Electronic Searches and Surveillance

Table of Contents

Introduction 2
Historical Context (Case Law) 2
Statutes Codifying Case Law 5
   Title III (Wiretapping) 5
   Stored Communications and Transactional Records 7
      Content Information 8
      “Records and Other Information” 9
   Miscellaneous Provisions 9
Pen Register and Trap and Trace Devices 10
Search Warrant Procedures 11
   Rule 41 of the Federal Rules of Criminal Procedure 11
   N.C. Search Warrants (15A-241 through 259) 12
   “Court Order” as a Substitute for Search Warrant 13
What to Look for in Orders Authorizing Electronic Searches 14
   Jurisdictional Problems 14
   Substituting the Wrong Legal Standard 15
   Lack of Particularity 16
   Contents of Communication 17
Issues Ripe for Challenge: Cell Phones/Real-Time Records/GPS 17
   Real-Time v. Historical Records 18
   GPS Tracking 19
      Is GPS Tracking a Trespass? 19
      Is GPS Tracking a Violation of Privacy? 20
      Federal Search Warrant for Tracking Device 21
      Example of Substituting a Wrong Standard 22

“[I]s it not asking too much that officers be required to comply with the basic command of the Fourth Amendment before the innermost secrets of one’s home or office are invaded. Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices. Some may claim that, without the use of such devices, crime detection in certain areas may suffer some delays since eavesdropping is quicker, easier, and more certain. However, techniques and practices may well be developed that will operate just as speedily and certainly and – what is more important – without attending illegality.” Justice Brennan dissenting in Lopez v. U.S., 373 U.S. 427, 464 (1963).

Introduction

From time to time, law enforcement may obtain evidence without following the letter of the law. This paper addresses the law of electronic searches and surveillance to assist public defenders in determining whether evidence has been illegally obtained. For the purposes of this paper, “electronic searches and surveillance” includes cell phone searches, cell phone and text message records, GPS tracking, wiretapping, email records, and other electronic records.

This paper begins with a survey of the case law pertaining to electronic searches and surveillance to provide the historical context. A summary of the federal and state statutes regulating electronic searches follows. Finally, there is a discussion of how to analyze court orders (using sample orders) and what issues are ripe for challenge and litigation.

Historical Context

In Katz v. United States, 389 U.S. 347, 351, 88 S.Ct. 507, 19 L.Ed.2d 675 (1967), the Supreme Court found that the government’s attachment of an electronic listening device to a public telephone booth to eavesdrop on the conversation of the occupant violated that person’s “reasonable expectation of privacy.” In that case, the Court stated that “the Fourth Amendment protects people, not places.” Id. For example, in Alderman vs. U.S., 394 U.S. 165, 176, 89 S.Ct. 961, 22 L.Ed.2d 176 (1969), the Court prohibited the use of conversations against the defendants that had been obtained by the warrantless placement of an electronic surveillance device in another person’s home.

Prior to Katz, the Court required a physical trespass of a person’s property in order to violate the Fourth Amendment. In Olmstead v. U.S., 277 U.S. 438, 48 U.S. 564, 72 L.Ed 944) (1928), the Supreme Court found that the Fourth Amendment did not apply because the wire “taps of the house lines were made in the streets near the houses” as opposed to inside the homes.
themselves. In Goldman v. U.S., 316 U.S. 129, 135, 62 S.Ct. 993, 86 L.Ed.2d 1322 (1942), no “search” occurred where a “detectaphone” was placed on the outer wall of defendant’s office to overhear conversation inside the office. On the other hand, when police officers inserted a “spike mike” through the wall of a house, that constituted “unauthorized physical penetration into the premises occupied” by the defendant. Silverman v. U.S., 365 U.S.505, 81 S.Ct. 679, 5 L.Ed.2d 734 (1961).

Katz did not overrule the “trespass” theory. In fact, that theory made a “come-back” with Justice’s Scalia’s majority opinion in U.S. v. Jones, ___ U.S. __, 132 S.Ct. 945, 948-49, 954, 181 L.Ed.2d 911 (2012). In Jones, the Court held that federal and state law enforcement officers’ secret installation and use of a GPS tracking device on a suspect’s vehicle to monitor the vehicle’s movements was a “search.” 132 S.Ct. at 948-49. Likewise, the U.S. Supreme Court in Grady v. N.C., 575 U.S. __, __S.Ct. __, L.Ed.2d __ (2015), held that the attachment of a GPS device to a sex offender’s body and use of it to monitor the individual’s location is a “search” within the Fourth Amendment.

After Katz, the more commonly employed theory of what constitutes a search was the “reasonable expectation of privacy” theory. When the government acts to invade a person’s reasonable expectation of privacy, the Fourth Amendment comes into play. For example, in U.S. v. Karo, 468 U.S. 705, 714-15, 104 S.Ct. 3296, 82 L.Ed.2d 530 (1984), the DEA placed a beeper inside a can of ether and received tracking information from the beeper while the can was inside a private residence. In Kyllo v. U.S., 533 U.S. 27, 34-35, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001), government agents unlawfully used a thermal imager to gather information about the interior of an individual’s home. By the time of the Kyllo decision, the Katz privacy test had evolved into two elements: (1) whether the individual manifested a subjective expectation of privacy in the object of the search, and (2) whether society is willing to recognize that expectation as reasonable. Id., 533 at 33.

Pursuant to Katz and its progeny, the contents of telephone calls or communications, under circumstances that show a reasonable expectation of privacy, are protected by the Fourth Amendment and probable cause is required for the interception of those communications. The privacy protection of the contents of communications also applies to the content of emails (U.S. v. Warshak, 631 F.3d 266, 287-88 (6th Cir. 2010)) as well as the contents of letters and packages (Ex parte Jackson, 96 U.S. 727, 733, 24 L.Ed.877 (1877)). The digital data stored inside a cell phone is protected by the Fourth Amendment. Riley v. California, ___ U.S. __, 134 S.Ct. 2473, 2485, ___ L.Ed.2d ___ (2014), held that officers must generally secure a warrant before searching data on a cell phone because such devices contain vast quantities of personal information.

On the other hand, there is no reasonable expectation of privacy for non-content information such as the outside of letters and packages (Jackson, 96 U.S at 733), the “to/from” addresses of emails (Forrester, 512 F.3d at 510), or telephone numbers that have been dialed (Smith, 442 U.S. at 743-44). In U.S. v. Knotts, 460 U.S. 276, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983), the Court found that the use of a surreptitiously planted a radio transmitter to monitor a
vehicle’s movements on public roads and into an open field did not amount to a search. Information that was displayed to the public or given to a third party was not protected by the Fourth Amendment.

This concept evolved into what is known as the “third-party doctrine” which means that an individual “enjoys no Fourth Amendment protection in information he voluntarily turns over to a third party.” Smith v. Maryland, 442 U.S. 735, 743-44, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979). In other words, a person cannot claim a legitimate expectation of privacy in information that he has voluntarily turned over to a third party. Id. In Smith, the government used a pen register on the defendant’s home telephone to record the outgoing phone numbers dialed from his landline telephone. The Court held that, by dialing those numbers from his home phone, the defendant voluntarily conveyed those numbers to the phone company by exposing that information to the phone company’s equipment during the ordinary course of business. Three years before, the Court found that a defendant had no reasonable expectation of privacy in his bank records that were maintained by the bank and procured by a government subpoena. U.S. v. Miller, 425 U.S. 435, 442-43, 96 S.Ct. 1619, 48 L.Ed.2d 71, 79 (1976).

