statutes do not require the application to be in any particular form, but typically the state files a written motion, together with a supporting affidavit.

Among North Carolina judges, only superior court judges may issue court orders for phone records, because 18 U.S.C. § 2703(d) allows only "court[s] of competent jurisdiction" to issue such orders. Under 18 U.S.C. § 2711, "court of competent jurisdiction" has the meaning assigned to it by 18 U.S.C. § 3127, which limits the term, as it applies to state courts, to "court[s] . . . authorized by the law of [the] State to enter orders authorizing the use of a pen register or a trap and trace device." Under G.S. 15A-262, only superior court judges are so empowered.[6] As noted

---

4. Is a search warrant or a court order issued by a North Carolina judicial official binding on a service provider located in another state? Probably so, under 18 U.S.C. § 2703(c)(1)(A), which provides for the disclosure of phone records based on "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or an equivalent state warrant." The use of the phrase "jurisdiction over the offense" appears to have been intended to ensure the efficacy of a warrant issued in one jurisdiction as to a service provider located in another. *Cf. In re* Search of Yahoo, Inc., 2007 WL 1539971 (D. Ariz. May 21, 2007) (unpublished) (relying on the quoted language as authority for a federal district judge to issue a search warrant regarding a service provider located in another district).

5. If no criminal case is pending but basic phone records would suffice, an officer or prosecutor could also ask the SBI to use its administrative subpoena power to obtain the records.

6. If an officer or a prosecutor decides to seek a search warrant instead of a court order, he or she is not limited to seeking one from a superior court judge, as the "court of competent jurisdiction" limitation in 18 U.S.C. § 2703(d) applies only to court orders, not to search warrants.

above, the legal standard for the issuance of such orders is whether the governmental entity seeking the order has shown specific and articulable facts providing reasonable grounds to believe that the requested records will be relevant to a criminal investigation.

Court orders for phone records are typically entered ex parte.[7] Furthermore, under 18 U.S.C. § 2705(b), such orders *may* require the service provider not to notify anyone, including the customer, of the existence of the order, if an adequate basis for such a requirement has been established. However, if criminal charges ultimately result, the order and any records produced under it appear to be discoverable pursuant to G.S. 15A-902(a)(1).

If a prosecutor or an officer obtains phone records through a procedure that violates the federal statutes, suppression is not required. No constitutional violation has taken place, so the Fourth Amendment exclusionary rule does not apply, and the statutory remedies for improper disclosure of records do not include suppression. *See* 18 U.S.C. § 2707 (listing remedies, including civil liability[8] for those who knowingly violate the statute but not including suppression); 18 U.S.C. § 2708 (providing that the remedies contained in section 2707 are the sole remedies for statutory noncompliance).

Pen Registers and Trap and Trace Devices

What Are They?

Historically, the term "pen register" referred to a device, installed on a phone or at a phone company's switching facility, that tracked all the numbers dialed from a particular phone line. The term "trap and trace device" referred to the converse, that is, a device that tracked all the numbers from which a particular phone line received calls. By using a pen register and a trap and trace device in conjunction, a law enforcement officer could collect a complete log of outgoing and incoming calls; in essence, he or she could have access to phone records in real time. Recently, at least under federal law, both terms have been expanded to include devices that capture "routing, addressing, or signaling information" regarding all electronic communications, not just phone calls.[9] For example, a pen register may be used to track all the addresses to which a particular computer user sends e-mails. The pen register would not record the content of the e-mails, only their destinations, just as a traditional pen register does not record the content of phone calls, only the numbers dialed.

---

7. Before charges are filed, there is no opposing party to serve, so any order must, of necessity, be entered ex parte. Furthermore, notice need not be given to the subscriber. 18 U.S.C. § 2703(c) ("A governmental entity receiving [phone records] is not required to provide notice to a subscriber or customer."). The propriety of seeking such an order ex parte after charges have been filed is not clear, but it appears to be common practice in many jurisdictions.

8. Officers and prosecutors should be aware of this civil liability provision. *See*, *e.g.*, Freedman v. America Online, Inc., 303 F. Supp. 2d 121 (D. Conn. 2004) (granting partial summary judgment in favor of a civil plaintiff who contended that two officers obtained records of his electronic communications in violation of federal law).

9. 18 U.S.C. § 3127. These broader definitions were adopted as part of the USA PATRIOT Act, Pub. L. No. 107-56, § 9, 115 Stat. 272, 288 (2001).

Status under the Federal Constitution

Because a telephone subscriber voluntarily discloses dialed and received call information to his or her service provider, the subscriber has no reasonable expectation of privacy in the information. Thus the use of a pen register or a trap and trace device on a telephone line is not a search under the Fourth Amendment. Smith v. Maryland, 442 U.S. 735 (1979). Presumably, the same reasoning applies to e-mail, text messaging, and other forms of electronic communication.

Relevant Federal Statutes

Although the Fourth Amendment does not restrict the use of pen registers and trap and trace devices, federal statutory law does. *See generally* 18 U.S.C. §§ 3121–27. These statutes make it a crime to install and use pen registers and trap and trace devices except by court order or pursuant to one of a few other narrow exceptions. 18 U.S.C. § 3121. A state prosecutor or law enforcement officer who installed or used such a device in violation of the statutes would be committing a federal crime.

The statutes allow "[a]n attorney for the government," or, in certain cases, a state law enforcement officer, to apply for an order authorizing the use of a pen register and/or a trap and trace device. 18 U.S.C. § 3122. An application for such a court order must be in writing, upon oath or affirmation, and must certify that "the information likely to be obtained is relevant to an ongoing criminal investigation." 18 U.S.C. § 3122.

If the application contains the proper certification, the court "shall enter" an ex parte order authorizing the use of a pen register or a trap and trace device. 18 U.S.C. § 3123(a)(1). The court need not, and may not, make an independent assessment of the likelihood that relevant information will be obtained. Only a "court of competent jurisdiction" may enter such an order, 18 U.S.C. § 3122(a)(1), meaning a federal district court (including a magistrate judge), or a state court empowered by state law to issue such orders.[10] *See* 18 U.S.C. § 3127(2).

