LEXSTAT O.C.G.A. 16-9-108

OFFICIAL CODE OF GEORGIA ANNOTATED
Copyright 2007 by The State of Georgia
All rights reserved.

*** Current Through the 2007 Regular Session Annotations Current Through February 8, 2008. ***

TITLE 16. CRIMES AND OFFENSES
CHAPTER 9. FORGERY AND FRAUDULENT PRACTICES
ARTICLE 6. COMPUTER SYSTEMS PROTECTION
PART 3. INVESTIGATION OF VIOLATIONS

O.C.G.A. § 16-9-108 (2008)

§ 16-9-108. Investigative and subpoena powers of district attorneys and the Attorney General

(a) In any investigation of a violation of this article or any investigation of a violation of *Code Section 16-12-100*, 16-12-100.1, 16-12-100.2, 16-5-90, or Article 8 of Chapter 9 of Title 16 involving the use of a computer in furtherance of the act, the Attorney General or any district attorney shall have the power to administer oaths; to call any party to testify under oath at such investigation; to require the attendance of witnesses and the production of books, records, and papers; and to take the depositions of witnesses. The Attorney General or any such district attorney is authorized to issue a subpoena for any witness or a subpoena to compel the production of any books, records, or papers.

(b) In case of refusal to obey a subpoena issued under this Code section to any person and upon application by the Attorney General or district attorney, the superior court in whose jurisdiction the witness is to appear or in which the books, records, or papers are to be produced may issue to that person an order requiring him or her to appear before the court to show cause why he or she should not be held in contempt for refusal to obey the subpoena. Failure to obey a subpoena may be punished by the court as contempt of court.

LEXSTAT O.C.G.A. 16-9-109

OFFICIAL CODE OF GEORGIA ANNOTATED
Copyright 2007 by The State of Georgia
All rights reserved.

*** Current Through the 2007 Regular Session Annotations Current Through February 8, 2008. ***

TITLE 16. CRIMES AND OFFENSES
CHAPTER 9. FORGERY AND FRAUDULENT PRACTICES
ARTICLE 6. COMPUTER SYSTEMS PROTECTION
PART 3. INVESTIGATION OF VIOLATIONS

O.C.G.A. § 16-9-109 (2008)

§ 16-9-109. Disclosures by service providers pursuant to investigations

(a) Any law enforcement unit, the Attorney General, or any district attorney who is conducting an investigation of a violation of this article or an investigation of a violation of *Code Section 16-12-100*, 16-12-100.1, 16-12-100.2, or 16-5-90 or Article 8 of this chapter involving the use of a computer, cellular telephone, or any other electronic device used in furtherance of the act may require the disclosure by a provider of electronic communication service or remote computing service of the contents of a wire or electronic communication that is in electronic storage in an electronic communications system for 180 days or less pursuant to a search warrant issued under the provisions of Article 2 of Chapter 5 of Title 17 by a court with jurisdiction over the offense under investigation. Such court may require the disclosure by a provider of electronic communication service or remote computing service of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than 180 days as set forth in subsection (b) of this Code section.

(b) (1) Any law enforcement unit, the Attorney General, or any district attorney may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service, exclusive of the contents of communications, only when any law enforcement unit, the Attorney General, or any district attorney:

(A) Obtains a search warrant as provided in Article 2 of Chapter 5 of Title 17;

(B) Obtains a court order for such disclosure under subsection (c) of this Code section; or

(C) Has the consent of the subscriber or customer to such disclosure.

(2) A provider of electronic communication service or remote computing service shall disclose to any law enforcement unit, the Attorney General, or any district attorney the:

(A) Name;

(B) Address;

(C) Local and long distance telephone connection records, or records of session times and durations;

(D) Length of service, including the start date, and types of service utilized;

(E) Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) Means and source of payment for such service, including any credit card or bank account number of a subscriber to or customer of such service when any law enforcement unit, the Attorney General, or any district attorney uses a subpoena authorized by *Code Section 16-9-108*, 35-3-4.1, or 45-15-17 or a grand jury or trial subpoena when any law enforcement unit, the Attorney General, or any district attorney complies with paragraph (1) of this subsection.

(3) Any law enforcement unit, the Attorney General, or any district attorney receiving records or information under this subsection shall not be required to provide notice to a subscriber or customer. A provider of electronic communication service or remote computing service shall not disclose to a subscriber or customer the existence of any search warrant or subpoena issued pursuant to this article nor shall a provider of electronic communication service or remote computing service disclose to a subscriber or customer that any records have been requested by or disclosed to any law enforcement unit, the Attorney General, or any district attorney pursuant to this article.

(c) A court order for disclosure issued pursuant to subsection (b) of this Code section may be issued by any superior court with jurisdiction over the offense under investigation and shall only issue such court order for disclosure if any law enforcement unit, the Attorney General, or any district attorney offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of an electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. A court issuing an order pursuant to this Code section, on a motion made promptly by a provider of electronic communication service or remote computing service, may quash or modify such order, if compliance with such order would be unduly burdensome or oppressive on such provider.

(d) (1) Any records supplied pursuant to this part shall be accompanied by the affidavit of the custodian or other qualified witness, stating in substance each of the following:

(A) The affiant is the duly authorized custodian of the records or other qualified witness and has authority to certify the records;

(B) The copy is a true copy of all the records described in the subpoena, court order, or search warrant and the records were delivered to the attorney, the attorney's representative, or the director of the Georgia Bureau of Investigation or the director's designee;

(C) The records were prepared by the personnel of the business in the ordinary course of business at or near the time of the act, condition, or event;

(D) The sources of information and method and time of preparation were such as to indicate its trustworthiness;

(E) The identity of the records; and

(F) A description of the mode of preparation of the records.

(2) If the business has none or only part of the records described, the custodian or other qualified witness shall so state in the affidavit.

(3) If the original records would be admissible in evidence if the custodian or other qualified witness had been present and testified to the matters stated in the affidavit, the copy of the records shall be admissible in evidence. When more than one person has knowledge of the facts, more than one affidavit shall be attached to the records produced.

(4) No later than 30 days prior to trial, a party intending to offer such evidence produced in compliance with this subsection shall provide written notice of such intentions to the opposing party or parties. A motion opposing the admission of such evidence shall be filed within ten days of the filing of such notice, and the court shall hold a hearing and rule on such motion no later than ten days prior to trial. Failure of a party to file such motion opposing admission prior to trial shall constitute a waiver of objection to such records and affidavit. However, the court, for good cause shown, may grant relief from such waiver.

LEXSTAT O.C.G.A. 15-6-9

OFFICIAL CODE OF GEORGIA ANNOTATED
Copyright 2007 by The State of Georgia
All rights reserved.

*** Current Through the 2007 Regular Session Annotations Current Through February 8, 2008. ***

TITLE 15. COURTS
CHAPTER 6. SUPERIOR COURTS
ARTICLE 1. GENERAL PROVISIONS

O.C.G.A. § 15-6-9 (2008)

§ 15-6-9. Authority of judges generally

The judges of the superior courts have authority:

(1) To grant for their respective circuits writs of certiorari, supersedeas, quo warranto, mandamus, habeas corpus, and bail in actions ex delicto;

(2) To entertain bills quia timet;

(3) To grant writs of injunction, prohibition, and ne exeat;

(4) To grant all other writs, original or remedial, either legal or equitable, which may be necessary to the exercise of their jurisdiction and which are not expressly prohibited;

(5) To hear and determine questions arising upon:

(A) Writs of habeas corpus or bail, when properly brought before them;

(B) All motions to grant, revive, or dissolve injunctions; and

(C) The giving of new security or the lessening of the amount of bail;

(6) To perform any and all other acts required of them at chambers;

(7) To hear and determine all motions to dismiss petitions for equitable relief, and all motions to revoke or change orders appointing receivers, after ten days' written notice has been given to the opposite party or his attorney by either party by service with a copy of such motion to dismiss or to revoke or change such order; and

(8) To administer oaths and to exercise all other powers necessarily appertaining to their jurisdiction or which may be granted them by law.

JUDICIAL DECISIONS

DUTIES OF ALL JUDGES. --Every court's judges are charged with the duty of administering justice and maintaining dignity and authority of the court. *Johnson v. State, 177 Ga. 881, 171 S.E. 699 (1933).*

PHRASE "ALL OTHER POWERS NECESSARILY APPERTAINING TO THEIR JURISDICTIONS" is broad and comprehensive. *Johnson v. State, 177 Ga. 881, 171 S.E. 699 (1933).*

COURT'S DISCRETIONARY POWER TO APPOINT ATTORNEYS. --Courts have discretionary power independent of any statutory power to appoint attorneys to assist prosecuting attorney in criminal cases. *Mach v. State, 109 Ga. App. 154, 135 S.E.2d 467 (1964).*

JUDGE OF SUPERIOR COURT HAS POWER TO APPOINT GRAND JURY FOREMAN, notwithstanding the practice that the grand jury selects its own foreman. *Johnson v. State, 177 Ga. 881, 171 S.E. 699 (1933).*

If judge of superior court requires grand jury to elect its own foreman, it is based upon authority delegated by the judge to the grand jury, and is equivalent to the exercise of the authority of the judge. *Johnson v. State, 177 Ga. 881, 171 S.E. 699 (1933).*

In the absence of any statute to the contrary, the judge of the superior court has inherent power as the presiding officer of the court to appoint the foreman of a grand jury from the number of those duly selected and required to serve. This authority vested in the judge by law is not affected by the custom of permitting the members of the grand jury to elect a foreman. *Peeples v. State, 178 Ga. 675, 173 S.E. 850 (1934).*

OFFICIAL CODE OF GEORGIA ANNOTATED
Copyright 2007 by The State of Georgia
All rights reserved.