The third-party doctrine has been applied to historical cell-site location information (CSLI). This historical CSLI indicates which cell tower (usually the closest one to the cellphone) transmitted a signal when the defendant used his cellphone to make and receive calls and text messages. As a matter course, cellphone companies generate records that include the time, date, numbers of calling and receiving party, duration of call, and cell tower locations of each call and text message. Such information is commonly used to place a cellphone in a general vicinity at the time of a crime. There is no Fourth Amendment protection of CSLI because the government did not spy on the defendant and create these historical records, it merely obtained records from the cellphone company. U.S. V. Graham, 824 F.3d 421, 424-27 (en banc, 4th Cir. 2016). [For a good 2-paragraph “published” description of how cellphones work and CSLI are created, see the panel decision in Graham, 796 F.3d 332, 343 and the concurring opinion in Perry, 776 S.E.2d at 543-544. See also, Attachment 6, “Cellular Analysis for Legal Professionals” by Larry Daniel (digital forensic examiner and cellular analyst.)

Other types of electronic data or information have been deemed to fall under the third-party doctrine and, therefore, outside of Fourth Amendment protection. U.S. v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010)(the sending and routing of electronic communication, phone and Internet subscriber records including a person’s name, email address, telephone number, and physical address, is not protected by the Fourth Amendment); U.S. v. Suing, 712 F.3d 1209, 1213 (8th Cir. 2013) and U.S. v. Christie, 624 F.3d 558, 574 (3rd Cir. 2010)(Internet Protocol (IP) addresses contain no protected privacy interests); U.S. v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008)(e-mail and Internet users have no expectation of privacy in the IP addresses or websites that they visit).

The future of the third-party doctrine, however, may be uncertain. Justice Sotomayor stated in Jones that the doctrine is “ill-suited to the digital age, in which people reveal a great
deal of information about themselves to third parties in the course of carrying out mundane
tasks.” 132 S.Ct. at 957. Therefore, “it may be necessary to reconsider the premise that an
individual has no reasonable expectation of privacy in information voluntarily disclosed to third
parties. Id.

Shortly after the Katz decision in 1967, Congress passed Title III of the Omnibus Crime
Control and Safe Streets Act of 1968 that imposed statutory restrictions on electronic
surveillance. Since then, electronic surveillance has been primarily governed by statute. Riley,
134 U.S. at 2497.

Statutes Codifying Case Law

In the wake of Smith v. Maryland, 442 U.S. 735 (1979), Congress passed the Electronic
Privacy Act of 1986 (ECPA) which created a statutory framework for the government to obtain
and gather information from service providers. The ECPA consists of three parts. The first part,
known as Chapter 119 or Title III, updated the 1968 laws regulating the interception of wire,
oral, or electronic communications. (18 U.S.C. 2510-2522). The second part, Chapter 121 or the
 Stored Communications Act (SCA), dealt with the privacy of and government access to stored
electronic communications. (18 U.S.C. 2701-2712). The third part, Chapter 206, addressed the
installation and use of pen registers and trap and trace devices (PR/T&T) (18 U.S.C. 3121-3127).
Most states have similar or identical statutes covering the same areas as the ECPA.

An excellent analysis of the ECPA was prepared by Charles Doyle (Senior Specialist in
American Public Law) entitled “Privacy: An Overview of the Electronic Communications
Mr. Doyle’s “Overview” appears herein in Attachment 1 of this paper. The text of the ECPA
can be found on pp. 50-80 of Doyle’s “Overview.”

The pertinent North Carolina statutes are N.C.G.S. 15A-286 through 298 for interception
of communications and N.C.G.S. 15A-260 through 264 for pen registers and trap and trace
devices. There is no North Carolina equivalent for the Stored Communications Act. The N.C.
statutes appear herein in Attachment 2.

Title III or “Wiretapping”

to the contents of communications in which there was a reasonable expectation of privacy, and
required probable cause for the interception of those communications. Congress codified the
Katz ruling in 1968 by passing the initial version of Title III. Eighteen years later, the ECPA
revised Title III. The resulting statutory scheme for obtaining the contents of communications
places a high burden on the government similar to that of a search warrant supported by probable
cause requiring particularity and procedural protections. (For the requirements of search
warrants, see Rule 41 of the Federal Rules of Criminal Procedure and N.C.G.S. 15A-241 through
259.)
Generally, federal and state law prohibit **the interception of wire, oral, or electronic communications by using an electronic, mechanical, or other device** unless one of the parties to the conversation has consented to the interception or the interception was authorized by law. (18 U.S.C. 2511 and N.C.G.S. 15A-287). The contents of face-to-face communications as well as communications using landline telephones, cellphones, voicemails, emails, and text messages are examples of what falls under Title III’s protection. The radio portion of a cordless telephone that is transmitted between the cordless handset and the base unit is not a protected communication because it is an easily intercepted radio transmission. (See Doyle’s “Overview,” pp. 9-13 for a discussion of what are protected communications.)

Although there are several exceptions to the general prohibition of the interception of communications (see Overview, pp. 13-23), the most common one is “authorized” wiretapping or eavesdropping by law enforcement. Because the contents of such communications are generally protected by the Fourth Amendment, stringent standards were developed for law enforcement to follow in obtaining wire, oral, or electronic communications. 18 U.S.C. 2510-2522. State procedures for “wiretapping” applications and court orders must be at a minimum as demanding as federal requirements. (18 U.S.C. 2516(2); North Carolina’s requirements are found in N.C.G.S. 15A-286 through 298 and appear in Attachment 2.)

The application for a “wiretapping” order must be made by a senior Justice Department official and it applies to a specific list of crimes. (18 U.S.C. 2516). N.C. statutes authorize the State Attorney General or his designee to make an application to “judicial review panel.” (15A-291 and 292). Federal and state law require that an application be particular in describing the details of what is sought and the time period to be involved, fully state the alternative investigative techniques used or explain why other techniques would be futile or dangerous, and provide the complete history of previous interception applications or efforts involving the same parties or places. (18 U.S.C. 2518 and N.C.G.S 15A-291)

Federal and state law provide that an interception order may be issued only if a court finds that:

(a) there is **probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense** enumerated [in 18 U.S.C. 2516 or G.S. 15A-290]…; (b) there is **probable cause for belief that particular communications concerning that offense will be obtained through such interception**; (c) **normal investigative procedures have been tried and have failed** or reasonably appear to be unlikely to succeed if tried or be too dangerous; and (d) [except in special applications] there is **probable cause for belief that the facilities from which, or the place where the communications are to be intercepted are being used…in connection with the commission of such offense** …by such person. (18 U.S.C. 2518(3) and G.S. 15A-293(a), emphasis added).