The order must contain the information set forth in 18 U.S.C. § 3123(b), which generally requires that the order name the subscriber, identify the target of the investigation, and list "the number or other identifier . . . of the telephone line or other facility" to which the order applies. The order lasts for sixty days and may be renewed upon the same showing that is required for initial issuance. 18 U.S.C. § 3123(c). The order is presumptively sealed unless the court orders otherwise, and the phone company, or other relevant person or entity, may not disclose its existence to the subscriber. 18 U.S.C. § 3123(d). Likewise, when presented with an order, the phone company or other persons or entities in a position to facilitate the installation of the pen register or the trap and trace device are required to assist as needed and must be compensated for reasonable expenses incurred while assisting. 18 U.S.C. § 3124. Emergency use of a pen register or a trap and trace device without a court order is authorized by 18 U.S.C. § 3125 under limited circumstances (including approval from the United States attorney general or from another listed official), provided that an order is obtained within forty-eight hours.

Relevant State Statutes

Federal statutes allow state law enforcement officers to seek orders authorizing the use of pen registers and/or trap and trace devices from certain state courts "[u]nless prohibited by State law." 18 U.S.C. § 3122(a)(2). North Carolina law explicitly authorizes certain state courts to issue

10. In North Carolina only superior court judges are so empowered. *See* G.S. 15A-262.

such orders, subject to procedural requirements that generally mirror, but sometimes exceed, those imposed by federal law. The relevant statutes are G.S. 15A-260 through G.S. 15A-264.

One important feature of the state statutes is that the definitions of "pen register" and "trap and trace device" set forth in G.S. 15A-260 refer exclusively to capturing "numbers dialed" on "telephone line[s]." Unlike the federal statutes, they have not been amended to govern the interception of equivalent information regarding nontelephone electronic communications. An appropriate North Carolina court may nonetheless authorize the interception of such nontelephone information under the federal statutes, which allow state judges to authorize the use of pen registers and trap and trace devices unless prohibited by state law. Because North Carolina's statutes do not *address* the use of pen registers and trap and trace devices to capture nontelephone information, they do not *prohibit* the same.

North Carolina's statutes forbid the installation and use of pen registers and trap and trace devices on telephone lines except by court order, though there are a few other narrow exceptions. G.S. 15A-261. A "law enforcement officer" may seek such an order only from a superior court judge. G.S. 15A-262. On its face this provision appears to preclude prosecutors from seeking such orders, though presumably collaborative efforts between prosecutors and law enforcement officers are permitted. The application must be in writing and under oath or affirmation. *Id.* An officer must certify that "the information likely to be obtained is relevant to an ongoing criminal investigation." *Id.*

A judge "may" issue an order if he or she finds that there is "reasonable suspicion to believe" that a felony or a Class A1 or Class 1 misdemeanor has been committed by the person who is the subject of the application and that the use of a pen register or a trap and trace device would "be of material aid" to the investigation. G.S. 15A-263(a). Because the judge must find reasonable suspicion and because he or she "may"—rather than "shall"—issue the order, the state statutes allow the judge more room to assess the need for the pen register or the trap and trace device than do the federal statutes.[11]

The contents of any order must conform to the requirements of G.S. 15A-263(b), which are generally similar to those set forth in the federal statutes. The order is limited to a period of sixty days under G.S. 15A-263(c), though that time period may be extended. The order must be issued ex parte, and it must be sealed until further order of the court. G.S. 15A-263(a), (d)(1). When presented with an order, a phone company, or any person or entity in a position to facilitate the installation of the pen register or the trap and trace device, is required to assist as needed. They must be compensated for reasonable expenses incurred while assisting, and they may not disclose the existence of the device, or the investigation, to the subscriber. G.S. 15A-263(a), (d); G.S. 15A-264.

---

11. Although the federal statutes and the North Carolina statutes normally harmonize, these provisions of North Carolina law conflict with the federal statutes' requirement that a state judge "*shall* enter an . . . order authorizing the use of a pen register or trap and trace device . . . if . . . [a] law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation." 18 U.S.C. § 3123(a)(2) (emphasis supplied). However, it is reasonably clear that the federal statutes were intended to allow states to enact stronger privacy protections than exist under federal law, and so the North Carolina statutes, if ever challenged by the state, would likely be upheld. *See*, *e.g.*, 18 U.S.C. § 3122(a)(2) (allowing state officers to seek orders from state courts "[u]nless prohibited by State law," i.e., unless state law is more protective of privacy than federal law).

Practice and Procedure

Telephone lines

When seeking authorization to use a trap and trace device or a pen register *on a telephone line*, it is necessary to comply with both the federal statutes and the state statutes. Fortunately, the North Carolina statutory scheme was designed with the federal statutory scheme in mind. In effect the federal statutes establish a minimum set of procedural protections that the state statutes slightly exceed with respect to the use of a trap and trace device or a pen register on a telephone line. Thus compliance with the federal statutes will follow as a matter of course from compliance with the state statutes.

As discussed above, compliance requires that a sworn, written application be submitted by a law enforcement officer to a superior court judge and that the application establish reasonable suspicion to believe that the order would materially aid the investigation of a felony or a Class A1 or Class 1 misdemeanor. If these conditions are met, the court may enter a sealed, ex parte order valid for no more than sixty days. It should contain the statutorily required information. If criminal charges ultimately result, the order and the resultant data appear to be discoverable under G.S. 15A-902(a)(1).

Other methods of communication

To obtain an order authorizing the use of a trap and trace device or a pen register on a communication method *other than a telephone line*, it is necessary to comply only with the federal statutes, as the state statutes do not apply. Compliance requires that a sworn, written application be submitted by an officer to a superior court judge. The application must certify the relevance of the requested authorization to a criminal investigation. The court need not make an independent determination of relevance, but rather must issue an ex parte order, presumptively sealed, and valid for no more than sixty days. It should contain the statutorily required information, as described above, and is subject to discovery if criminal charges result.

Post-cut-through dialed digits

One problematic issue regarding the use of pen registers and trap and trace devices on telephone lines merits separate discussion. The federal statutes require that law enforcement "shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications." 18 U.S.C. § 3121(c). This appears to be an attempt to address the fact that a pen register typically records all dialed digits, including digits dialed after a connection is made. These so-called post-cut-through dialed digits may include account numbers, passwords, and other protected call content (e.g., when a person uses a telephone to check a bank account balance) that should not be available to officers or prosecutors except through a wiretap order.