*** Current Through the 2007 Regular Session Annotations Current Through February 8, 2008. ***

CONSTITUTION OF THE STATE OF GEORGIA
ARTICLE VI. JUDICIAL BRANCH
SECTION I. JUDICIAL POWER

Ga. Const. Art. VI, § I, Para. IV (2008)

PARAGRAPH IV. Exercise of judicial power

Each court may exercise such powers as necessary in aid of its jurisdiction or to protect or effectuate its judgments; but only the superior and appellate courts shall have the power to issue process in the nature of mandamus, prohibition, specific performance, quo warranto, and injunction. Each superior court, state court, and other courts of record may grant new trials on legal grounds.

OFFICIAL CODE OF GEORGIA ANNOTATED
Copyright 2007 by The State of Georgia
All rights reserved.

*** Current Through the 2007 Regular Session Annotations Current Through February 8, 2008. ***

CONSTITUTION OF THE STATE OF GEORGIA
ARTICLE VI. JUDICIAL BRANCH
SECTION IV. SUPERIOR COURTS

Ga. Const. Art. VI, § IV, Para. I (2008)

PARAGRAPH I. Jurisdiction of superior courts

The superior courts shall have jurisdiction in all cases, except as otherwise provided in this Constitution. They shall have exclusive jurisdiction over trials in felony cases, except in the case of juvenile offenders as provided by law; in cases respecting title to land; in divorce cases; and in equity cases. The superior courts shall have such appellate jurisdiction, either alone or by circuit or district, as may be provided by law.

JUDICIAL DECISIONS

GENERAL CONSIDERATION

LEGISLATURE AND JUDGES MAY NOT ALTER JURISDICTION OF SUPERIOR COURT. --The Constitution has vested all the judicial power in the courts of the state, and neither the legislature nor a judge, nor the judges of a superior court have authority to limit or expand the jurisdiction and authority of a superior court. *Fulton County v. Woodside, 222 Ga. 90, 149 S.E.2d 140 (1966).*

LEXSTAT 18 USCS 2703

UNITED STATES CODE SERVICE
Copyright © 2008 Matthew Bender & Company, Inc.
a member of the LexisNexis Group.
All rights reserved

*** CURRENT THROUGH P.L. 110-247, APPROVED 6/20/2008 ***
*** WITH GAPS OF 110-234 and 110-246 ***

TITLE 18. CRIMES AND CRIMINAL PROCEDURE
PART I. CRIMES
CHAPTER 121. STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

18 USCS § 2703

§ 2703. Required disclosure of customer communications or records

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

(b) Contents of wire or electronic communications in a remote computing service.
(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection--
(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or
(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity--
(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or
(ii) obtains a court order for such disclosure under subsection (d) of this section;
except that delayed notice may be given pursuant to section 2705 of this *title [18 USCS § 2705*].

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service--

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) Records concerning electronic communication service or remote computing service.

(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity--

(A) obtains 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 equivalent State warrant;

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

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

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this *title [18 USCS § 2325*]); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the--

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

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

(d) Requirements for court order. A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal

investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) No cause of action against a provider disclosing information under this chapter. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter [*18 USCS §§ 2701* et seq.].

(f) Requirement to preserve evidence.

(1) In general. A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) Period of retention. Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

(g) Presence of officer not required. Notwithstanding section 3105 of this *title [18 USCS § 3105*], the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter [*18 USCS §§ 2701* et seq.] requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

LEXSTAT 18 USCS 3117

UNITED STATES CODE SERVICE
Copyright © 2008 Matthew Bender & Company, Inc.
a member of the LexisNexis Group.
All rights reserved

*** CURRENT THROUGH P.L. 110-247, APPROVED 6/20/2008 ***
*** WITH GAPS OF 110-234 and 110-246 ***

TITLE 18. CRIMES AND CRIMINAL PROCEDURE
PART II. CRIMINAL PROCEDURE
CHAPTER 205. SEARCHES AND SEIZURES

18 USCS § 3117

§ 3117. Mobile tracking devices

(a) In general. If a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction.

(b) Definition. As used in this section, the term "tracking device" means an electronic or mechanical device which permits the tracking of the movement of a person or object.

LEXSTAT 28 USCS 1651

UNITED STATES CODE SERVICE
Copyright © 2008 Matthew Bender & Company, Inc.
a member of the LexisNexis Group.
All rights reserved

TITLE 28. JUDICIARY AND JUDICIAL PROCEDURE
PART V. PROCEDURE
CHAPTER 111. GENERAL PROVISIONS

28 USCS § 1651

§ 1651. Writs

(a) The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.

(b) An alternative writ or rule nisi may be issued by a justice or judge of a court which has jurisdiction.

UNITED STATES CODE SERVICE
Copyright © 2008 Matthew Bender & Company, Inc.

*** CURRENT THROUGH CHANGES RECEIVED APRIL 15, 2008 ***

FEDERAL RULES OF CRIMINAL PROCEDURE
TITLE VIII. SUPPLEMENTARY AND SPECIAL PROCEEDINGS

USCS Fed Rules Crim Proc R 41

Rule 41. Search and Seizure [Caution: For amendments effective December 1, 2008, see prospective amendment note to this rule.]

(a) Scope and Definitions.

(1) *Scope.* This rule does not modify any statute regulating search or seizure, or the issuance and execution of a search warrant in special circumstances.

(2) *Definitions.* The following definitions apply under this rule:

(A) "Property" includes documents, books, papers, any other tangible objects, and information.

(B) "Daytime" means the hours between 6:00 a.m. and 10:00 p.m. according to local time.

(C) "Federal law enforcement officer" means a government agent (other than an attorney for the government) who is engaged in enforcing the criminal laws and is within any category of officers authorized by the Attorney General to request a search warrant.

(D) "Domestic terrorism" and "international terrorism" have the meanings set out in *18 U.S.C. § 2331*.

(E) "Tracking device" has the meaning set out in *18 U.S.C. § 3117(b)*.

(b) Authority to Issue a Warrant. At the request of a federal law enforcement officer or an attorney for the government:

(1) a magistrate judge with authority in the district--or if none is reasonably available, a judge of a state court of record in the district--has authority to issue a warrant to search for and seize a person or property located within the district;

(2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;

(3) a magistrate judge--in an investigation of domestic terrorism or international terrorism--with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district; and

(4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both.

(c) Persons or Property Subject to Search or Seizure. A warrant may be issued for any of the following:

(1) evidence of a crime;

(2) contraband, fruits of crime, or other items illegally possessed;

(3) property designed for use, intended for use, or used in committing a crime; or

(4) a person to be arrested or a person who is unlawfully restrained.

(d) Obtaining a Warrant.

(1) *In General.* After receiving an affidavit or other information, a magistrate judge--or if authorized by Rule 41(b), a judge of a state court of record--must issue the warrant if there is probable cause to search for and seize a person or property or to install and use a tracking device.

(2) *Requesting a Warrant in the Presence of a Judge.*

(A) *Warrant on an Affidavit.* When a federal law enforcement officer or an attorney for the government presents an affidavit in support of a warrant, the judge may require the affiant to appear personally and may examine under oath the affiant and any witness the affiant produces.

(B) *Warrant on Sworn Testimony.* The judge may wholly or partially dispense with a written affidavit and base a warrant on sworn testimony if doing so is reasonable under the circumstances.

(C) *Recording Testimony.* Testimony taken in support of a warrant must be recorded by a court reporter or by a suitable recording device, and the judge must file the transcript or recording with the clerk, along with any affidavit.

(3) *Requesting a Warrant by Telephonic or Other Means.*

(A) *In General.* A magistrate judge may issue a warrant based on information communicated by telephone or other reliable electronic means.

(B) *Recording Testimony.* Upon learning that an applicant is requesting a warrant under Rule 41(d)(3)(A), a magistrate judge must:

(i) place under oath the applicant and any person on whose testimony the application is based; and

(ii) make a verbatim record of the conversation with a suitable recording device, if available, or by a court reporter, or in writing.

(C) *Certifying Testimony.* The magistrate judge must have any recording or court reporter's notes transcribed, certify the transcription's accuracy, and file a copy of the record and the transcription with the clerk. Any written verbatim record must be signed by the magistrate judge and filed with the clerk.