The “wiretapping” interception order must include: a) the identity (if known) of the persons whose conversations are to be intercepted; b) the nature and location of facilities and place covered by the order; c) a particular description of the type of communication to be intercepted and an indication of the crime to which it relates; d) the individual approving the application and the agency executing the order, e) the period of time during which the
interception may be conducted and an indication of whether it may continue after the
communication sought has been seized; f) an instruction that the order shall be executed as soon
as practicable and so as to minimize the extent of innocent communication seized; and, g) upon
request, a direction for the cooperation of communications providers and others necessary or
useful for the execution of the order. (18 U.S.C. 2518(4) and (5)).

After an interception order is issued, it will remain in effect for 30 days. The court may
require progress reports describing the status of the execution of the order. Within 90 days after
the expiration of the order, notice to the party whose communications was intercepted is
required. (18 U.S.C. 2518). For a detailed discussion of applications and orders for
communication interceptions, see Doyle’s “Overview,” pp. 24-29.

The federal wiretap statute has its own exclusionary rule which bars admission into
evidence of an intercepted communication that 1) is the product of an unlawful interception, 2)
an interception authorized by a facially insufficient court order, or 3) an interception executed in
a manner substantially contrary to the order authorizing interception. (18 U.S.C. 2515 and
2518(10(a)). This statutory exclusionary rule may require suppression in instances where the
Fourth Amendment would not. (Gelbard v. U.S., 408 U.S. 41, 52 (1972) and “Overview”, p.
34).

**Stored Communications and Transactional Records**

While Title III addressed the interception of communication in transmission, it did not
deal with the intrusion into communications “at rest” (or stored communications) such as email,
electronic bulletin boards, voice mail, pagers, and remote computer storage. The second part of
the ECPA, the Stored Communications Act (SCA), regulates access to and disclosure of wire or
electronic communications at rest. (18 U.S.C. 2701-2712; for a detailed explanation of the SCA,
see Mr. Doyle’s “Overview,” pp. 35-46).

The SCA generally prohibits intentionally accessing and obtaining or altering a wire or
electronic communication while it is in electronic storage. (18 U.S.C. 2701(a)). The most
notable exceptions to the general prohibition allow access for the providers and users, and for
government officials pursuant to a warrant, court order, or subpoena. (18 U.S.C. 2701(c)).

The SCA specifically bans service providers from disclosing of the “*contents of any
communication*” while it is in electronic storage including disclosure to government entities.
(18 U.S.C. 2702(a)(1 and 2)). Service providers are also prohibited from knowing divulging “*a
record or other information pertaining to a subscriber or customer*” to any governmental
entity. (18 U.S.C. 2702(a)(3)). There are several exceptions to these prohibitions. A provider
may disclose “content information” or “records and other information” to an intended recipient
or addressee of the communication. A provider may make disclosures with the lawful consent of
the originator/sender or addressee/intended recipient of the communication, or the subscriber in
the case of a remote computing service. A service provider may disclose content information or
customer or subscriber records and other information to government officials pursuant to a Title
III (wiretapping) order or Section 2703(d) disclosure order (which will be described below). Finally, a service provider may make disclosures to government or law enforcement officials in cases of an emergency involving the danger of death or serious physical injury, and in cases where the contents were inadvertently obtained and appear to pertain to the commission of a crime. (18 U.S.C. 2702(b and c)).

Section 2703 outlines the procedure for government entities to obtain stored wire or electronic communications and transaction records. These procedures are less demanding than the procedures under Title III or a federal or state search warrant. It is important to note that there are two types of information addressed: 1) the contents of electronic or wire communications, and 2) the records or other information pertaining to the communications. Katz’s privacy expectation provides protection of the “contents” while Smith’s third-party disclosure rule gives little or no protection to the “transactional records.”

Content Information

With respect to disclosure of the contents of wire and electronic communications to governmental entities, a distinction is drawn between communications that are in electronic storage for a period of 180 days or less and communications that are in electronic storage for over 180 days. The contents of communications that have been in storage for 180 days or less, may be released only pursuant to a warrant [based on probable cause] issued using the procedures of Rule 41 of the Federal Rules of Criminal Procedure or, in the case of a State court, the warrant must be issued using State warrant procedures (i.e., N.C.G.S. 15A-241 through 259). For communications held for more than 180 days, the government may use a warrant, subpoena, or court order authorized in subsection 2703(d) to force disclosure of content information. If a subpoena or court order is used, notice must be given to the customer or subscriber. (18 U.S.C. 2703(a)). Rule 41(f)(1)(C) of the Federal Rules of Criminal Procedure requires notice by “receipt” to be given following the execution of a search warrant.

The rules for disclosure of the contents of communications that are held or maintained in a remote computing service are slightly different with notice to the customer or subscriber being the key distinction instead of the 180-day cut-off. No notice to the customer/subscriber is required if the government obtains a warrant [based on probable cause] using the procedures outlined in the Federal Rules of Criminal Procedures in order to obtain the contents of communications that are held or maintained on a remote computing service (since Rule 41 requires notice by receipt). In the case of a State court, the warrant [based upon probable cause] must be issued pursuant to State warrant procedures. If prior notice is given to the customer/subscriber, the government may use a subpoena or an order issued under subsection 2703(d) instead of a warrant. (18 U.S.C. 2703(b)).

In those cases where notice is required, there are provisions authorizing “delayed notification.” A court may delay a 2703(b) notice for a period of 90 days if there is reason to believe that notification of the existence of the court order or subpoena may have an “adverse result.” An adverse result is defined as “endangering the life or physical safety of an individual, flight from prosecution, destruction of or tampering with evidence, intimidation of potential
witness, or otherwise seriously jeopardizing an investigation or unduly delaying a trial"). Notice may be delayed for additional 90-day periods upon a re-showing of the danger of an adverse result. (18 U.S.C. 2705).

“Records and Other Information”

Absent the consent of the customer/subscriber, a governmental entity may obtain records of other information pertaining to a customer or subscriber (not including contents of communication) by 1) a warrant [supported by probable cause and issued using federal or state warrant procedures], 2) a subsection 2703(d) order, or 3) a subpoena for subscriber and payment information and call detail records. Prior notice to the customer/subscriber is not required for records of other information. (18 U.S.C. 2703(c)).

A subsection 2703(d) order may be issued by any federal judge or federal magistrate judge, or by a State court of general criminal jurisdiction that is authorized to issue search warrants. (18 U.S.C. 2711(3)). Such “a court order for disclosure…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.” (18 U.S.C. 2703(d)). This standard appears to be similar to a “Terry reasonable suspicion” standard as opposed to the “probable cause” standard as required by Katz, Jones, and Riley. (For suggestions in challenging the search and seizure of content information, see the section below entitled “What to Look For in Orders Authorizing Electronic Searches”.)

Miscellaneous Provisions

A provision of the SCA imposes a duty on providers to preserve “records and other evidence” in its possession pending the issuance of a court order upon the request of the government. (18 U.S.C. 2703(f)). It is unclear if this covers the “contents” of emails and other communications. Another provision of the SCA allows the government to require that providers create a backup copy of the “contents” of communications in order to preserve those communications. (18 U.S.C. 2704(a)). Section 2704 directs that the customer or subscriber be given notice and have the right to challenge the relevancy of the information sought. (18 U.S.C. 2704(a)(3) and (b)(4)).