Apparently, however, there is no "technology . . . that restricts" pen registers so that they do not record post-cut-through dialed digits. It appears that courts have not generally focused on, or perhaps even been aware of, this problem and that many pen register orders have been issued without regard to this issue. Recently, however, a number of decisions have addressed this concern. The decisions have generally agreed that it is improper for law enforcement to obtain information about post-cut-through dialed digits using a pen register, but they have disagreed about the legality of work-around approaches, such as having the post-cut-through dialed digits stripped from the data by the service provider or by a "taint team" of officers not involved in the

investigation before the data is provided to the investigating officers. *See, e.g., In re* United States, 622 F. Supp. 2d 411 (S.D. Tex. 2007) (rejecting government's request to collect post-cut-through dialed digits notwithstanding government's promise not to use such digits for investigative purposes and summarizing the dispute about this issue); *In re* United States, 441 F. Supp. 2d 816 (S.D. Tex. 2006) (rejecting a pen register application that sought access to post-cut-through dialed digits); *In re* United States, 515 F. Supp. 2d 325 (E.D.N.Y. 2007) (same); *In re* United States, 632 F. Supp. 2d 202 (E.D.N.Y. 2008) (approving a pen register application that stated that the service provider would record post-cut-through dialed digits and transmit them to law enforcement but that law enforcement would immediately delete them); *In re* United States, 2008 WL 5255815 (E.D.N.Y. Dec. 16, 2008) (unpublished) (rejecting a pen register application to the extent that it would permit the pen register to record post-cut-through dialed digits, even if the digits were not transmitted to law enforcement or were immediately deleted by law enforcement).

No reported North Carolina case addresses the issues surrounding post-cut-through dialed digits. Although the North Carolina statutes do not contain the federal requirement regarding restricting recording of electronic impulses that constitute the content of communications, 18 U.S.C. § 3121(c) makes that requirement applicable to orders issued "under State law" as well. Furthermore, even as a matter of state law alone, obtaining such information requires a wiretap order. Specifically, G.S. 15A-287 makes it illegal to "intercept" an electronic communication without a court order; G.S. 15A-286(13) defines "intercept" as acquiring the content of a communication through the use of an electronic or mechanical device. Thus law enforcement officers should offer to implement, and judges should require, procedures designed to ensure that officers do not receive or review any information about the content of communications. The federal cases discussed above may provide a starting point for crafting such procedures.

Remedies for noncompliance

Finally, it is worth considering the consequences of a law enforcement officer's unauthorized use of a pen register or a trap and trace device. Because the use of such a device does not violate a reasonable expectation of privacy, suppression is not required by the Fourth Amendment exclusionary rule. Nor do the federal or state pen register statutes provide for statutory exclusion. Thus suppression is appropriate only if a judge finds a "substantial violation" of the state statutes under the general statutory exclusionary rule, G.S. 15A-974, which would only be possible with respect to the use of a pen register or a trap and trace device on a telephone line because that is the only type of use that is addressed in G.S. Chapter 15A. However, an officer who uses a pen register or a trap and trace device without authorization commits a federal felony under 18 U.S.C. § 3121 and a Class 1 misdemeanor under G.S. 15A-261.

Wiretaps

What Are They?

Historically, the term "wiretap" referred to a device that allowed law enforcement to listen to all telephone calls involving a specified phone line. However, both the federal and state statutes governing such devices also encompass the interception of the content of other wire and electronic communications, not just telephone calls. *See generally* 18 U.S.C. §§ 2510–22; G.S. 15A-286 through G.S. 15A-298. Thus the term "wiretap" is now used to refer to the interception of the content of electronic communications in any format, whether the communications

occur via phone, fax, e-mail, text messaging, etc. *See, e.g.*, United States v. Councilman, 418 F.3d 67 (1st Cir. 2005) (en banc). Wiretaps are relatively rare; most are for drug offenses. Statistics gathered by the Administrative Office of the United States Courts (USAOC) indicate that about 2,000 state and 500 federal wiretap orders are issued each year. In 2007, the USAOC reported that just five wiretap orders were issued by North Carolina's state courts, four of which were for drug offenses. *See* Administrative Office of the United States Courts, 2007 Wiretap Report, *available at* www.uscourts.gov/wiretap07/contents.html). However, the SBI states that the USAOC's statistics should be interpreted to mean that wiretap orders were issued in five *investigations*, not that only five *orders* were issued.

Federal Constitution

Individuals have a reasonable expectation of privacy in the content of their wired telephone communications, so a wiretap of such communications is a search for Fourth Amendment purposes. Katz v. United States, 389 U.S. 347 (1967). Some have argued that, because cordless phones broadcast the content of telephone calls in an easily intercepted format, one cannot not have a reasonable expectation of privacy in the content of a conversation held on a cordless phone. (This argument implies that it would not be a search to listen in on cordless phone calls using a radio frequency scanner.) *See, e.g.*, State v. McGriff, 151 N.C. App. 631, 638 n.1 (2002). Theoretically, this analysis might be extended to cellular phones, but the calls are encrypted, making the argument both weaker and less likely to arise. *See generally* 2 Wayne R. LaFave et al., Criminal Procedure § 4.3(b) (3d ed. 2007). The constitutional status of the contents of other methods of electronic communication is also not perfectly clear, as described below under the heading "Stored Electronic Communications." Still, existing precedent tends to suggest, and a cautious officer or prosecutor should therefore assume, that the content of most electronic communications is normally subject to a reasonable expectation of privacy.[12]

That said, wiretaps are so thoroughly regulated by statute that the statutory scheme has largely supplanted the Fourth Amendment as a constraint on the conduct of law enforcement. The statutory scheme appears to be more protective of individual privacy than the Fourth Amendment requires—for example, the relevant statutes demand findings above and beyond probable cause in order to permit the use of a wiretap—so that in virtually all cases, compliance with the relevant statutes should suffice to ensure compliance with the Fourth Amendment.

Federal Statutes

The key federal law is the Wiretap Act, 18 U.S.C. §§ 2510–21, sometimes called "Title III" because it was enacted as Title III of the Omnibus Crime Control and Safe Streets Act of 1968. With few exceptions, the act makes wiretapping without a court order a felony.[13] 18 U.S.C. § 2511. Of particular importance to North Carolina law enforcement officers and prosecutors, the statute also provides that, if authorized by state law, "[t]he principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof," may seek

12. When a person is informed that his or her communications are subject to monitoring or recording, this is normally sufficient to defeat any expectation of privacy. For example, inmates who place telephone calls from jails or prisons typically are warned that their calls may be recorded; this overcomes both constitutional and statutory objections to such recordings. *See, e.g.*, State v. Troy, ___ N.C. App. ___, 679 S.E.2d 498 (2009) (holding that the defendant, a jail inmate, implicitly consented to having his telephone calls recorded by making the calls after being informed that they would be recorded).