(D) *Suppression Limited.* Absent a finding of bad faith, evidence obtained from a warrant issued under Rule 41(d)(3)(A) is not subject to suppression on the ground that issuing the warrant in that manner was unreasonable under the circumstances.

(e) Issuing the Warrant.

(1) *In General.* The magistrate judge or a judge of a state court of record must issue the warrant to an officer authorized to execute it.

(2) *Contents of the Warrant.*

(A) *Warrant to Search for and Seize a Person or Property.* Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

(i) execute the warrant within a specified time no longer than 10 days;

(ii) execute the warrant during the daytime, unless the judge for good cause expressly authorizes execution at another time; and

(iii) return the warrant to the magistrate judge designated in the warrant.

(B) *Warrant for a Tracking Device.* A tracking-device warrant must identify the person or property to be tracked, designate the magistrate judge to whom it must be returned, and specify a reasonable length of time that the device may be used. The time must not exceed 45 days from the date the warrant was issued. The court may, for good cause, grant one or more extensions for a reasonable period not to exceed 45 days each. The warrant must command the officer to:

(i) complete any installation authorized by the warrant within a specified time no longer than 10 calendar days;

(ii) perform any installation authorized by the warrant during the daytime, unless the judge for good cause expressly authorizes installation at another time; and

(iii) return the warrant to the judge designated in the warrant.

(3) *Warrant by Telephonic or Other Means.* If a magistrate judge decides to proceed under Rule 41(d)(3)(A), the following additional procedures apply:

(A) *Preparing a Proposed Duplicate Original Warrant.* The applicant must prepare a "proposed duplicate original warrant" and must read or otherwise transmit the contents of that document verbatim to the magistrate judge.

(B) *Preparing an Original Warrant.* If the applicant reads the contents of the proposed duplicate original warrant, the magistrate judge must enter those contents into an original warrant. If the applicant transmits the contents by reliable electronic means, that transmission may serve as the original warrant.

(C) *Modification.* The magistrate judge may modify the original warrant. The judge must transmit any modified warrant to the applicant by reliable electronic means under Rule 41(e)(3)(D) or direct the applicant to modify the proposed duplicate original warrant accordingly.

(D) *Signing the Warrant.* Upon determining to issue the warrant, the magistrate judge must immediately sign the original warrant, enter on its face the exact date and time it is issued, and transmit it by reliable electronic means to the applicant or direct the applicant to sign the judge's name on the duplicate original warrant.

(f) Executing and Returning the Warrant.

(1) *Warrant to Search for and Seize a Person or Property.*

(A) *Noting the Time.* The officer executing the warrant must enter on it the exact date and time it was executed.

(B) *Inventory.* An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. The officer must do so in the presence of another officer and the person from whom, or from whose premises, the property was taken. If either one is not present, the officer must prepare and verify the inventory in the presence of at least one other credible person.

(C) *Receipt.* The officer executing the warrant must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken or leave a copy of the warrant and receipt at the place where the officer took the property.

(D) *Return.* The officer executing the warrant must promptly return it--together with a copy of the inventory--to the magistrate judge designated on the warrant. The judge must,

on request, give a copy of the inventory to the person from whom, or from whose premises, the property was taken and to the applicant for the warrant.

(2) *Warrant for a Tracking Device.*

(A) *Noting the Time.* The officer executing a tracking-device warrant must enter on it the exact date and time the device was installed and the period during which it was used.

(B) *Return.* Within 10 calendar days after the use of the tracking device has ended, the officer executing the warrant must return it to the judge designated in the warrant.

(C) *Service.* Within 10 calendar days after the use of the tracking device has ended, the officer executing a tracking-device warrant must serve a copy of the warrant on the person who was tracked or whose property was tracked. Service may be accomplished by delivering a copy to the person who, or whose property, was tracked; or by leaving a copy at the person's residence or usual place of abode with an individual of suitable age and discretion who resides at that location and by mailing a copy to the person's last known address. Upon request of the government, the judge may delay notice as provided in Rule 41(f)(3).

(3) *Delayed Notice.* Upon the government's request, a magistrate judge--or if authorized by Rule 41(b), a judge of a state court of record--may delay any notice required by this rule if the delay is authorized by statute.

(4) *Return.* The officer executing the warrant must promptly return it--together with a copy of the inventory--to the magistrate judge designated on the warrant. The judge must, on request, give a copy of the inventory to the person from whom, or from whose premises, the property was taken and to the applicant for the warrant.

(g) Motion to Return Property. A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return. The motion must be filed in the district where the property was seized. The court must receive evidence on any factual issue necessary to decide the motion. If it grants the motion, the court must return the property to the movant, but may impose reasonable conditions to protect access to the property and its use in later proceedings.

(h) Motion to Suppress. A defendant may move to suppress evidence in the court where the trial will occur, as Rule 12 provides.

(i) Forwarding Papers to the Clerk. The magistrate judge to whom the warrant is returned must attach to the warrant a copy of the return, of the inventory, and of all other related papers and must deliver them to the clerk in the district where the property was seized.

HISTORY:

(Dec. 26, 1944, eff. March 21, 1946, as amended Dec. 27, 1948, eff. Oct. 20, 1949; April 9, 1956, eff. 90 days after April 9, 1956; April 24, 1972, eff. Oct. 1, 1972; March 18, 1974, eff. July 1, 1974; April 26, 1976, eff. Aug. 1, 1976 and Oct. 1, 1977; Act July 8, 1976, P.L. 94-349, § 1, 90 Stat. 822; Act July 30, 1977, P.L. 95-78, §§ 2(e), 4, 91 Stat. 320, 322, eff. Oct. 1, 1977; eff. Aug. 1, 1979; Aug. 1, 1987; Dec. 1, 1989; Dec. 1, 1990; Dec. 1, 1993.)

(As amended Oct. 26, 2001, P.L. 107-56, Title II, § 219, 115 Stat. 291; Dec. 1, 2002; Dec. 1, 2006; Dec. 1, 2008.)

HISTORY; ANCILLARY LAWS AND DIRECTIVES

Prospective amendment:

Amendment of Rule 41, effective December 1, 2008. By order dated April 23, 2008, the Supreme Court of the United States approved the following amendments to Rule 41, effective December 1, 2008, and authorized their transmission to Congress in accordance with *28 USCS § 2072*:

Rule 41. Search and Seizure

* * * * *

(b) Authority to Issue a Warrant. At the request of a federal law enforcement officer or an attorney for the government:

* * * * *

(3) a magistrate judge -- in an investigation of domestic terrorism or international terrorism -- with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;

(4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and

(5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following:

(A) a United States territory, possession, or commonwealth;

(B) the premises -- no matter who owns them -- of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or

(C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

* * * * *

Committee Note

Subdivision (b)(5). Rule 41(b)(5) authorizes a magistrate judge to issue a search warrant for property located within certain delineated parts of United States jurisdiction that are outside of any State or any federal judicial district. The locations covered by the rule include United States territories, possessions, and commonwealths not within a federal judicial district as well as certain premises associated with United States diplomatic and consular missions. These are locations in which the United States has a legally cognizable interest or in which it exerts lawful authority and control. Under the rule, a warrant may be issued by a magistrate judge in any district in which activities related to the crime under investigation may have occurred, or in the District of Columbia, which serves as the default district for venue under *18 U.S.C. § 3238*.

Rule 41(b)(5) provides the authority to issue warrants for the seizure of property in the designated locations when law enforcement officials are required or find it desirable to obtain such warrants. The Committee takes no position on the question whether the Constitution requires a warrant for searches covered by the rule, or whether any international agreements, treaties, or laws of a foreign nation might be applicable. The rule

does not address warrants for persons, which could be viewed as inconsistent with extradition requirements.

Notes of Advisory Committee on 2006 amendments. The amendments to Rule 41 address three issues: first, procedures for issuing tracking device warrants; second, a provision for delaying any notice required by the rule; and third, a provision permitting a magistrate judge to use reliable electronic means to issue warrants.

Note to Subdivision (a). Amended Rule 41(a)(2) includes two new definitional provisions. The first, in Rule 41(a)(2)(D), addresses the definitions of "domestic terrorism" and "international terrorism," terms used in Rule 41(b)(2). The second, in Rule 41(a)(2)(E), addresses the definition of "tracking device."

Note to Subdivision (b). Amended Rule 41(b)(4) is a new provision, designed to address the use of tracking devices. Such searches are recognized both by statute, *see 18 U.S.C. § 3117(a)* and by caselaw, *see, e.g., United States v. Karo, 468 U.S. 705 (1984); United States v. Knotts, 460 U.S. 276 (1983).* Warrants may be required to monitor tracking devices when they are used to monitor persons or property in areas where there is a reasonable expectation of privacy. *See, e.g., United States v. Karo, supra* (although no probable cause was required to install beeper, officers' monitoring of its location in defendant's home raised Fourth Amendment concerns). Nonetheless, there is no procedural guidance in current Rule 41 for those judicial officers who are asked to issue tracking device warrants. As with traditional search warrants for persons or property, tracking device warrants may implicate law enforcement interests in multiple districts.