Unlike Title III, there is no statutory exclusionary rule for violations of the SCA. Nevertheless, violations of the SCA, which also constitute violations of the Fourth Amendment, will trigger the Fourth Amendment exclusionary rule.

There is no North Carolina equivalent to the SCA. The only relevant statute is N.C.G.S. 15A-298 that provides the SBI Director or designee may issue an administrative subpoena to a communications common carrier for toll records or subscriber information that “are material to an active criminal investigation being conducted by the SBI.”
Pen Registers and Trap/Trace Devices (PR/T&T)

Pen registers and trace and trace devices were used long before the advent of cellphones and the internet. Originally, a pen register (PR) was an electronic device that recorded all outgoing numbers dialed from a particular telephone line. A trap and trace device (T&T) was an electronic device that identified all incoming calls to a particular telephone. As technology evolved, the same program or device could perform both functions of recording all incoming and outgoing numbers. PR/T&T devices are now able to capture the sender and addressee information relating to email and other electronic (internet) communications. (See “Overview,” pp., 46-47).

Since PR/T&T devices did not capture the “contents” of the phone conversation, they did not fall under Fourth Amendment protection or the provisions of Title III (wiretapping act). In other words, a search warrant supported by probable cause and accompanied by the other procedural protections associated with warrants are not required for the use of PR/T&T devices. Nevertheless, Congress and most states have regulated the use of PR/T&T devices. (See 18 U.S.C. 3121-3127 and N.C.G.S. 15A-260 to 264; and “Overview,” pp. 46-50).

Generally, federal law outlaws the installation and use of a PR/T&T device except pursuant to a court order, with the consent of the user, or in an emergency situation. (U.S.C. 3121(a)). However, a [federal] court shall enter an ex parte order authorizing the installation and use of a pen register or a trap and trace device anywhere within the United States, if the court finds...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)(1)). Federal law allows states to use PR/T&T devices. Upon application made [by a State investigative or law enforcement officer], a [state] court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device within the jurisdiction of the court, if the court finds...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)).

North Carolina law allows the installation and use of a PR/T&T device. A superior court judge may enter an ex parte order for the installation and use...of the device within the State if the judge finds: 1) there is reasonable grounds to believe that a felony offense, or a Class A1 or Class 1 misdemeanor offense has been committed; 2) that there are reasonable grounds to suspect that the person named or described...committed the offense...; and 3) that the results of procedures involving pen registers or trap and trace devices will be of material aid in determining whether the person named...committed the offense. (N.C.G.S. 15A-263).

Government attorneys in federal court and state or local police officers in state court may apply for a court order for the installation and use of a PR/T&T device upon certification that the intercepted information “is relevant to a pending criminal investigation.” (18 U.S.C. 3122 and N.C.G.S. 15A-262(b)).

An order authorizing installation and use of a PR/T&T device is not as demanding as a “wiretapping” order. Such an order must: 1) specify...a) the person (if known) upon whose telephone line the device is to be installed, b) the person (if known) who is the subject of the
criminal investigation, c) the telephone number (if known) of the location of the line to which the device is to be attached, d) the geographical range of the device, and e) a description of the crime to which the investigation relates, 2) upon request, direct carrier assistance pursuant to 18 U.S.C. 3124, 3) terminate within 60 days unless extended, 4) require a report of the particulars of the order’s execution in Internet cases, and 5) impose necessary nondisclosure requirements. (18 U.S.C. 3123 and N.C.G.S. 15A-263(b-c)).

Unlike search warrant or Title III requirements, there is no rule directing that the target of an PR/T&T order be notified after the order has expired. Also, there is no statutory exclusionary rule for a violation of the PR/T&T statutes, however, the Fourth Amendment’s exclusionary rule may apply to unlawful captures of “content” information. (“Overview,” p. 49).

With respect to “content” information, there may be some information captured by PR/T&T devices in the modern era that qualify as “content” information. “Post-cut-through dialed digits” are digits that are transmitted (other than telephone numbers) such as credit card numbers, bank account numbers, Social Security numbers, or prescription numbers which constitute “content” communication. If this is the case, officials must use a Title III (“wiretap”) order based on probable cause to obtain that information. (See Overview, pp. 10-11).

Authorities have tried to use orders issued pursuant to the Stored Communications Act (18 U.S.C. 2701-2712) and the PR/T&T statutes (18 U.S.C. 3121-3127) to obtain information necessary to track cell phone users in conjunction with an ongoing criminal investigation with mixed results. This type of tracking may be a violation of the Fourth Amendment. (See, section below entitled “Issues Ripe for Challenge” and “Overview,” pp. 48-49).

Search Warrant Procedures

If law enforcement intends to search for information that is protected by the Fourth Amendment, the officer must obtain a search warrant supported by “probable cause.” The search warrant or its functional equivalent must also follow federal or state statutes for search warrants that provide procedural protections against unreasonable searches.

Rule 41 of the Federal Rules of Criminal Procedure

Rule 41 governs the issuance of search warrants by a federal court. The full text of Rule 41 appears as Attachment 3. Rule 41 has special provisions for the installation and use of tracking devices. These special provisions are omitted here and will be addressed below under the section entitled “Issues Ripe for Challenge…GPS Tracking.”

Rule 41 (b)(1-6) dictates the circumstances and geographical limits of when a federal magistrate judge may issue a search warrant. A State court within a federal district has authority to only issue a warrant to search for and seize a person or property located within the federal district if no federal judge is reasonably available. Rule 41(b)(1).
A warrant may be issued for: 1) evidence of a crime; 2) contraband, fruits of a crime, or other items illegally possessed; 3) property designed for use, intended for use, or used in committing a crime; and 4) a person to be arrested or a person who is unlawfully restrained. Rule 41(c). A warrant must be issued “if there is probable cause to search for and seize a person or property...” Rule 41(d)(1). “Property” includes “information” which may include “electronic storage media or...electronically stored information.”

A warrant application by affidavit, sworn testimony or both must be made by a federal law enforcement officer or an attorney for the government. Rule 41(b). An applicant may request the issuance of a warrant in the presence of a judge or by telephonic or other reliable means. The court may question the applicant and any testimony must be recorded and filed with the clerk. Rule 41(d)(2-3).

If a warrant is issued, it must be issued to an officer who is authorized to execute it. The warrant must identify the person or property to be searched or seized, and designate the judge to whom the warrant must be returned. The warrant must command the officer to execute the warrant within 14 days or sooner, execute the warrant during the daytime (unless the judge, for good cause, expressly authorizes execution at another time), and return the warrant to the designated judge. Rule 41(e)(1-2).

There are specific requirements for executing and returning the warrant. The officer must enter the exact date and time the warrant was executed. The officer must prepare an inventory of any property seized. The officer must give a copy of the warrant and a receipt of the property taken to the person from whom, or from whose premises, it was seized, or leave a copy of the warrant and receipt at the place the officer took the property. In cases of electronically stored information, the officer may serve a copy of the warrant and receipt by electronic means. After a warrant has been returned to the judge, upon request, the judge must give a copy of the inventory to the person from whom, or from whose premises, the property was taken. Rule 41(f). Finally, the judge must attach a copies of the return, the inventory, and all other related papers to the warrant and deliver it to the clerk. Rule 41(i).