13. The exceptions to this rule include emergency situations as defined in 18 U.S.C. § 2518(7).

a wiretap order from an appropriate state judge. 18 U.S.C. § 2516(2). Thus, whereas the federal pen register statute awards state judges the power to authorize the use of pen registers and trap and trace devices unless state law explicitly *removes* such authority, the federal wiretap statute reverses the presumption, giving state judges the power to authorize the use of wiretaps only if state law explicitly *grants* such authority. Even then, any state wiretap order must be issued "in conformity with [federal law] *and* with the applicable State statute." *Id.* (emphasis supplied). Thus North Carolina officers, prosecutors, and judges should be familiar with the basic outlines of federal law, as well as with the relevant state statutes.

The federal statutes limit who may apply for a wiretap order. Wiretap orders concerning "wire or oral communications"—essentially, phone calls—may be sought from a federal judge only if a high-level official within the United States attorney general's office approves the application in connection with an investigation into certain enumerated crimes. 18 U.S.C. § 2516(1). Wiretap orders concerning other "electronic communications"—such as e-mails and text messages—may be sought from a federal judge upon the approval of any federal prosecutor in connection with an investigation into any federal felony. 18 U.S.C. § 2516(3). The application must be in writing, under oath or affirmation, and must contain the information listed in 18 U.S.C. § 2518(1), including a complete statement of facts supporting the application.

The judge to whom the application is submitted "may enter an ex parte order" authorizing a wiretap if the judge finds probable cause to believe that (1) an individual is committing, has committed, or is about to commit one of the offenses listed in 18 U.S.C. § 2516; (2) "communications concerning that offense" will be obtained through the wiretap; (3) "normal investigative procedures" short of wiretapping have failed or are too dangerous; and (4) "the facilities from which, or the place where, the wire . . . communications are to be intercepted are being used, or are about to be used, in connection with the commission of such an offense, or are leased to, listed in the name of, or commonly used by such person." 18 U.S.C. § 2518(3). The application, and any order issued, must be sealed. 18 U.S.C. § 2518(8)(b).

The order must provide particular information about the identity of the person whose communications are to be intercepted, the type of communications that may be intercepted, which agency is authorized to do the wiretapping, and so forth. 18 U.S.C. § 2518(4). The order shall, upon the applicant's request, compel the assistance of the suspect's landlord, the phone company, or other people or entities that are in a position to aid in effectuating the wiretap. *Id.*

The order may not last longer than necessary, and in any event, not longer than thirty days, though it may be renewed for up to thirty days at a time. 18 U.S.C. § 2518(5). The order may require that reports be made to the issuing judge "showing what progress has been made toward achievement of the authorized objective and the need for continued interception." 18 U.S.C. § 2518(6).

The order "shall contain a provision" that the wiretap "be conducted in such a way as to minimize the interception of communications not otherwise subject to interception," that is, communications that are not pertinent to the investigation that gave rise to the wiretap. 18 U.S.C. § 2518(5). The statute does not specify how this is to be accomplished, and courts have generally upheld efforts at minimization, such as listening to the first two minutes of every phone call and then ending monitoring if the call is not relevant. *See* 2 Wayne R. LaFave et al., Criminal Procedure 497 (3d ed. 2007).

Within ninety days of the denial or expiration of a wiretap order, a judge must serve an inventory on "the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine . . . is in the interest of justice." 18 U.S.C. § 2518(8)(d).

The inventory must provide basic information, such as the date of the application, the period of interception, if any, and whether or not communications were, in fact, intercepted.

Because some suspects use multiple phone lines, sometimes in an attempt to evade wiretapping, the statute allows so-called roving wiretaps, which allow the wiretapping of any phone line used by a suspect without specific advance authorization as to each line. 18 U.S.C. § 2518(11)(b). Roving wiretaps are permitted only upon application by a federal law enforcement officer with approval from a senior official in the United States attorney general's office. *Id.*

State Statutes

As authorized under federal law, the General Statutes provide for the issuance of wiretap orders. The state statutes, which begin with G.S. 15A-286, often track, and are intended to conform to, federal law "except where the context indicates an intent to provide safeguards even more protective of individual privacy and constitutional rights." G.S. 15A-297. (There would be no point to drafting statutes less protective of privacy than are the federal statutes; as noted above, any state order must comply with federal law.) They generally prohibit the interception of "any wire, oral, or electronic communication" without authorization, meaning that the state statutes, like the federal statutes, apply to a range of technologies other than telephones. G.S. 15A-287. Wiretapping without authorization, such as a court order, is a Class H felony. *Id.*

Only the North Carolina attorney general or his designee may apply for an order authorizing the use of a wiretap. G.S. 15A-291. The head of any law enforcement agency, or any district attorney, may request that the attorney general submit an application. The procedure for making such a request is outlined in G.S. 15A-292. However, the attorney general may decline to do so or may submit an application without such a request. *Id.* In practice, counsel for the SBI is the contact point for wiretap requests.

An application is proper only if a wiretap would provide evidence of, or would expedite the apprehension of a person indicted for, one of the offenses listed in G.S. 15A-290. The list is extensive, and includes drug trafficking, murder, kidnapping, robbery, rape, and sexual offenses. It also includes "[a]ny felony offense against a minor" and felony offenses against jurors, witnesses, certain government officials, and so forth. *Id.*

The application must be submitted to a three-judge review panel, G.S. 15A-286(16), "composed of such judges as may be assigned by the Chief Justice" of the state supreme court or by another justice acting as his or her designee, G.S. 15A-291(a). The application "shall comply with all procedural requirements" set forth in 18 U.S.C. § 2518, and the statute lists various requirements that are taken nearly verbatim from the federal statute. G.S. 15A-291(d).

The review panel "may enter an ex parte order" upon a finding of the same four factors described that must be found under federal law. *Compare* G.S. 15A-293(a) *with* 18 U.S.C. § 2518(3). As is true of applications, orders "shall comply with all procedural requirements" set forth in 18 U.S.C. § 2518, G.S. 15A-291(d), and the statute again lists various requirements that are taken nearly verbatim from the federal statute. G.S. 15A-293(b). Both applications and orders must be sealed. G.S. 15A-293(d)(2). No judge who participates in a review panel may preside "at any trial or proceeding resulting from or in any manner related to information gained pursuant to a lawful electronic surveillance order issued by that panel." G.S. 15A-291(c).