The amendment provides that a magistrate judge may issue a warrant, if he or she has the authority to do so in the district, to install and use a tracking device, as that term is defined in *18 U.S.C. § 3117(b)*. The magistrate judge's authority under this rule includes the authority to permit entry into an area where there is a reasonable expectation of privacy, installation of the tracking device, and maintenance and removal of the device. The Committee did not intend by this amendment to expand or contract the definition of what might constitute a tracking device. The amendment is based on the understanding that the device will assist officers only in tracking the movements of a person or property. The warrant may authorize officers to track the person or property within the district of issuance, or outside the district.

Because the authorized tracking may involve more than one district or state, the Committee believes that only federal judicial officers should be authorized to issue this type of warrant. Even where officers have no reason to believe initially that a person or property will move outside the district of issuance, issuing a warrant to authorize tracking both inside and outside the district avoids the necessity of obtaining multiple warrants if the property or person later crosses district or state lines.

The amendment reflects the view that if the officers intend to install or use the device in a constitutionally protected area, they must obtain judicial approval to do so. If, on the other hand, the officers intend to install and use the device without implicating any Fourth Amendment rights, there is no need to obtain the warrant. *See, e.g., United States v. Knotts, supra,* where the officers' actions in installing and following tracking device did not amount to a search under the Fourth Amendment.

Note to Subdivision (d). Amended Rule 41(d) includes new language on tracking devices. The tracking device statute, *18 U.S.C. § 3117*, does not specify the standard an applicant must meet to install a tracking device. The Supreme Court has acknowledged that the standard for installation of a tracking device is unresolved, and has reserved ruling

on the issue until it is squarely presented by the facts of a case. *See United States v. Karo, 468 U.S. 705, 718 n. 5 (1984).* The amendment to Rule 41 does not resolve this issue or hold that such warrants may issue only on a showing of probable cause. Instead, it simply provides that if probable cause is shown, the magistrate judge must issue the warrant. And the warrant is only needed if the device is installed (for example, in the trunk of the defendant's car) or monitored (for example, while the car is in the defendant's garage) in an area in which the person being monitored has a reasonable expectation of privacy.

Note to Subdivision (e). Rule 41(e) has been amended to permit magistrate judges to use reliable electronic means to issue warrants. Currently, the rule makes no provision for using such media. The amendment parallels similar changes to Rules 5 and 32.1(a)(5)(B)(i).

The amendment recognizes the significant improvements in technology. First, more counsel, courts, and magistrate judges now routinely use facsimile transmissions of documents. And many courts and magistrate judges are now equipped to receive filings by electronic means. Indeed, some courts encourage or require that certain documents be filed by electronic means. Second, the technology has advanced to the state where such filings may be sent from, and received at, locations outside the courthouse. Third, electronic media can now provide improved quality of transmission and security measures. In short, in a particular case, using facsimiles and electronic media to transmit a warrant can be both reliable and efficient use of judicial resources.

The term "electronic" is used to provide some flexibility to the rule and make allowance for further technological advances in transmitting data. Although facsimile transmissions are not specifically identified, the Committee envisions that facsimile transmissions would fall within the meaning of "electronic means."

While the rule does not impose any special requirements on use of facsimile transmissions, neither does it presume that those transmissions are reliable. The rule treats all electronic transmissions in a similar fashion. Whatever the mode, the means used must be "reliable." While the rule does not further define that term, the Committee envisions that a court or magistrate judge would make that determination as a local matter. In deciding whether a particular electronic means, or media, would be reliable, the court might consider first, the expected quality and clarity of the transmission. For example, is it possible to read the contents of the warrant in its entirety, as though it were the original or a clean photocopy? Second, the court may consider whether security measures are available to insure that the transmission is not compromised. In this regard, most courts are now equipped to require that certain documents contain a digital signature, or some other similar system for restricting access. Third, the court may consider whether there are reliable means of preserving the document for later use.

Amended Rule 41(e)(2)(B) is a new provision intended to address the contents of tracking device warrants. To avoid open-ended monitoring of tracking devices, the revised rule requires the magistrate judge to specify in the warrant the length of time for using the device. Although the initial time stated in the warrant may not exceed 45 days, extensions of time may be granted for good cause. The rule further specifies that any installation of a tracking device authorized by the warrant must be made within ten calendar days and, unless otherwise provided, that any installation occur during daylight hours.

Note to Subdivision (f). Current Rule 41(f) has been completely revised to accommodate new provisions dealing with tracking device warrants. First, current Rule 41(f)(1) has been revised to address execution and delivery of warrants to search for and seize a person or property; no substantive change has been made to that provision. New Rule 41(f)(2)

addresses execution and delivery of tracking device warrants. That provision generally tracks the structure of revised Rule 41(f)(1), with appropriate adjustments for the particular requirements of tracking device warrants. Under Rule 41(f)(2)(A) the officer must note on the warrant the time the device was installed and the period during which the device was used. And under new Rule 41(f)(2)(B), the officer must return the tracking device warrant to the magistrate judge designated in the warrant, within 10 calendar days after use of the device has ended.

Amended Rule 41(f)(2)(C) addresses the particular problems of serving a copy of a tracking device warrant on the person who has been tracked, or whose property has been tracked. In the case of other warrants, current Rule 41 envisions that the subjects of the search typically know that they have been searched, usually within a short period of time after the search has taken place. Tracking device warrants, on the other hand, are by their nature covert intrusions and can be successfully used only when the person being investigated is unaware that a tracking device is being used. The amendment requires that the officer must serve a copy of the tracking device warrant on the person within 10 calendar days after the tracking has ended. That service may be accomplished by either personally serving the person, or both by leaving a copy at the person's residence or usual abode and by sending a copy by mail. The Rule also provides, however, that the officer may (for good cause) obtain the court's permission to delay further service of the warrant. That might be appropriate, for example, where the owner of the tracked property is undetermined, or where the officer establishes that the investigation is ongoing and that disclosure of the warrant will compromise that investigation.

Use of a tracking device is to be distinguished from other continuous monitoring or observations that are governed by statutory provisions or caselaw. *See* Title III, Omnibus Crime Control and Safe Streets Act of 1968, *as amended* by Title I of the 1986 Electronic Communications Privacy Act, *18 U.S.C. §§ 2510-2520*; *United States v. Biasucci, 786 F.2d 504* (2d Cir. 1986) (video camera); *United States v. Torres, 751 F.2d 875* (7th Cir. 1984) (television surveillance).

Finally, amended Rule 41(f)(3) is a new provision that permits the government to request, and the magistrate judge to grant, a delay in any notice required in Rule 41. The amendment is co-extensive with *18 U.S.C. § 3103a(b)*. That new provision, added as part of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, authorizes a court to delay any notice required in conjunction with the issuance of any search warrants.

BALDWIN COUNTY
OCMULGEE JUDICIAL CIRCUIT
STATE OF GEORGIA

IN RE:
2006 FORD F-150 PICKUP TRUCK,
VIN XXXXXXXXXXXXXXXXXX,
REGISTERED TO JOE BUSYDOPER

APPLICATION FOR AN ORDER AUTHORIZING THE INSTALLATION, USE, SURVEILLANCE, AND MONITORING OF AN ELECTRONIC TRACKING DEVICE
AND
AFFIDAVIT IN SUPPORT THEREOF

Appearing before the undersigned Judge of Superior Court came Sgt. Dudley Dooright, Royal Canadian Mounted Police of Georgia, a duly sworn peace officer of the State of Georgia and/or a political subdivision thereof, who, having been duly sworn, makes this application for an order authorizing the installation, use, surveillance, and monitoring of an electronic tracking device and affidavit in support thereof, as follows, to-wit:

1.

Applicant has probable cause to believe, upon the basis of facts and circumstances which have come to Applicant's personal knowledge and attention from trustworthy informational sources, and accordingly avers upon information and belief that Joe Busydoper and other known and unknown persons conspiring with him are committing the crimes of importation, manufacture, sale, possession, possession with intent to distribute, purchase and distribution of cocaine hydrochloride [“cocaine”], a Schedule II narcotic drug, and other controlled substances, in violation of the Official Code of Georgia Annotated, Title 16, Chapter

13, Article 2, §30, and Title 21, United States Code, §841 (a) (1), and that they are using the above-described vehicle to commit and to facilitate the commission of these criminal acts in the Ocmulgee Judicial Circuit and the Middle and Northern Districts of Georgia.

2.