North Carolina Search Warrants (N.C.G.S. 15A-241 through 259)

The N.C. General Statutes outline the procedures for the application and issuance of a search warrant based upon probable cause. A copy of N.C.G.S. 15A 241 through 259 appears in this paper as Attachment 2.

A search warrant is a court order and process directing a law enforcement officer to search designated premises, vehicles, or persons for the purpose of seizing items and accounting for any items so obtained to the court which issued the warrant. (15A-241).

N.C.G.S. 15A-242 provides that: An item is subject to seizure pursuant to a search warrant if there is probable cause to believe that it: 1) is stolen or embezzled; 2) is contraband or otherwise unlawfully possessed; 3) has been used or is possessed for the purpose of being used to commit or conceal the commission of a crime; or 4) constitutes evidence of an offense or the identity of a person participating in an offense.
N.C.G.S. 15A-243(a) provides that a search warrant valid throughout the State may be issued by...an appellate justice or judge, or a judge of the superior court. [Note that N.C.G.S 15A-263(a) states that “a superior court judge may enter an ex parte order authorizing the installation and use of a pen register or a trap and trace device within the State...”] A district court judge, a clerk, or a magistrate may issue a search warrant for their district or county.

An application for a search warrant must be made in writing and under oath. An application must contain “allegations of fact supporting the statements...particularly setting forth the facts and circumstances establishing probable cause to believe that the items are in the places or in the possession of the individuals to be searched...” N.C.G.S. 15A-244. A judge may question the applicant under oath and, if that information is to be considered, the information must be recorded and made part of the record. If the judge finds that there is probable cause that the search will discover the items specified in the application and are subject to seizure, the court must issue the warrant. If the judge does not find probable cause, the court must deny the application. If a warrant is issued, the issuing official must retain a copy of the application and the warrant and must promptly file them with the clerk. N.C.G.S. 15A-245.

A warrant must contain, among other things, “a designation sufficient to establish with reasonable certainty the premises, vehicles, or persons to be searched; and a description or a designation of items constituting the object of the search and authorized to be seized.” 15A-246(4) and (5).

A search warrant may be executed by any law enforcement officer acting within his territorial jurisdiction, whose investigative authority encompasses the crime(s) involved. N.C.G.S. 15A-247. A search warrant must be executed within 48 hours of the time it was issued. 15A-248. Upon executing a search warrant, the officer must read the warrant and give a copy of the warrant application to the person to be searched or the person in apparent control of the premises or vehicle to be searched. If no one is present, the officer must leave a copy of the warrant affixed to the premises or vehicle. N.C.G.S. 15A-252. If any items are seized pursuant to the execution of a warrant, those items must be listed in an itemized receipt or inventory. 15A-254. After the execution of a warrant, the warrant and any inventory list must be returned to the clerk of the issuing court. 15A-257.

“Court Order” as a Substitute for a Search Warrant

In many cases, a law enforcement officer will seek a “court order” instead of a search warrant. In certain circumstances, a “court order” may serve as a functional equivalent of a warrant. If a court order is being substituted for a warrant, the order must contain “all of the indicia of a warrant.” Dalia v. United States, 441 U.S. 238, 255-56, 99 S.Ct. 1682, 60 L.Ed.2d 177 (1979).

The Supreme Court has interpreted the Fourth Amendment to require that warrants must be 1) issued by a neutral, disinterested magistrate, 2) supported by probable cause, and 3) particularly describe the place to be searched and the things to be seized. Stanford v. Texas, 379 U.S. 476, 481, 485 (1965). The Fourth Amendment requires “that a warrant be no broader than the probable cause on which it is based.” United States v. Hurwitz, 459 F.3rd 463, 473 (4th Cir. 2006); United States v. Zimmerman, 277 F.3d 426, 432 (3rd Cir. 2002). The particularity
requirement “makes general searches...impossible and prevents the seizure of one thing under a
warrant describing another. As to what is to be taken, **nothing is left to the discretion of the
officer executing the warrant.**” *Andresen v. Maryland*, 427 U.S. 463, 480-82, 96 S.Ct. 2737, 49
(1965) (emphasis added). The purpose of the particularity requirement is to guard against
general warrants and to “assure the individual whose property is searched...of the lawful
authority of the executing officer, his need to search, and the limits of his power to search.”

The analogous principle in Article I, Section 20 of the N.C. Constitution provides,
“[G]eneral warrants, whereby any officer or other person may be commanded to search
suspected places without evidence of the act committed, or to seize any person or persons not
named, whose offense is not particularly described and supported by the evidence, are dangerous
to liberty and shall not be granted.”

**What To Look For In Orders Authorizing Electronic Searches**

In order to determine if an order was unconstitutionally or illegally issued, a defense
lawyer needs to carefully review the application and order, and compare the order to the
requirements of case law and the pertinent statutes. Examples of orders authorizing electronic
searches appears as Attachment 4. A meticulous review of these orders may reveal the existence
of a lack of jurisdiction, a lack of particularity, too much discretion given to executing officers,
and the application of wrong legal standards. In evaluating any order or materials obtained
pursuant to the order, special attention should be given to whether “contents of communications”
are involved. These sample orders contain highly technical language for cell phone technology
and records. A “Glossary for Technical Terminology” to assist in defining these terms appears
in Attachment 5 of this paper.

In making a challenge to illegally obtained evidence, remember to state that evidence
obtained in violation of the defendant’s Fourth Amendment rights as well as rights secured by
Article I, Section 20 of the N.C. Constitution must be excluded from trial pursuant to *Mapp v.
derivative evidence from an unconstitutional search, be sure to allege that evidence and
statements that were the fruits of the unconstitutional search should be excluded pursuant to

**Jurisdiction for N.C. Search Warrant or Order**

N.C.G.S. 15A-243(a) provides that a search warrant valid throughout the State may be
issued by...an appellate justice or judge, or a judge of the superior court. Likewise, N.C.G.S
15A-263(a) states that “a superior court judge may enter an ex parte order authorizing the
installation and use of a pen register or a trap and trace device within the State...” A district
court judge, a clerk, or a magistrate may issue a search warrant for their district or county.
Beware of State orders that authorize action and searches outside of North Carolina. For example, see Detective A’s application (in Attachment 4B) and Judge Dardess’ order (in Attachment 4C) contain the following language:

[B]ecause the property described above to be tracked is mobile and due to the nature of the offenses being committed, it may be necessary to track said vehicles outside the jurisdiction of the court and it is therefore ordered that monitoring officers be allowed to continue to use the electronic tracking device in any jurisdiction within the United States, in the event that the subject vehicle travels outside the territorial jurisdiction of the Court.

A federal court has jurisdiction to order a search in other states. 18 U.S.C. 3117(a). Federal law, however, does not authorize a state judge to issue a warrant or order to allow police to conduct searches outside his or her district. See Rule 41(b)(1) of the Federal Rules of Criminal Procedure.

Substitution of the Wrong Standards

There are different standards for obtaining different types of information ranging from “probable cause” for GPS data and cellphone contents to “likely to be relevant” for pen register and trap and trace devices.