The time limits are the same as under federal law, that is, no longer than necessary and not longer than thirty days, renewable. G.S. 15A-293(c). The judicial review panel may require periodic progress reports that establish the need for continued interception. G.S. 15A-293(d). The same minimization requirement applies as under federal law. *See* 15A-293(c). Roving wiretaps

are authorized under G.S. 15A-294(i). The same inventory requirement applies as under federal law. G.S. 15A-294(d). The state may appeal, ex parte and in camera, from the denial of an application. G.S. 15A-294(h)(2).

The state statutes contain a few provisions that are different from the federal statutes. First, state law only permits the results of a wiretap to be used at trial if each party has been provided with a copy of the application and order at least twenty working days before trial. G.S. 15A-294-(f). Second, the statutes provide that the SBI "shall own or control and may operate" any equipment used to implement a wiretap. G.S. 15A-293(e).

Practice and Procedure

This is a complex area of law. Because violations of the law may require the suppression of evidence, as explained below, and because violations of the law may be serious crimes, law enforcement officers and prosecutors should proceed with caution. An officer or prosecutor who is interested in obtaining a wiretap order should have the head of his or her agency contact the legal department of the SBI and should follow the lead of that agency and the attorney general's office in navigating the process.

Judges considering wiretap applications should be especially attentive to whether other investigative procedures have been tried or have been shown to be dangerous or unlikely to succeed, *see generally* 2 Wayne R. LaFave et al., Criminal Procedure § 4.6(e) (3d ed. 2007), and whether the minimization requirement has been met. *See generally id.* §4.6(h). Regarding the latter issue, there is some authority suggesting that an applicant should disclose whether he or she intends to use civilians to monitor the wiretap, a practice that is especially common when the conversations to be intercepted are likely to be in a language other than English. *See, e.g.*, United States v. Lopez, 300 F.3d 46 (1st Cir. 2002) (holding that "the government must disclose its intention to use civilian monitors" so that the court can craft an order ensuring minimization).

Under the federal statutes a defendant may move to suppress the results of a wiretap, and if the wiretap was not properly authorized under the statute, the results must be suppressed. 18 U.S.C. § 2515; 18 U.S.C. § 2518(10). State law likewise provides that a defendant may move to suppress the results of a wiretap based on noncompliance with the statute.[14] G.S. 15A-294(g). Federal case law provides, however, that suppression is not appropriate in response to minor, technical violations of the wiretap laws. United States v. Donovan, 429 U.S. 413 (1977); United States v. Giordano, 416 U.S. 505 (1974); United States v. Chavez, 416 U.S. 562 (1974). *See generally* 2 Wayne R. LaFave et al., Criminal Procedure § 4.6(m) (3d ed. 2007).[15]

If a motion to suppress is granted in a wiretap case, the state may appeal the order on an interlocutory basis. *See* G.S. 15A-294(h)(1). A wiretap order and any resultant data or recordings appear to be discoverable under G.S. 15A-902(a)(1) if criminal charges result.

---

14. Although only the state may violate the Fourth Amendment, a private person may violate the wiretap statutes; the results of a private person's illegal wiretapping activity must be suppressed in any civil or criminal proceeding. *See, e.g.*, United States v. Crabtree, 565 F.3d 887 (4th Cir. 2009); Rickenbaker v. Rickenbaker, 290 N.C. 373 (1976); Kroh v. Kroh, 152 N.C. App. 347 (2002); State v. Shaw, 103 N.C. App. 268 (1991).

15. Interestingly, the federal statute's exclusionary rule applies only to interceptions of "wire or oral" communications, not electronic communications, apparently because, at one time, electronic communications were viewed as less deserving of protection than wire and oral communications. *See* 2 Wayne R. LaFave et al., Criminal Procedure § 4.6(m) (3d ed. 2007). However, North Carolina's statutory exclusionary rule encompasses electronic communications as well. *See* G.S. 15A-294(g).

Stored Electronic Communications

What Are They?

Copies of certain electronic communications—such as text messages and e-mails—may be held by service providers during or after transmission of those communications.[16] Federal statutes regulate the ability of law enforcement officers and prosecutors to access the content of these stored communications—in effect, to obtain something akin to a retrospective wiretap.

Service providers also may possess envelope information about electronic communications, that is, they may be able to generate logs indicating when and with whom a particular subscriber communicated, without disclosing the content of the communications. The ability of law enforcement officers and prosecutors to access this information is also determined mostly by federal statutory law. Phone records are the most frequently sought type of envelope information. The rules regarding phone records, discussed above, are generally applicable to other technologies, discussed below, as well.

Federal Constitution

The contents of traditional paper mail are subject to a reasonable expectation of privacy while in the hands of the postal service. *See*, *e.g.*, United States v. Jacobsen, 466 U.S. 109, 114 (1984) ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy.") As noted above, the content of telephone calls also is protected. Thus, although one could argue that the content of an e-mail or a text message is not subject to a reasonable expectation of privacy on the theory that it is disclosed to a telecommunications service provider without any protective packaging, existing precedent tends to suggest otherwise. *See* 2 Wayne R. LaFave et al., Criminal Procedure § 4.4(c) (3d ed. 2007).

Even if the content of electronic communications is generally subject to a reasonable expectation of privacy, however, there may be exceptions and limitations to that expectation. Determining if a particular e-mail, for example, is subject to a reasonable expectation of privacy may depend on factors including whether

- the sender was an employee, whose employer warned him or her that messages sent from his or her work computer were subject to inspection;
- the sender's Internet service provider (ISP) provided for monitoring in its user agreement; and
- a third party received and reviewed the message before it was obtained by law enforcement.

See generally id. at § 4.4(e).

There are a few federal cases that explore these issues. *See generally*, *e.g.*, Warshak v. United States, 532 F.3d 521 (6th Cir. 2008) (en banc) (vacating as unripe a district court's order that was based in part on the conclusion that the contents of e-mail are subject to a reasonable expectation of privacy and suggesting that whether a reasonable expectation of privacy exists may depend in part on the terms of service or user agreement that applies to the e-mail account); Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892 (9th Cir. 2008) (holding that text messages are subject to a reasonable expectation of privacy); Guest v. Leis, 255 F.3d 325, 333 (6th Cir.

16. As noted in the introduction, such communications may also be stored on an end user's computer, cellular phone, or other electronic device, but searches of those devices are beyond the scope of this bulletin.