The basis of probable cause referred to in this Application are the following facts and circumstances, presented under oath first administered:

[Insert here all facts setting forth probable cause to establish that the vehicle is about to be used, within the next 7 days (staleness rules apply), to facilitate the described offense(s) and that information establishing the real-time location of the vehicle will enable LE to prevent the completion of the offense, to arrest the person(s) involved, and/or to be used as evidence in the prosecution of the persons utilizing the vehicle, etc., depending on the type of case you have. If you are using CI information, be sure to qualify your CI as reliable, just like a search warrant. Also establish p/c to support the necessity for covert entry to install, maintain (e.g., change batteries, tighten loose wires, etc.), and eventually remove the device; necessity for trespass onto curtilage or into garages, etc., in order to accomplish above, if needed; necessity to connect to vehicle power if requested; necessity to continue monitoring location even if vehicle enters into protected areas where it cannot be visually observed from public areas; necessity for monitoring vehicle even if it leaves the circuit or state; the necessity for the duration of the surveillance requested; etc.]

3.

Applicant avers that in order to continue the criminal investigation of Joe Busydoper and other known and unknown persons conspiring with him who are presently committing the offenses detailed above, it is necessary that law enforcement officers be authorized and

permitted to install and make use of a mobile electronic tracking device in or on the vehicle specified below. Applicant shows that continuous visual surveillance of the subject vehicle is not practicable for a variety of reasons, including, but not limited to, the difficulties and limitations inherent in the surveillance of a vehicle. Applicant further shows that the information submitted to the Court sets forth probable cause to believe that information and evidence concerning the aforesaid offense(s) will be ascertained upon surveillance and monitoring of the location and movement of the subject vehicle.

a) The vehicle to be surveilled:

A 2006 Ford F-150 Pickup Truck [the best vehicle made, by the way], white in color, Georgia license plate number xxx-xxx, VIN TH4KA7679MC039286, registered to Joe Busydoper.

b) The device or devices to be used will not affect the operation of the subject vehicle, and will be installed while the subject vehicle is located within the Ocmulgee Judicial Circuit.

4.

Applicant shows that in order to install, maintain and eventually remove the requested mobile electronic tracking device, it will be necessary for law enforcement officers to surreptitiously enter the described vehicle and/or any buildings and structures containing the vehicle or any premises on which the vehicle is located. Applicant shows that these entries will take place only in the Ocmulgee Judicial Circuit, and only as authorized by the Court.

5.

Applicant further shows that in order to effectuate the investigative purposes of the authorization requested herein, it will be necessary for law enforcement agents and officers to conduct surveillance and monitoring of the location and movement of the electronic tracking device in or on the

subject vehicle in any and all places within or outside the Ocmulgee Judicial Circuit, including, but not limited to, private residences and other locations not open to visual surveillance, for a reasonable period of time, not to exceed X days from the entry of the order.

WHEREFORE, on the basis of the allegations contained in this Application and Affidavit [and accompanying testimony, if offered], Applicant asks:

1) That the Court issue an Order authorizing the installation, use, surveillance and monitoring of a mobile electronic tracking device in or on the described vehicle for a reasonable time, not to exceed X days, unless the authorization is extended or renewed by the Court for good cause;

2) That the Court authorize law enforcement agents and officers to surreptitiously enter the described vehicle while physically located within the Ocmulgee Judicial Circuit, and any buildings and structures containing said vehicle or any premises on which the vehicle is located in order to install, maintain, and eventually remove the electronic tracking device in or on said vehicle;

3) That the Court authorize law enforcement agents and officers to conduct surveillance and monitoring of the location and movement of the mobile electronic tracking device in or on the subject vehicle in any and all places within or outside the Ocmulgee Judicial Circuit, including, but not limited to, private residences and other locations not open to visual surveillance, for a reasonable period of time, not to exceed X days from the entry of the order;

4) That the Court provide that no notice shall be given to the owner/occupier of the subject vehicle or location(s) entered/surveilled, and/or any person(s) whose movements and/or locations are recorded by the authorized surveillance, until

and unless such persons are indicted by a grand jury upon criminal offenses depending in whole or in part upon the evidence obtained by such surveillance, or until further Order of this Court, whichever comes first; and

5) That the Court order the sealing of this Application and Affidavit, all attached exhibits and attachments, and the Court's order.

Respectfully Submitted, this _____ day of _____, 20___.

_____
[Name and title]
[Agency]

Sworn to and subscribed before
me this____ day of _____, 20___

_____
Judge of Superior Court
Ocmulgee Judicial Circuit

Oral Testimony provided: [__] Yes _____ (Initialed by Judge)

[__] No _____ (Initialed by Judge)

[NOTE: If oral testimony is given, be sure to tape record it or immediately afterward otherwise memorialize for evidence - the judge is guaranteed to have forgotten by the time of the suppression motion.]

IN THE SUPERIOR COURT FOR BALDWIN COUNTY
OCMULGEE JUDICIAL CIRCUIT
STATE OF GEORGIA

IN RE:
APPLICATION FOR AN ORDER AUTHORIZING
THE INSTALLATION, USE, SURVEILLANCE,
AND MONITORING OF AN ELECTRONIC
TRACKING DEVICE ON A 2006 FORD
F-150 PICKUP TRUCK,
VIN XXXXXXXXXXXXXXXXX,
REGISTERED TO JOE BUSYDOPER

O R D E R

Upon consideration of the Application and Affidavit in support thereof of Sgt. Dudley Dooright, Royal Canadian Mounted Police of Georgia, [and other evidence presented before me in connection therewith], seeking an order or warrant authorizing the installation, use, surveillance, and monitoring of a mobile electronic tracking device in or on the above-described vehicle, this Court finds that the Applicant has set forth such facts and circumstances to lead a person of reasonable caution to conclude that probable cause exists to believe that the following crimes have been, are being and/or are about to be committed by Joe Busydoper and other known and unknown persons conspiring with him:

> Importation, manufacture, sale, possession, possession with intent to distribute, purchase and distribution of cocaine hydrochloride ["cocaine"], a Schedule II narcotic drug, and other controlled substances, in violation of the Official Code of Georgia Annotated, Title 16, Chapter 13, Article 2, §30, and Title 21, United States Code, §841 (a) (1);

and that the above-described vehicle is being and/or is about to be utilized to further this criminal activity as alleged in the Application.

It appearing that the Application and Affidavit has been made in good faith in furtherance of a pending criminal investigation, that it establishes probable cause to believe that the described vehicle will be used to facilitate and/or in connection with the commission of the offenses described above, that the use of the mobile electronic tracking device with respect to the described vehicle will further the aforesaid investigation, and that the electronic tracking device will be installed in or on the described vehicle in the Ocmulgee Judicial Circuit in such a manner that the installation shall not affect the operation of the vehicle,

IT IS HEREBY ORDERED that, pursuant to the holding in Dunivant v. State, 155 Ga. App. 884, as well as 18 U.S.C.A. §3117, OCGA §15-6-9, and Art. VI, § I, ¶ IV and Art. VI, §IV, ¶ I of the Georgia Constitution, agents and officers of the Ocmulgee Drug Task Force, Drug Enforcement Administration, and/or any other federal, state and/or local law enforcement officers assisting them in connection with the investigation described in the Application and Affidavit of Sgt. Dudley Dooright, Royal Canadian Mounted Police of Georgia, are hereby authorized to surreptitiously enter and re-enter the described vehicle while within the Ocmulgee Judicial Circuit, as well as any buildings and structures containing said vehicle or any premises on which said vehicle is located, and install, use, maintain, and conduct surveillance and monitoring of the location and movement of a mobile electronic tracking device in or on said vehicle in any and all places within or outside the Ocmulgee Judicial Circuit, including, but not limited to, private residences and other locations not open to visual surveillance. Said surveillance shall commence as soon as feasible, and shall continue as long as is reasonably necessary to effect the purposes of the investigation, not exceeding X days from today's date, unless said period of time is extended by this Court upon good cause shown.

a) The vehicle to be surveilled:

A 2006 Ford F-150 Pickup Truck [the best vehicle made, by the way], white in color, Georgia license plate number xxx-xxx, VIN TH4KA7679MC039286, registered to Joe Busydoper.

b) The device or devices to be used will not affect the operation of the subject vehicle, and will be installed while the subject vehicle is located within the Ocmulgee Judicial Circuit.

IT IS FURTHER ORDERED:

1. That law enforcement agents and officers shall remove the electronic tracking device as soon as practicable after the objectives of the surveillance are accomplished or the last date provided by this order and/or any extension thereof;
2. That, due to the covert nature of this installation, law enforcement agents and officers may perform the installation, maintenance and removal of the authorized device during the hours of darkness, if necessary, and that said officers and/or agents are not required to leave a copy of the court order or any other notice at the premises or vehicle entered;
3. That no notice shall be given to the owner/occupier of the subject vehicle or location(s) entered/surveilled pursuant to this Order, and/or to any person(s) whose movements and/or locations are monitored/recorded by the authorized surveillance, until and unless such persons are indicted by a grand jury upon criminal offenses depending in whole or in part upon the evidence obtained by such surveillance or until further Order of this Court, whichever first occurs;
4. That within thirty (30) days after the termination of the authorized surveillance, including any extensions thereof, the District Attorney shall submit a Return and Inventory to the Court summarizing the conduct of the surveillance undertaken pursuant to the Court's authorization, and any evidence obtained thereby; and,

5. That the surveillance authorized herein shall be permitted commencing immediately, and shall cease on the _____ day of _____, 20___, unless sooner terminated or extended by Order of this Court.