The “probable cause standard” is required for searches that are protected by the Fourth Amendment (i.e., GPS tracking, cellphone searches, and real-time location records). Federal law allows law enforcement to obtain stored records when “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.” (18 U.S.C. 2703(d), emphasis added). Pen register and trap and trace records may be obtained “if the court finds…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)(1) and (2), emphasis added). North Carolina state law has a standard that is slightly more demanding for records of pen registers and trap and trace devices. N.C.G.S. 15A-263 provides that a superior court judge may enter an order for the installation and use…of the device within the State if the judge finds: 1) there is reasonable grounds to believe that a felony offense, or a Class A1 or Class 1 misdemeanor offense has been committed; 2) that there are reasonable grounds to suspect that the person named or described…committed the offense…; and 3) that the results of procedures involving pen registers or trap and trace devices will be of material aid in determining whether the person named…committed the offense. (Emphasis added).

Review the application and order to ensure that the correct standard has been used. For example in the sample GPS order, the judge found that “The officer has offered specific and articulable facts showing that there is probable cause to believe that above referenced vehicle(s) are being used/operated by Mr. E and that the placement, monitoring of and records obtained from the electronic tracking device…are relevant and material to an ongoing criminal investigation conducted by the Raleigh Police Department.” (See Attachment 4C.) With exception to the phrase “probable cause,” the standard used in this case was identical to the standard for obtaining stored wire and electronic records, and that standard is far more lenient.
than any standard for obtaining a search warrant. The mere substitution of “probable cause” for “reasonable grounds” does not convert a lesser standard into a higher standard that is required for search warrants. To comply with Jones and N.C.G.S. 15A-242, the order should have stated that “there was probable cause to believe that the information obtained by the installation and use of a GPS tracking device constituted evidence of an offense or would lead to the identification of a person(s) participating in the offense.”

Lack of Particularity

In Berger v. New York, 388 U.S. 41, 87 S.Ct. 1873, 18 L.Ed.2d 1040 (1967), the Supreme Court struck down New York’s eavesdropping statute because it did not require a particularized description of the place to be searched, and the persons or things to be seized, and it allowed officers too much discretion in executing the eavesdropping order. An order authorizing an electronic search for which probable cause is required should contain the particularity of a search warrant. Berger provides guidance for evaluating an order for particularity requirements. In order to pass a particularity analysis, the order must contain:

- A particularized description of the place to be searched;
- A particularized description of the crime to which the search and seizure related;
- A particularized description of the [information] to be seized;
- Limitations to prevent general searches (In other words, the order should not provide the officer with discretion in the execution of the warrant or court order. The order should lay down “precise and discriminate” requirements to prevent the indiscriminate use of electronic devices to conduct a “general search.” Berger, 388 U.S. at 58. “As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.” Id., quoting Marron v. U.S., 275 U.S. 192, 196 (1927));
- Termination of the interception when the [information] sought has been seized;
- Prompt execution of the order;
- Return to the issuing court detailing the items seized; and
- A showing of exigent circumstances to overcome the want of prior notice.

Berger, 388 U.S. at 58-60.

The defense lawyer should compare the application or order in his or her case to the Berger list and the procedural requirements of a search warrant or a lesser applicable statute to see if the application or order complies with the law. If it does not, the defense lawyer could argue that the order is invalid on its face because of a lack of particularity, too much discretion given to executing officers, no jurisdiction, etc.
The Contents of the Communications

Review the application and order for the records to see if the contents of communications was requested or authorized. Also, review the records themselves to see if they contain any “content” information. For example, PR/T&T devices originally only captured incoming and outgoing call logs and did not touch upon content information. In the modern era, PR/T&T devices may capture “post-cut-through dialed digits” which are digits that are transmitted (other than telephone numbers) such as credit card numbers, bank account numbers, Social Security numbers, or prescription numbers. This information may constitute “content” communication. In addition, with respect to smart phones, records of call logs may show up as “my house” or the name or nickname of an individual. Riley, 134 U.S. at 2492-93. Such identifying information may be considered “content” information instead of mere transactional records.

“Contents of communications” that are obtained using an order issued pursuant to 18 U.S.C. 2703(d) (under the Stored Communication Act) or a subpoena may be ripe for a Fourth Amendment challenge. Under the SCA, the contents of communications that have been in electronic storage for over 180 days or communications that are held or maintained in a remote computing service may be obtained by a subpoena or a court order issued pursuant to 18 U.S.C. 2703(d). Such a court order for disclosure…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.” (18 U.S.C. 2703(d)). The standard for an SCA order looks like a “Terry reasonable suspicion” standard as opposed to a “probable cause” standard that is required for content information in which one has a reasonable expectation of privacy. In U.S. v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010), a Sixth Circuit panel held that “a subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent through, a commercial ISP. The government may not compel a commercial [provider] to turn over the contents of a subscriber’s email without first obtaining a warrant based on probable cause.”

Issues Ripe for Challenge: GPS, Cellphones, and Real-Time Records

Any information obtained from cellphones without a warrant is ripe for litigation. Riley v. California, ___ U.S. ___, 134 S.Ct. 2473, ___ L.Ed.2d ___ (2014) held that a search warrant is necessary for the search of the contents of a cell phone since cell phones are integral to modern life and all kinds of personal information are stored on those devices. Any information obtained from or relating to a cell phone should be challenged such as records other than incoming and outgoing calls, location information, and payment and billing information. Riley and Jones contain language that recognizes far ranging privacy interests in cell phones. (See below quotes from Riley and Jones.)

In Riley v. California, the Supreme Court recognized how pervasive cellphones are in modern society and how the devices contain extremely personal information. Chief Justice Roberts commented that “modern cell phones…are now such a pervasive and insistent part of life that the proverbial visitor from Mars might conclude they were an important part of human anatomy.” Id. at 2484. These modern cell “phones are based on technology nearly inconceivable
just a few decades ago.” Many cell phones “are in fact minicomputers that also happen to have the capacity to be used as a telephone” in which are stored many sensitive records previously found in the home…[and]...a broad array of private information…” Id. at 2489, 2491. “The fact that technology allows an individual to carry [the privacies of life] in his hand does not make the information any less worthy of the protection for which the Founders fought.” Id. at 2495.

For a good explanation of how cell phones work and cell site location information records are generated, see State v. Perry, 776 S.E.2d 528, 543-44 (N.C.App. 2015); U.S. v. Graham, 796 F.3d 332, 343 (4th Cir. 2015), and a powerpoint presentation by Larry Daniel (Forensic Examiner and Cellular Analyst) that appears in Attachment 6.

**Real-Time Information vs. Historical Records**

A battle line between “historical” versus “real-time” cell phone records appears to be forming. The crucial issue in this debate seems to depend on how “real-time” records are defined. Generally speaking, “real-time” information falls within the Fourth Amendment and requires a warrant based upon probable cause. However, “historical” records have been voluntarily conveyed to the service provider and fall outside the Fourth Amendment.

“Historical” records may be obtained by a mere showing of “specific and articulable” facts pursuant to 18 U.S.C. 2703. State v. Perry, __ N.C.App. __, 776 S.E.2d 528, 544-45 (2015).