2001) ("Users would logically lack a legitimate expectation of privacy in the materials intended for publication or public posting. They would lose a legitimate expectation of privacy in an e-mail that had already reached its recipient; at this moment, the e-mailer would be analogous to a letter-writer, whose expectation of privacy ordinarily terminates upon delivery of the letter."); United States v. Polizzi, 549 F. Supp. 2d 308 (E.D.N.Y. 2008) (Weinstein, J.) ("Courts have generally found a reasonable expectation of privacy in the email messages themselves."). There may be so few cases in part because of the extensive federal statutory scheme that governs law enforcement access to the content of electronic communications; as is true in the wiretap context, the statutory scheme has largely supplanted constitutional considerations.

Envelope information regarding electronic communications likely is unprotected by the Fourth Amendment, just as envelope information regarding telephone calls is unprotected.

Federal Statutes

Many service providers are subject to federal statutes that regulate the disclosure of both the content of stored electronic communications and envelope information about such communications. The statutory scheme is set forth in the Stored Communications Act (SCA), 18 U.S.C. §§ 2701–12. The details of the SCA can be confusing, but in general the SCA makes it a crime to access stored wire or electronic communications without authorization, 18 U.S.C. § 2701, and sets forth procedures by which law enforcement may obtain authorization, 18 U.S.C. § 2703.

State officers and prosecutors must understand and comply with federal law not only to avoid committing a federal crime and risking civil liability, but also because service providers, which also may face civil liability for improper disclosure of stored electronic communications, will refuse to comply with orders that do not satisfy the federal statutes. As discussed below, the General Statutes do not regulate access to stored electronic communications, making federal law the only relevant body of authority.

Covered service providers and communications

The statute regulates the disclosure of information held by two types of service providers. The rules for the two types of providers are sometimes different, so it is important to categorize a service provider correctly.

Electronic communication services. The first type of service provider is an *electronic communication service* (ECS), which is "any service which provides to users thereof the ability to send or receive wire or electronic communications."[17] A company that offers e-mail accounts, such as an ISP or a cellular telephone company, would be an ECS.

In order for a communication held by an ECS to fall within the scope of the SCA, the communication must be held in "electronic storage." That term is defined in 18 U.S.C. § 2510(17) to mean "temporary, intermediate storage . . . incidental to . . . transmission," or "any storage . . . for purposes of backup protection."[18] Most communications held by ECSs, including most communications in which law enforcement officers are likely to be interested, will fall within this definition. The main concern regarding the definition is whether it includes opened e-mails and text messages stored on service providers' servers. That issue is addressed below.

---

17. 18 U.S.C. § 2510(15) (definition of "electronic communication service" in the Wiretap Act). *See also* 18 U.S.C. § 2711 (importing into the Stored Communications Act (SCA) the definitions of terms defined in 18 U.S.C. § 2510).

18. Again, this definition is imported into the SCA by operation of 18 U.S.C. § 2711.

Remote computing services. Under 18 U.S.C. § 2711 a *remote computing service* (RCS) is an entity that "provi[des] to the public . . . computer storage or processing services by means of an electronic communications system." A Web-based data backup business that allows users to upload data to its servers for a monthly fee would be an RCS, though many other types of entities store or process users' data, making them, at least arguably, RCSs.

In order for a communication held by an RCS to fall within the scope of the SCA, the communication must be held "on behalf of, and received . . . from . . . a subscriber or customer . . . solely for the purpose of providing storage or computer processing services to such subscriber or customer." 18 U.S.C. § 2702(a)(2). Again, most communications held by RCSs will fall within this definition.

It is often difficult to determine whether an entity is an ECS, an RCS, or neither. A single provider may offer multiple services, sometimes acting as an ECS, sometimes acting as a RCS, and other times acting as neither. For example, Google usually acts as an ECS with respect to Gmail account holders, but it usually acts as an RCS with respect to account holders who store copies of word processing documents online using Google Docs. Although eBay is likely neither an ECS nor an RCS in most capacities, it may act as an ECS when it allows prospective buyers and sellers to send messages to one another. When law enforcement officers seek to compel a service provider to disclose information, the key issue is what role the service provider is playing with respect to the information in question.

General prohibition against voluntary disclosure

The SCA generally prohibits ECSs and RCSs from voluntarily providing the "contents of a communication" or a "record . . . pertaining to a subscriber or customer" to law enforcement. 18 U.S.C. § 2702(a). As a result, law enforcement officers normally may obtain relevant information from an ECS or an RCS only through compulsory disclosure, discussed below.

However, the rule prohibiting voluntary disclosure has one important caveat: it applies only if the ECS or RCS provides services "to the public." As noted above, the very definition of an RCS requires that it provide services "to the public." The definition of ECS contains no such requirement, but the voluntary disclosure prohibition in the SCA applies only to ECSs that provide services "to the public." 18 U.S.C. § 2702(a)(1) & (3). Thus a nonpublic service provider—such as a large corporation, government agency, or university that maintains its own e-mail servers for the use of its own employees or students—may voluntarily provide the content of communications and noncontent records to law enforcement, should it so desire, subject only to any limitations that the Fourth Amendment may impose. Commercial service providers such as AOL, Yahoo!, Google, and most cellular telephone service providers, may not. Thus law enforcement officers normally will need to seek compulsory disclosure of such material.[19]

19. There are a few exceptions in the statute, under which an electronic communication service (ECS) or a remote computing service (RCS) that provides services "to the public" may voluntarily disclose information. 18 U.S.C. § 2702(b). However, the exceptions that are relevant to law enforcement are quite narrow.

Compulsory disclosure

Law enforcement officers can turn to 18 U.S.C. § 2703 for guidance on the information that is available to them through compulsory disclosure and the showing that they must make in order to obtain such disclosure. The statute establishes five separate sets of rules: three for various form of content and two for various forms of noncontent information.

Content rules.

- The contents of an electronic communication stored by an ECS for less than 180 days—such as recent, unopened e-mails—can be obtained only through a search warrant. 18 U.S.C. § 2803(a). This is the highest level of protection offered by the SCA.
- The contents of an electronic communication stored by an ECS for more than 180 days may be obtained through (1) a search warrant, (2) a subpoena, or (3) a court order,[20] based on a showing of "specific and articulable facts showing . . . reasonable grounds to believe that the [information is] relevant . . . to an ongoing criminal investigation." 18 U.S.C. § 2703(d). Although the use of a subpoena or a court order normally requires that prior notice be given to the subscriber, 18 U.S.C. § 2703(b)(1)(B), notice may be delayed by up to ninety days if, in the case of a court order, the court finds reason to believe that prior notice would jeopardize the investigation in one of the ways set forth in 18 U.S.C. § 2705(a)(2) or if, in the case of a subpoena, a "supervisory official" as defined in 18 U.S.C. § 2705(a)(6) makes a similar determination. The ninety-day delay may subsequently be extended if appropriate. 18 U.S.C. § 2705(a)(4).
- The content of an electronic communication stored by an RCS, regardless of the age of the communication or the length of the storage, may be obtained through the same three methods that can be used to obtain content of communications held by an ECS for more than 180 days. 18 U.S.C. § 2703(a).