IT IS FURTHER ORDERED that the Application and Affidavit of Sgt. Dudley Dooright, Royal Canadian Mounted Police of Georgia, and all exhibits and attachments thereto, and this Order shall be sealed and remain in the custody of the Court until further Order, except that those officers effectuating this Order shall be permitted to retain copies for legitimate law enforcement and prosecution purposes.

SO ORDERED this ____ day of _____, 20 ___.

_____
JUDGE OF SUPERIOR COURT
OCMULGEE JUDICIAL CIRCUIT

IN THE SUPERIOR COURT FOR BALDWIN COUNTY
OCMULGEE JUDICIAL CIRCUIT
STATE OF GEORGIA

IN RE:

M.P.D. INVESTIGATION # x

ORDER

Upon motion of the State, upon good cause shown, and upon testimony provided to me under oath by Det. Jeff Duncan, Milledgeville Police Department, that certain records of wire, oral and/or electronic communications, not including message content, are relevant and material to the above-referenced ongoing criminal investigation and that said records are to be found in the location or in the custody of the institution(s) described below,

IT IS HEREBY THE FINDING OF THIS COURT that the State has shown by "specific and articulable facts" that there are reasonable grounds to believe that the records sought are relevant and material to an ongoing criminal investigation, and that said records kept and maintained by BellSouth Corporation and/or other providers of telecommunications services.

IT IS THEREFORE ORDERED pursuant to OCGA §16-11-66.1 and 18 USC §2701 *et seq.*, that the BellSouth Subpoena Compliance Department, 1960 West Exchange Place, Suite 165, Tucker, GA, 30083, and/or any other telecommunications services provider in possession of applicable records, provide and otherwise make available to the officer bearing this Order, for inspection and/or copying, the following records, to-wit:

1. Any and all current telephone subscriber information for telephone number (XXX)XXX-XXXX, ESN XXXXXXXX, to include the name, address, local and long distance telephone connection records including session times and durations for the immediate past three (3) months; local and long distance toll billing records for the immediate past three (3) months; current cell-site information as requested, as well as records pertaining to cell-site information for the past three (3) months, if available; telephone number or other subscriber number or identity, social security number, credit and employment information, length of service, type(s) of services provided, means and source of payment for such service (including credit card and/or bank account number), and all other relevant information in the custody of said provider.

2. Upon the request of the officer/agency set forth above, the current telephone subscriber information, to include the name, address, local and long distance telephone connection records including session times and durations for the immediate past three (3) months, local and long distance toll billing records for the immediate past three (3) months, telephone number or other subscriber number or identity, social security number, credit and employment information, length of service, type(s) of services provided, means and source of payment for such service (including credit card and/or bank account number), and all other relevant information in the custody of said provider, as to any derivative

telephone numbers and/or subscribers which appear on the records pertaining to the telephone number set forth above.

3. This Order shall apply to any and all said records pertaining to the immediate past three (3) billing cycles and to Verbatim records for the past ten (10) days, if applicable.

4. This Order shall remain in effect for a period of six (6) months from today's date, unless extended or renewed by the Court, and shall apply to any applicable records generated during that period of time.

IT IS FURTHER ORDERED that the BellSouth Subpoena Compliance Department, and/or any other telecommunications services provider in possession of applicable records, may comply with this Order by directing these records by U.S. Mail to the Milledgeville Police Dept., Attn: Det. Jeff Duncan, 125 W. McIntosh St., Milledgeville, GA, 31061, or via FAX to (912)445-0901.

IT IS FURTHER ORDERED that the existence of this Order shall not be disclosed to any person, specifically including the subscriber(s) of the above service(s), unless otherwise ordered by this Court. Any such disclosure would impede the investigation being conducted and therefore interfere with the enforcement of the law. This information is to be used as evidence by the State of Georgia in this Court.

HEREIN FAIL NOT, UNDER PENALTY OF LAW.

SO ORDERED this ____ day of _____, 20___.

_____
JUDGE OF SUPERIOR COURT
OCMULGEE JUDICIAL CIRCUIT

IN THE SUPERIOR COURT FOR BALDWIN COUNTY
OCMULGEE JUDICIAL CIRCUIT
STATE OF GEORGIA

IN RE:

GBI INVESTIGATION # XXXXXXXXXXXX

ORDER

Upon motion of the State, upon good cause shown, and upon testimony provided to me under oath by Agent John Straightarrow, GBI, that certain records of [wire] [electronic] communications, not including message content, are relevant and material to the above-referenced ongoing criminal investigation concerning violations of [Title 16 Article 6, Computer Crimes] [Title 16 Article 8, Identity Fraud] [OCGA §16-12-100, Sexual Exploitation of Children] [OCGA §16-12-100.1, Electronically Furnishing Obscene Material to Minors] [OCGA §16-12-100.2, Computer Pornography] [OCGA §16-5-90, Stalking], and that said records are to be found in the location or in the custody of the institution(s) described below,

IT IS HEREBY THE FINDING OF THIS COURT that the State has shown by "specific and articulable facts" that there are reasonable grounds to believe that the records sought are relevant and material to an ongoing criminal investigation, and that said records are being kept and maintained by XYZ Service Provider.

IT IS THEREFORE ORDERED pursuant to OCGA §§16-9-109 and 16-11-66.1, and 18 USC §2701 et seq., that the XYZ SERVICE PROVIDER, [address], provide and otherwise make available to the officer bearing this Order, for inspection and/or copying, the following records, to-wit:

_____
__

_____
___

_____
___.

IT IS FURTHER ORDERED that the XYZ Service Provider may comply with this Order by directing these records by U.S. Mail to the Georgia Bureau of Investigation, Identity Theft Unit, Attn: Agt. John Straightarrow, P.O. Box XXX, Decatur, GA XXXXX, or via FAX to (xxx)xxx-xxxx.

IT IS FURTHER ORDERED that the existence of this Order shall not be disclosed to any person, specifically including the subscriber(s) of the above service(s), unless otherwise

ordered by this Court. Any such disclosure would impede the investigation being conducted and therefore interfere with the enforcement of the law. This information is to be used as evidence by the State of Georgia in this Court.

HEREIN FAIL NOT, UNDER PENALTY OF LAW.

SO ORDERED this ____ day of _____, 20___.

_____
JUDGE OF SUPERIOR COURT
OCMULGEE JUDICIAL CIRCUIT

Tracking the Bad Guys: Legal Considerations in Using GPS[1]

I. Introduction

The ready availability and affordability of Global Positioning System (GPS) devices allows law enforcement to efficiently, accurately, and safely track the movement of vehicles.[2] The results of GPS tracking will create a permanent and credible record of precisely where the tracked vehicle was and the time it was there. To use this technology, officers must be able to lawfully get to the target vehicle and install certain devices.

- The simplest form of installation consists of a GPS receiver, antenna, power supply, and logging device that record where the vehicle has moved. Depending on the equipment, the data on the logging device can be remotely obtained electronically or may require physically retrieving the device to access the data. The devices could be in single or multiple units.

- Live tracking applications will require the above items (less perhaps the logging device), but will also require a transmitter and separate antenna for that transmitter. This article surveys some fundamental legal considerations for federal officers and agents in placing and using GPS devices to track vehicles. Because many states have separate statutory schemes, only brief mention will be made of state law in Section VIII.

II. The Law That Applies

A common question is whether Title III (wiretaps) laws are implicated in the use of GPS devices or intercepting their transmissions, and the answer is clearly no. Title 18 U.S.C. §

---

[1]By Federal Law Enforcement Training Center Legal Division Senior Instructor Keith Hodges. The author wishes to thank and commend Senior Instructor Jenna Solari for her invaluable editing skills.

[2]For an overview of how GPS works and many other technical details, to include GPS tracking technology, go to: http://en.wikipedia.org/wiki/GPS (last visited July 18, 2006). For an excellent survey of GPS uses and applicability to law enforcement, see John S. Ganz, Comment: It's Already Public: Why Federal Officers Should not Need Warrants to Use GPS Tracking Devices, 95 J. CRIM. L. & CRIMINOLOGY 1325 (Summer 2005).

2510(12)(C) specifically excludes signals by mobile tracking devices, like GPS, from federal wiretap law.

Fourth Amendment considerations do apply, however, to the installation of GPS devices. In this regard, it is all about whether officers need to intrude into an area where one has a reasonable expectation of privacy (REP) to perform the installation. If so, the Fourth Amendment applies and the officers will need a warrant. This is addressed in detail in Section IV. Section VI will address the requirement for a warrant if the tracked vehicle is moving in an REP area.