Federal district courts have been divided over the question of what standard applies when the government seeks either current or historical cell phone location information from a provider. (See, In re Application of the United States, 733 F.Supp.2d 939, 940 n. 1 (N.D.Ill. 2009)(for a listing of cases up to that point.) The Third Circuit, in In re Application of the United States, 620 F.3d 304, 313-19 (3rd Cir. 2010), held that while the issuance of a subsection 2703(d) order does not require probable cause, the circumstances of a given case may require it. See also, In re Application of the United States, 747 F.Supp2d 827, 838-40 (S.D.Tex. 2010)(access to provider records relating to cell phone location over the course of an earlier 2-month period requires a warrant); In re Application of the United States, 727 F.Supp2d 571, 583-84 (W.D.Tex. 2010)(access to provider records relating to cell phone location either historically or prospectively should only be available under a warrant).

The majority of federal courts which have considered the issue have concluded that “real-time” location information may only be obtained pursuant to a warrant supported by probable cause since those records fall within an individual’s reasonable expectation of privacy. State v. Perry, __ N.C.App. __, 776 S.E.2d 528, 534 (2015). See U.S. v. Espudo, 954 F.Supp. 2d 1029-1034-35 (S.D.Cal. 2013); In re Application of U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013); In re Application for an Order…, 620 F.3d 304, 307-08 (3rd Cir. 2010). If law enforcement uses GPS, “real-time” information, electronically contacts, or otherwise physically trespasses upon a defendant’s cell phone, an invasion of the defendant’s reasonable expectation of privacy may occur. Perry, 776 S.E.2d at 540.
Despite the majority opinion’s twisting the meaning of “historical” records in State v. Perry, the dissenting judge provided a more accurate and honest definition of “historical” v. “real-time” records. The Fourth Circuit struggled with the same issue. The original panel held 2-1 that the government’s procurement of cell site location information (CSLI) was an unreasonable search under the Fourth Amendment. U.S. V. Graham, 796 F.3d 332, 343 (4th Cir. 2015). The en banc opinion found that CSLI fell within the third-party doctrine and was not protected by the Fourth Amendment. U.S. v. Graham, 824 F.3d 421 (2016). Judge Wynn’s dissent in the en banc opinion explains why CSLI is not voluntarily conveyed. Id. at 441-49. If you have a “historical v. real-time” issue, you need to carefully read both the Perry and Graham opinions. (Both were cases of first impression in North Carolina and the Fourth Circuit.)

As commonly used, “historical” cell site location data refers to the acquisition of cell site data for a period RETROSPECTIVE to the date of the order. “Real-time” or “prospective” cell site data refers to the acquisition of data for a period of time GOING FORWARD FROM the date of the order. “Real-time” information can be used by the government to identify the location of a phone at the present moment. Even if the cell phone user makes or receives no calls, real-time data may include records of the handset’s automatic registrations which occur every 7-10 minutes. Records stored by the wireless service provider that detail the location of a cell phone in the past (i.e., PRIOR TO THE ENTRY of the court order authorizing government acquisition) are known as “historical” cell site records. Perry, 776 S.E.2d at 544.

One should argue that “real-time” or GPS data falls within the Fourth Amendment because an individual had a reasonable expectation of privacy in his or her current location. In addition, a trespass theory may be appropriate if law enforcement electronically contacts, or otherwise physically trespasses upon a defendant’s cell phone. Perry, 776 S.E.2d at 540.

GPS Tracking

In United States v. Jones, __ U.S. __, 132 S.Ct. 945, 949, 181 L.Ed.2d 911 (2012), The U.S. Supreme Court held that the installation of a GPS device on a suspect’s vehicle and the use of that device to monitor the vehicle’s movements is a “search” because the government “trespassed” upon the defendant’s property when it installed and used the device to obtain information. In short, “where the government obtains information by physically intruding on a constitutionally protected area, such a search has undoubtedly occurred.” Id. at 951. Since the Court found a Fourth Amendment violation based upon the “trespass” theory, it did not reach the question of whether GPS tracking is a search under the “expectation of privacy” analysis as enunciated in Katz v. United States, 389 U.S. 347 (1967). Jones, 132 S.Ct. at 954.

Is GPS Tracking a Trespass?

A search is a physical intrusion by the government into the private life of an individual to gather information. Id. at 949. The Global Positioning System is based on satellites owned by the government that are orbiting the Earth. The satellites send electronic signals to a GPS tracking device that command the device to disclose its location. Electric signals have mass and
thus have physical or tangible substance. The transmission of an electric signal through or to a vehicle is a physical intrusion.

The Court in Jones did not directly address whether an electronic transmission by a GPS device could constitute a physical intrusion but the Court realized that technology is changing at a rapid pace. Justice Scalia recognized that “whatever new methods of investigation may be devised, our task, at a minimum, is to decide whether the action in question would have constituted a search…..” Id. at 951. GPS monitoring by itself could constitute a physical intrusion or “trespass” under the 4th Amendment.

“Some [courts] have held that even the transmission of electrons that occurs when a communication is sent from one computer to another is enough to establish a physically intrusive trespass.” Jones, 132 S.Ct. at 962 (Alito, J., concurring, citing CompuServe v Cyber Promotions, 962 F.Supp. 1015, 1021 (S.D. Ohio 1997); Thrifty-Tel v. Bezenek, 46 Cal.App.4th 1559, n. 6 (1996); and Register.Com v. Verio, 356 F.3d 393, 404-05 (2nd Cir. 2004). The transmission of electronic mail between devices is sufficiently physical to “constitute a trespass to property.” America Online v. LGCM, Inc., 46 F.Supp. 444, 452 (E.D.Va. 1998).

The use of a GPS device is just another way that the government may conduct a “search” by intruding into property with electric signals. U.S. v. Haynie, 637 F.2d 227, 230 (4th Cir. 1980)(the examination of a briefcase by an airport X-ray scanner was a search within the meaning of the Fourth Amendment); U.S. v. Epperson, 454 F.2d 769, 770 (4th Cir. 1972)(scanning a person’s body with a magnetometer was a search).

Is GPS Tracking Violation of Privacy?

Even if the mere transmission of electronic signals did not constitute a trespass, GPS monitoring would still remain subject to the “violation of privacy” analysis under Katz. Jones, 132 S.Ct. at 953. The Court recognized that an electronic search without an accompanying trespass may be an unconstitutional invasion of privacy. Id. at 954. In two concurring opinions by Justices Sotomayor and Alito, five justices held the view that long-term GPS tracking is a search under the expectation of privacy theory. Id. at 955-964. Even short-term GPS monitoring may fall under the Katz analysis. Id. at 955.

According to Justice Sotomayor, “GPS monitoring generates a precise, comprehensive record of a person’s public movements that reflect a wealth of detail about her familial, political, professional, religious, and sexual associations.” Id. at 955. The government can store GPS records and mine them for years. Since GPS monitoring is cheap compared to conventional surveillance techniques, it evades the normal constraints on abusive law enforcement practices, limited resources and community hostility. The fact the government may be watching may chill associational and expressive freedoms. The government’s power to assemble GPS data that reveal private aspects is also susceptible to abuse. These factors may “alter the relationship between citizen and government in a way that is inimical to democratic society” and thereby affect society’s reasonable expectation of privacy in the sum of one’s public movements. Id. at 956.