Noncontent rules.

- All "record[s] or other information pertaining to a subscriber . . . or customer . . . not including the contents of communications," 18 U.S.C. § 2703(c), held by an ECS or an RCS, may be obtained through (1) a search warrant or (2) a court order based on a showing of reasonable grounds to believe that the records are relevant to an ongoing criminal investigation. This is the standard that likely governs e-mail logs and similar documents, discussed below. It is also the provision of law that governs the production of detailed phone records, as discussed under the heading "Phone Records," above.
- Basic subscriber or customer information, held by an ECS or an RCS, including the subscriber or customer's name, address, means of payment, and "telephone connection

20. The fact that the SCA allows access to the contents of these communications on a showing of less than probable cause and through instruments more easily obtained than a warrant raises Fourth Amendment questions. If the contents are subject to a reasonable expectation of privacy—which is likely, though not completely certain, as noted above—one could argue that the Fourth Amendment requires a warrant or a valid exception in order to permit disclosure. The question of whether the SCA falls short of the constitutional minimum was raised but not decided in *United States v. McCreary*, 2008 WL 399148 (9th Cir. Feb. 12, 2008) (unpublished) (holding that even if the government should not have been allowed to obtain the defendant's text messages via subpoena, the error was harmless in light of other evidence), and *United States v. Jackson*, 2007 WL 3230140 (D.D.C. Oct. 30, 2007) (unpublished) (although the government sought to obtain text messages by court order rather than warrant, it had full probable cause sufficient to support a warrant, so there was no Fourth Amendment problem).

records, or records of session times and locations," 18 U.S.C. § 2703(c)(2), may be obtained through a subpoena or through a search warrant or court order. This is the provision of law that governs the production of basic phone records, also discussed above.

The court orders that may be used in several of the circumstances described above may be issued only by a "court of competent jurisdiction." That term is defined in 18 U.S.C. § 2711 to mean a court described in 18 U.S.C. § 3127, which in turn defines it as any federal appellate or district court, including a magistrate judge, and any state court that is empowered to authorize the use of trap and trace devices. Under G.S. 15A-262, only superior court judges are empowered to do so, meaning that court orders authorizing the disclosure of the contents of, or records about, electronic communications must come from superior court judges.

Recurrent issues

Opened e-mail. It is unclear which of the above levels of protection applies to e-mail that has been opened and viewed but left on a service provider's server. An example may help to illustrate the issue. Suppose that A sends B an e-mail. A types up the e-mail, hits send, and the e-mail goes to A's ISP. A's ISP stores a temporary copy of the e-mail in case there are problems with transmission. A's ISP is acting as an ECS, and the copy is clearly in electronic storage, incidental to the transmission of the e-mail. A's ISP then sends the e-mail to B's ISP. B's ISP stores the e-mail until B accesses it. Until B accesses it, B's ISP is acting as an ECS and the e-mail is still in electronic storage incidental to transmission. Now suppose that B accesses the e-mail, reads it, and decides not to delete it, choosing instead to leave it on his ISP's server, perhaps for later reference. What is the status of the e-mail now? There are two possibilities:

1. The e-mail is still in "electronic storage" and B's ISP is still acting as an ECS. According to this theory, although the transmission is complete—meaning that the e-mail is no longer stored incidental to transmission (the first prong of the definition of "electronic storage")—it is stored for the purposes of "backup protection" (the second prong). Specifically, this theory assumes the e-mail is being stored for the backup protection of B, not for the backup protection of his ISP.
2. The e-mail is no longer in "electronic storage." The argument here is that "backup protection" refers to temporary copies made during transmission, like the copy made by A's ISP before it sent the e-mail to B's ISP, and that when B decided to leave the e-mail on his ISP's server, it was no longer a temporary copy made during transmission. According to this theory, the e-mail is not in electronic storage with an ECS, because it is not in electronic storage at all. But, it does not necessarily follow that the e-mail is totally unprotected under the SCA. Instead, one might argue that when B decided to leave the e-mail on the server, he began to use his ISP as an RCS, rather than an ECS, and the (somewhat less protective) RCS rules therefore apply to the e-mail.

The statutory text doesn't conclusively resolve this dispute about the meaning of "backup protection." The second option, above, reflects the understanding of the SCA held by the United States Department of Justice and several leading commentators. *See generally* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1216–17 (2004); Clifford S. Fishman & Anne T. McKenna, Wiretapping & Eavesdropping: Surveillance in the Internet Age §§ 7:6–7:9 (3d ed. 2008). However, most courts have rejected this position in favor of the first option. *See* Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004); Bailey v. Bailey, 2008 WL 324156 (E.D. Mich. Feb. 6, 2008)

(unpublished) (following *Theofel*); Cardinal Health 414, Inc. v. Adams, 528 F. Supp. 2d 967 (M.D. Tenn. 2008) (same); *cf.* Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107 (3d Cir. 2003) (in dicta, questioning district court's contrary ruling). *But see* Bansal v. Russ, 513 F. Supp. 2d 264 (E.D. Pa. 2007) (holding, without analysis, that opened e-mails are not protected by the SCA). Thus a cautious officer or prosecutor will seek access to recent, opened e-mails only by search warrant to ensure compliance with the statute.

Although there are few cases on point, text messages appear to raise the same issue. When A sends B a text message, it is in electronic storage with an ECS (B's cellular phone company) until B accesses it, at which point, if B does not delete it, it is either (1) still in electronic storage with an ECS, or (2) now stored with an RCS, depending on which of the above views prevail. *See* Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892 (9th Cir. 2008) (holding that provider of text messaging services was an ECS, even as to opened text messages); United States v. Jackson, 2007 WL 3230140 (D.D.C. Oct. 30, 2007) (unpublished) (noting the parties' disagreement regarding whether opened text messages are in electronic storage with an ECS or are maintained by an RCS; the court did not resolve the issue but ordered the service provider to provide any messages stored *qua* RCS).