III. The Upcoming Rules of Federal Criminal Procedure and Tracking Devices

18 U.S.C. § 3117 provides that if a court is empowered to issue a warrant "or other order" for the installation of a mobile tracking device, the tracking can be conducted in districts other than the district in which the warrant was issued. The continued relevance of this statute is uncertain, however, in light of upcoming changes to Federal Rules of Criminal Procedure that provide specific rules in this area.

New Federal Rule of Criminal Procedure 41 has been substantially modified to specifically address how officers are to obtain and process warrants for tracking.[3] These changes will take effect on December 1, 2006, unless Congress takes affirmative action to block their implementation. After that date, it appears that Section 3117 will become irrelevant except for the definition of a tracking device.[4] Below is a summary of the changes.

A. Authority to issue the warrant - Rule 41(b)(4)

A magistrate judge in the district where the device will be installed may issue a warrant to install a tracking device. The issuing magistrate judge may authorize tracking in the district where the device will be installed, another district, or both.

B. Contents of the warrant - Rule 41(e)(2)(B)

The warrant must contain the following:

- Identity of the person or property to be tracked.
- Identity of the magistrate judge to whom the return on the warrant will be made.
- A reasonable period of time that the device may be used.
  - The time will not exceed 45 days.
  - Other extensions for not more than 45 days may be granted for good cause shown.[5]

---

[3]See the attachments at the end of this article for the full text of the new Rule 41 in both red line format and "clean."

[4]"As used in this section, the term 'tracking device' means an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117(b) (2006).

[5]If the results of the tracking device thus far disclose evidence of criminal activity, that fact should always be mentioned in the request for an extension.

- A command that the device be installed:
  - Within 10 days or less from the time the warrant is issued, and
  - During the daytime, unless the magistrate for good cause shown authorizes another time.
- A command that there shall be a return on the warrant.

C. Return on Warrant – Rule 41(f)(2)
Within ten days after use of the device has ended, the officer executing the warrant must make the return to the magistrate judge specified in the warrant. The return must contain the exact dates and times of both installing the device and the period in which it was used. The return must be served on the person who was tracked, or whose property was tracked, within ten days after use of the device has ended.[6]

D. Delays in the Return – Rule 41(f)(3)
Upon request of the government, the magistrate judge may delay providing the notice required by the return.

It is important to recognize that the new Rule 41 does not change the law regarding when a warrant is required to install or track. It only sets forth the procedure to request and issue a warrant if a warrant is required.[7]

IV. The Big Picture – All About REP

It is clear from federal law that people:

---

[6]Any delay in the required notification must be one "authorized by statute." See 18 U.S.C. § 3103a (2006).

[7]"The amendment [to Rule 41] reflects the view that if the officers intend to install or use the device in a constitutionally protected area, they must obtain judicial approval to do so. If, on the other hand, the officers intend to install and use the device without implicating any Fourth Amendment rights, there is no need to obtain the warrant. See e.g. United States v. Knotts, where the officer's actions in installing and following tracking device did not amount to a search under the 4th Amendment. . . . . Amended Rule 41(d) includes new language on tracking devices. . . . . The Supreme Court has acknowledged that the standard for installation of a tracking device is unresolved, and has reserved ruling on the issue until it is squarely presented by the facts of a case. The amendment to Rule 41 does not resolve this issue or hold that such warrants may issue only on a showing of probable cause. Instead, it simply provides that if probable cause is shown, the magistrate must issue the warrant. And the warrant is only needed if the device is installed (for example, in the trunk of the defendant's car) or monitored (for example, while the car is in the defendant's garage) in an area in which the person being monitored has a reasonable expectation of privacy." Judicial Conference of the United States, Report of the Advisory Committee on Criminal Rules, May 17, 2005, Committee Note, Rules App. D-34. (internal citation omitted).

- have REP in the interior of their vehicles.
- do not have REP in the exterior of their vehicles.[8]8
- have REP in certain places where a vehicle may be located, such as the curtilage of a home.

From these concepts, we can conclude that a search warrant is required under the Fourth Amendment in the following instances:

- The vehicle is located in an REP area when the GPS device is to be installed.
- No matter where the vehicle is located, officers want to intrude into the vehicle to install the device so as to better conceal or protect the device or tap into the vehicle's power supply.
- Officers want to seize a vehicle so technicians can install a device.

A search warrant is not required to attach a device to the exterior of a vehicle provided the vehicle is in a non-REP place at the time of installation. Officers may conduct a warrantless installation of a GPS device only when there is no REP in either the place the device is installed on the vehicle, or the place where the vehicle is located at the time of installation. In more practical terms, a warrant is not required to install a GPS device on the exterior of a vehicle when the vehicle is in a public

[8]New York v. Class, 475 U.S. 106 (1986); Cardwell v. Lewis, 417 U.S. 583 (1974); United States v. McIver, 186 F.3d 1119 (9th Cir. 1999), cert. denied, 528 U.S. 1177 (2000); United States v. Rascon-Ortiz, 994 F.2d 749 (10th Cir. 1993); United States v. Gonzalez-Acosta, 989 F.2d 384 (10th Cir. 1993); United States v. Muniz-Melchor, 894 F.2d 1430 (5th Cir. 1990), cert. denied, 495 U.S. 923 (1990); and United States v. Lyons, 2005 U.S. Dist. LEXIS 6963 (D. Kan. 2005).

place.[9]

V. REP Places

Exterior/interior of a vehicle. Those installations that intrude into the passenger compartment, trunk, or under the hood of the vehicle to access the vehicle's wiring or power sources, or to install a device or antenna, are "interior installations."[10] Officers should be conservative and consider an external (no REP) installation to be one that involves the installation of all

[9]One federal district court judge has agreed with a magistrate judge's recommendation that reasonable suspicion is required before placing a GPS device on the exterior of a vehicle that is located in a public place. In the author's opinion, that recommendation is unsupported by any other case except in dicta or by innuendo. The chances are, however, that this issue may not receive any further appellate review because the magistrate later concluded, and recommended the federal district court judge find, that there was not only reasonable suspicion, but also probable cause (albeit no warrant) to install the tracking device. United States v. Garcia, No. 05-CR-155-C, 2006 U.S. Dist. LEXIS 4642 (W.D. Wis. February 3, 2006); United States v. Garcia, No. 05-CR-0155-C-01, 2006 U.S. Dist. LEXIS 6424 (W.D. Wis. February 16, 2006). United States v. Garcia, No. 05-CR-155-C, 2006 U.S. Dist. LEXIS 29596 (W.D. Wis. May 10, 2006).

[10]Except when looking for a Vehicle Identification Number, the author is unaware of any case that stands for the clear proposition that a governmental intrusion under the hood of an automobile is outside the protection of the Fourth Amendment. Cases that discuss REP and the exterior of automobiles often do mention whether, as an REP factor, there has been interference with the operation of the vehicle or penetration into it. Tapping into a vehicle's power supply or placing items under the hood might trigger that factor.

components of the tracking device, and any transmitters (to include power sources and antennas), on the exterior of the vehicle.

REP and the location of vehicle during installation. Those areas where law enforcement officers have the right to be (public places) are not REP places. So, vehicles parked on public streets, in apartment parking lots,[11] and in gated communities[12] are not located in REP places. A vehicle parked in a garage or covered carport of a residence, however, is probably within the curtilage of a home, placing the vehicle in an REP area.

Residential driveways are a closer call. Federal cases support the position that there is no REP in the usual residential driveway,[13] but this determination will always be dependent on the driveway's length, what measures the homeowner has taken to remove his driveway from

---

[11] United States v. Cruz-Pagan, 537 F.2d 554 (1st Cir. 1976) and Cornelius v. State, No. A03-704, 2004 Minn. App. LEXIS 149 (Minn. Ct. App. February 10, 2004).

[12] United States v. Harris, No. 99-5435, 2001 U.S. App. LEXIS 3918 (6th Cir. March 7, 2001) and Wheeler v. State, No. 05-94-01957-CR, 1996 Tex. App. LEXIS 2546 (Tex. App. June 26, 1996).

[13] United States v. Hatfield, 333 F.3d 1189 (10th Cir. 2003); United States v. Reyes, 283 F.3d 446 (2d Cir. 2002), cert. denied, 537 U.S. 822 (2002); United States v. Hammett, 236 F.3d 1054 (9th Cir. 2001), cert. denied, 534 U.S. 866 (2001); Rogers v. Vicuna, 264 F.3d 1 (1st Cir. 2001); United States v. Garcia, 997 F.2d 1273 (9th Cir. 1993); Maisano v. Welcher, 940 F.2d 499 (9th Cir. 1991), cert. denied sub nom. Maisano v. IRS, 504 U.S. 916 (1992); United States v. Smith, 783 F.2d 648 (6th Cir. 1986); and United States v. Ventling, 678 F.2d 63 (8th Cir. 1982). For an exhaustive review of the law of driveways as REP areas, see Vanessa Rownaghi, Comment, "Driving Into Unreasonableness: The Driveway, The Curtilage, and Reasonable Expectations of Privacy," 11 AM. U.J. GENDER SOC. POL'Y & L. 1165 (2003).

public view and access, and other considerations that should be discussed with an Assistant U.S. Attorney before attempting a warrantless installation. Obtaining a warrant or waiting for the vehicle to move to a public place might be a better option.