The authors of the majority and concurring opinions clearly recognized that the use of GPS monitoring will raise all kinds of issues under the Katz analysis. Justice Sotomayor stated that even cases involving short-term GPS monitoring will require particular attention under the
Katz analysis. Id. at 955. Justice Scalia noted that “different constitutional principles may be applicable to invasive law enforcement practices such as GPS tracking.” Id. at 956. Justice Alito said that, in the absence of legislative regulation, the courts will have “to apply existing Fourth Amendment doctrine and ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated.” Id. at 964.

Justice Alito explained that the Katz test is based on the assumption that a reasonable person has a well-developed and stable set of privacy expectations, however, technology can change those expectations. The dramatic technological changes may have affected popular expectations of privacy. For example, automatic toll road chip cards, closed-circuit television monitoring, and smart phones equipped with a GPS device continue to shape an average person’s expectations about privacy of his or her daily movements. Id. at 962-63. Justice Sotomayor believes that “owners of GPS-equipped cars and smartphones do not contemplate that these devices will be used to enable covert surveillance of their movements.” Id. at 956.

New technology has provided increased convenience or security at the expense of privacy, and society will have to determine how far it will tolerate the intrusion into privacy. Justice Alito opined that the new intrusions may spur the enactment of legislation to protect privacy just as Congress acted to regulate wiretapping after Katz. Id. at 962-63.

Jones has clearly required a search warrant based upon cause for the installation and use of a GPS tracking device. If your client has been tracked by a GPS device (or a functional equivalent), you may argue a Fourth Amendment violation based on a “trespass” or “privacy” theory or both. If there was no search warrant or court order issued, or the order was invalid (due to various problems discussed above), you should claim that a warrantless search by the police is invalid unless it falls within one of the narrow and well-delineated exceptions to the warrant requirement. Flippo v. West Virginia, 528 U.S. 11, 13 (1999) (per curiam); State v. Arrington, 311 N.C. 633, 643, 319 S.E.2d 254, 260 (1984) (Art. I, Sec. 20 of the N.C. Constitution provides the same protections as the Fourth Amendment). There is no exception to the warrant requirement for the installation and monitoring of individuals using a GPS tracking device.

Federal Search Warrant for a Tracking Device (FRCrimP. 41)

Unlike the N.C. General Statutes, Rule 41 of the Federal Rules of Criminal Procedure has special provisions that address the installation and use of a “tracking device” (i.e., “an electronic or mechanical device which permits the tracking of the movement of a person or object.” (18 U.S.C., sec. 3117(b); the text of Rule 41 appears in Attachment 3). In some cases, state officers have “cherry picked” the federal provisions to ostensibly provide authority for the use of a GPS device but omitted the protections that are contained in the federal rules. (See Attachment 4B and 4C).

After receiving an affidavit from a federal law enforcement officer or government attorney, a judge must issue the warrant if there is probable cause to support the installation and use a tracking device. Rule 41(d)(1). A tracking device warrant must identify the person or property to be tracked, designate the judge to whom it must be returned, and specify a reasonable time that the device may be used. That time period of the validity of the warrant must not exceed
45 days from the date the warrant was issued, however, extensions may be granted by the court for good cause. Rule 41(e)(2)(C). Federal law mandates that the officer 1) complete any installation of the device within 10 days, 2) perform the installation of the device during the daytime unless the judge for good cause expressly authorizes installation at another time, 3) return the warrant to the issuing judge within 10 days after the use of the device has ended, and 4) the officer executing the tracking device warrant must record “the exact date and time [that] the device was installed and the period during which it was used.” Rule 41(e)(2)(C)(i-iii) and Rule 41(f)(2). Finally, within 10 days after the use of the tracking device has ended, the officer must serve a copy of the warrant on the person who or whose property was tracked unless the court has specifically delayed such notice. Rule 41(f)(2)(C) and (f)(3).

If a GPS order is based on the federal rule, it should include the federal procedural protections. The sample GPS order fails to cite the authority upon which it is based, however, the application and order appear to be loosely based on Rule 41 of the Federal Rules of Criminal Procedure. (See Attachment 4C). Yet, the application and resulting order did not follow the limitations of Rule 41. The state order allowed “any authorized officer” to execute the order and provided wide discretion to officers in the execution of the order. Unlike the federal rule, the judge’s order gave the officers 30 days to install the device instead of 10 days. The installation of the device by the officers triggered the 45-day monitoring period instead of having the date of the order trigger the 45-day period. The federal rule provides for “daytime” installation unless the court has specified otherwise while the order in this case allows for the installation of the device “at any hour of the day or night.” The federal rule mandates that the officer return the executed warrant to the issuing judge within 10 days after the use of the device has ended and requires the officer to record “the exact date and time [that] the device was installed and the period during which it was used.” In addition, Rule 41 requires the tracking officer to serve the suspect with the warrant within 10 days after the monitoring period has ended unless the court has specifically delayed such notice. The sample order omits the return, recordation, and service requirements of a federal tracking device order.

Example of Substituting the Wrong Standards

In addition to omitting various statutory requirements, the sample GPS order (Attachment 4C) employed a legal standard far less strict than a standard used for a search warrant. The judge’s “probable cause” finding was that “The officer has offered specific and articulable facts showing that there is probable cause to believe that above referenced vehicle(s) are being used/operated by Mr. E and that the placement, monitoring of and records obtained from the electronic tracking device…are relevant and material to an ongoing criminal investigation conducted by the Raleigh Police Department.” (Emphasis added.) With exception to the phrase “probable cause,” the standard used in this case was identical to the standard for obtaining stored wire and electronic records, and that standard is far more lenient than any standard for obtaining a search warrant.

Federal law allows law enforcement to obtain stored wire and electronic communication and transactional records 18 USC 2703(d) when “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.” (18 U.S.C. 2703(d), emphasis added). This
The Jones decision requires a warrant based upon probable cause for police to install and use a GPS tracking device. 132 S.Ct. at 949. Although there is no North Carolina statute authorizing a GPS search warrant, N.C.G.S. 15A-242 provides that a search warrant may issue “if there is probable cause to believe that [an item]... is stolen or embezzled; or is contraband or otherwise unlawfully possessed; or has been used or is possessed for the purpose of being used to commit or conceal the commission of a crime; or constitutes evidence of an offense or the identity of a person participating in an offense.” (Emphasis added). There is a significant difference between the high standard for issuing a search warrant and a standard requiring that a GPS device merely being “relevant and material to an ongoing criminal investigation.” The substitution of “probable cause” for “reasonable grounds” does not automatically create a Fourth Amendment standard of protection.

**Attachments**

1) Charles Doyle, Privacy: An Overview of the Electronic Communications Privacy Act (2012)
2) Text of N.C.G.S. 15A-241 through 264 and 15A-286 through 298;
3) Text of Rules 41 of the Federal Rules of Criminal Procedure;
4) Sample Application and Orders;
5) Glossary of Technical Terms
6) Larry Daniel, “Cellular Analysis for Legal Professionals”

May 19, 2017

Michael G. Howell
Assistant Public Defender
Wake County Justice Center
300 South Salisbury Street, Suite 5000
Raleigh, NC 27601
(919) 792-5461