E-mail logs and text message logs. E-mail logs and text message logs, so long as they are held by an ECS or an RCS, fall within the SCA's protections for noncontent information. Recall that the SCA contains two different standards for noncontent information, with certain basic information being available by subpoena and all information being available by search warrant or court order. Although at least one court has concluded that e-mail logs fall within the subpoena-for-basic-information provision, *see* United States v. Jackson, 2007 WL 3230140 (D.D.C. Oct. 30, 2007) (unpublished), this appears to be incorrect. The only log-type information that is available by subpoena is "telephone connection records, or records of session times or durations" and "telephone or instrument number or other subscriber number or identity," 18 U.S.C. § 2703(c)(2). E-mail logs fall within neither category; thus they should be available only by search warrant or court order.

Whether text message logs are available by subpoena is a more challenging question. Again, the key issue is whether text message logs are "telephone connection records, or records of session times or durations" or "telephone or instrument number or other subscriber number or identity." Because text messages are generally sent from one cellular phone to another over a cellular network used principally for telephone traffic, one could argue that they are "telephone connection records." On the other hand, one might argue that the devices involved are not acting as "telephones" when they send and receive text messages and/or that the sending of a text message, because it is asynchronous with receipt, does not involve a "connection." There are few if any cases on point, but the cautious view is to treat text message logs like e-mail logs and to seek access to them only via search warrant or court order.

State Statutes

There are no North Carolina statutes that directly address stored electronic communications; thus the protections established by the SCA are both the floor and the ceiling. Again, although the SCA is a federal statute, state law enforcement officers and prosecutors must comply with the SCA in order to avoid committing a federal crime, and because service providers will require compliance with the SCA before disclosing information about stored electronic communications.

Practice and Procedure

Court orders under the SCA are typically obtained ex parte. At least prior to the filing of charges, there is no opposing party to serve, so there is no alternative to an ex parte filing. However, if the order compels the disclosure of the contents of communications, prior notice to the subscriber or customer is required under 18 U.S.C. § 2703(b)(1)(B), unless notice may be delayed for one of the reasons listed in 18 U.S.C. § 2705. Conversely, if the order compels the disclosure only of records concerning communications—that is, envelope information—notice is not required. 18 U.S.C. § 2703(c)(3).

The SCA does not indicate whether applications for court orders, or the orders themselves, may be sealed. Presumably, a court may exercise its inherent authority to seal such applications and orders when appropriate. *See, e.g., In re* United States, 36 F. Supp. 2d 430 (D. Mass. 1999) (issuing order under seal). Like the other orders discussed in this bulletin, court orders under the SCA appear to be discoverable under G.S. 15A-902(a)(1) if criminal charges are filed.

Finally, the SCA provides for certain consequences, or remedies, in the case of a violation. These remedies include civil actions by aggrieved parties under 18 U.S.C. § 2707, though the civil remedies provisions of the statute are "somewhat unclear." Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1241 (2004).

Importantly, such consequences do not include suppression of evidence, unless there is also a constitutional violation. *See* 18 U.S.C. § 2708 (statutory remedies are exclusive for "nonconstitutional" violations). As noted above, the constitutional status of the contents of electronic communications is not settled, creating some uncertainty about the consequences of violations that involve the contents of communications. Violations that involve only envelope information, which is not protected by the Fourth Amendment, should not entail suppression.[21]

Conclusion

There are clear legal rules governing law enforcement officers' access to forms of electronic communication that have existed for a long time. For example, the rules regarding phone records and the rules regarding trap and trace devices are well settled. The rules governing newer methods of communication, such as e-mail and text messaging, are not as clear. Although this bulletin sets out the law as it exists now, future legislation and litigation may change both the procedures by which law enforcement may gain access to electronic communications and the level of protection that those forms of communications receive.

21. Because nothing in G.S. Chapter 15A regulates access to the communications and other information that is the subject of the SCA, it is unlikely that a nonconstitutional violation of the SCA would be a "substantial violation" of G.S. Chapter 15A under the statutory exclusionary rule in G.S. 15A-974.

This bulletin is published and posted online by the School of Government to address issues of interest to government officials. This publication is for educational and informational use and may be used for those purposes without permission. Use of this publication for commercial purposes or without acknowledgment of its source is prohibited.

To browse a complete catalog of School of Government publications, please visit the School's website at www.sog.unc.edu or contact the Publications Division, School of Government, CB# 3330 Knapp-Sanders Building, UNC Chapel Hill, Chapel Hill, NC 27599-3330; e-mail sales@sog.unc.edu; telephone 919.966.4119; or fax 919.962.2707.

Appendix: Summary of Rules regarding Prosecution and Law Enforcement Access to Information about Electronic Communications

	Historical Information		Real-time Access	
	Envelope	Contents	Envelope	Contents
Wired phone	Phone records are not protected by the Fourth Amendment, but federal statutory law restricts access to (1) basic information by subpoena or (2) extensive information by (a) warrant or (b) court order based on a showing of reasonable grounds to believe the information will be relevant. See section on "Phone Records."	N/A	This information is collected via pen registers or trap and trace devices. The information isn't protected by the Fourth Amendment, but federal and state statutes prohibit use except by court order based on certification of relevance. See section on "Pen Registers and Trap and Trace Devices."	This information is collected via wiretap. The Fourth Amendment protects this information, but the federal and state statutory schemes are likely even more protective. The statutes prohibit wiretaps except by court order based on probable cause plus additional showings, such as that other methods of investigation are not feasible. See section on "Wiretaps."
Cellular phone	See above.	N/A	See above.	See above.
Voicemail	See above, but see discussion in section on "Phone Records."	Probably same as e-mail, below, but see discussion in section on "Stored Electronic Communications."	See above.	See above.
Text message	Probably same as E-mail, below, but see discussion in section on "Stored Electronic Communications."	See E-mail, below.	See above.	See above.
E-mail	Addressing information may be unprotected by the Fourth Amendment. However, many e-mail logs are protected by federal statutory law, which allows access only by (a) warrant or (b) court order based on a showing of reasonable grounds to believe the information will be relevant. See section on "Stored Electronic Communications."	The scope of Fourth Amendment protection for this information is unclear, but in many cases it is protected by federal statutory law. The showing required by the statute varies depending on the age of the e-mail, how it is stored, and perhaps on whether it has been opened; in some cases, a search warrant is required. See section on "Stored Electronic Communications."	See above.	See above.