VI. Tracking Issues: Location of the Vehicle During Tracking

Not only do Fourth Amendment REP considerations apply to the installation of GPS devices on vehicles, but tracking the vehicle itself may require a warrant. The Supreme Court has held, in a case involving Radio Frequency (RF) tracking,[14] that the Fourth Amendment warrant requirement is not triggered if the vehicle is tracked in public places, which include all public roads and highways.[15] If the tracking will be done while the vehicle is in an REP protected place, however, a warrant is required.[16]

This warrant requirement will not often arise in GPS tracking because GPS, unlike RF transmitters and receivers, does not work in areas where the GPS receiver cannot see the sky to get a signal directly from a GPS satellite. Since most REP places in which a vehicle could go are indoors or under shelter, the REP tracking issue is not a frequent concern.

In summary, no federal case requires a warrant to track in public places, assuming the installation of the device was lawful. While the Supreme Court has not yet decided the issue with regard to GPS, the Court did decide in 1983 that RF (beeper) tracking on public roadways does not trigger the Fourth Amendment.[17]

Law enforcement must always keep abreast of developments in the law, and a word of caution might be appropriate here. GPS is more intrusive than RF tracking because of GPS's ability to capture greater detail. Also, unlike RF tracking technology, GPS can be placed on a vehicle and the data retrieved many days or weeks later. Based on these differences, the prevalence

[14]Prior to GPS, law enforcement had only Radio Frequency tracking technology, also commonly called "beepers" or "beacons." This technology required placing a transmitter on the target vehicle that transmitted a radio signal that law enforcement could follow. GPS devices, on the other hand, do not send signals but must receive them from GPS satellites. In live tracking applications, a transmitter can be combined with the GPS receiver so the location of the vehicle can be transmitted.

[15]United States v. Knotts, 460 U.S. 276 (1983); United States v. Forest, 355 F.3d 942 (6th Cir. 2004) cert. denied, 543 U.S. 856 (2004) (cell-phone tracking in public place); and United States v. Moran, 349 F. Supp. 2d 425 (D.N.Y. 2005).

[16]United States v. Karo, 468 U.S. 705 (1984).

[17]United States v. Knotts, 460 U.S. 276 (1983).

of GPS tracking, and the state law uncertainty,[18] the issue may reach the Supreme Court in the next few years.

VII. Preserving the Data

One issue that may be receiving insufficient attention in the law enforcement community is the need for officers to preserve GPS tracking information for presentation in court.

[18]See Section VIII, infra.

Under federal evidence law, only the original of a writing may be admitted unless certain exceptions apply. This is the crux of the "best evidence rule.[19]" What officers see on a computer screen or the display of a GPS device is a "writing." An officer's testimony about what he saw on the screen or display - without having the writing available in court - should not withstand a best evidence objection. What is needed is either a photograph of the screen or display, or a "screen print," to satisfy the requirement for an original.[20] The best option is to download the GPS data and create a printout or display for court.

The consequences of not following these principles can be seen in United States v. Bennett.[21] Federal officers boarded a drug-laden vessel, and to determine whether the vessel had traveled "from any place outside the United States" in violation of importation laws, the officers examined the "backtrack" feature on a GPS device found onboard. The data were not downloaded from the device and the device was not seized. The trial court permitted the boarding officers to testify that the GPS display indicated the vessel had traveled from Mexican waters into those of the United States. On appeal, however, the importation conviction was reversed because the officer's testimony violated the best evidence rule.

To summarize, in any case involving GPS data seized or collected by law enforcement, officers must preserve the data and be prepared to either display the tracking information in court or have printouts available.

VIII. State Law

This article addressed U.S. Constitutional and federal law concerning GPS tracking. State law can differ widely.

- Some states follow federal law as outlined in this article.[22]
- Some states require probable cause to install devices, and others reasonable suspicion. Federal law, however, would require no articulable suspicion for cases in which tracking will be done in public places only, the vehicle is in a public place when the device is installed, and the installation is purely external.
- Some states require a warrant to track a vehicle in a public place.[23]

---

[19]FED. R. EVID. 1002.

[20]An original is the writing or recording itself, a negative or print of a photograph or, "if data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately." FED. R. EVID. 1001(3).

[21]363 F.3d 947 (9th Cir.), cert. denied, 543 U.S. 950 (2004).

[22]As of this writing, California (People v. Zichwic, 114 Cal. Rptr. 2d 733 (Cal. Ct. App. 2001)) and Nevada (Osburn v. State, 44 P.3d 523 (Nev. 2002)). In GA, see Dunivant v. State, 155 Ga. App. 884.

[23]As of this writing, Oregon (State v. Campbell, 759 P.2d 1040 (Or. 1988)); Washington (State v. Jackson, 76 P.3d 217 (Wash. 2003)); and New York (People v. Lacey, 787 N.Y.S.2d

The scope of this article does not permit a more exhaustive survey of state cases and statutes.

IX. Recommendations

Use warrants whenever possible because:

a. Warrants are more likely to fulfill the Fourth Amendment's reasonableness requirement.

b. State officers may not know whether a state court will read the state constitution to require a warrant even if the Fourth Amendment and federal case law would not.

c. Warrants give officers flexibility in the event the initial plan to make a warrantless installation is thwarted. For example, when attempting to execute a warrantless installation officers discover the vehicle has moved into an REP area, or that only an internal installation is feasible. Having a warrant in hand will still allow the installation to go forward.

d. Officers may need a warrant if they have to change out, maintain, reinstall, or retrieve the device in an REP area, as when the vehicle is garaged in an REP place after the device is installed.

680, (N.Y. Misc., 2004)).

Accessing Internal Memory of Personal Electronic Devices

Intercepting messages to and from cell phones, pagers, PDAs and other personal electronic devices is the subject of both federal and state law, and generally requires court authorization. However, simply accessing the internal memory of such personal electronic devices is not subject to the various wiretap and electronic surveillance statutes of federal and state law. There is no interception involved in accessing this internal memory, either because the message you are retrieving has already been sent/received, or because you are not retrieving messages at all (internal phone book of cell phone, PDA, or electronic Rolodex for example). See U.S. v. Diaz-Lizaraza, 981 F.2d 1216 (11th Cir. 1993); United States v. Meriwether, 917 F.2d 955, 960 (6th Cir. 1990); United States v. Reyes, 922 F.Supp. 818 (S.D.N.Y. 1996)(definition of "intercept" requires the acquisition of the data simultaneously with the original transmission, even if the intended recipient has not yet read the message). In addition, accessing the internal memory of a personal electronic device is not controlled by 18 USC Chapter 121, Stored Wire and Electronic Communications, because storage in the internal memory of such devices does not fit within the statutory definitions. 18 USC §§2510, 2701-2703. Instead, such access is controlled solely by constitutional "reasonable expectation of privacy" considerations. See U.S. v. David, 756 F Supp 1385(D Nev 1991).

In general, persons have a reasonable expectation of privacy in the internal memory of their personal electronic devices, just like they do in the contents of their wallet or "little black book." There is no legal difference between the constitutional privacy protection of a personal electronic device that a person carries, such as a pager, cell phone or PDA containing notes and phone numbers, and a wallet or a spiral-bound notepad in their pocket which also contains notes and phone numbers. There is an equal expectation and protection of privacy interests in the two types of items. This is a pretty good rule of thumb for your officers to follow: if under the circumstances being considered, officers would have the right to look into and examine the contents of a wallet, notebook, address book, etc., then they will have the authority to access the internal memory of a personal electronic device.

In general, there are four general situations when officers will be authorized to examine the internal memories of electronic devices:

- Consent
- Lost/abandoned property
- Search incident to arrest
- Search incident to execution of search warrant

A. Consent

The issues regarding consent searches are obvious and warrant little discussion. As long as the officer has obtained valid consent, the internal memory of any personal electronic device may be examined. Issues in this type of search generally focus on the validity of the consent. Given the types of devices and the information contained in them (especially PDAs), consent is rarely involved. On the other hand, in many investigations when officers have been stymied in identifying the target's cell phone number, the number was finally learned as the result of a traffic stop when an officer simply asked the target if he could "take a look at" his cell phone.

B. Lost/abandoned Property

Officers respond to the scene of a reported burglary, and find someone's wallet lying on the ground nearby. No one at the scene claims it. Officers realize that the wallet could be a clue as to the identity of the perpetrator. They will immediately open it up and examine the contents. The same holds true for the internal memory of a personal electronic device that comes into police custody in a similar way. There is no reasonable expectation of privacy in lost or abandoned property, and officers may examine it to their hearts' content.

C. As a Search Incident to Arrest

A criminal defendant is arrested and taken to jail. Officers will search any open or closed containers or hiding places that were near the defendant at the time of his arrest. Once he gets to the jail, his wallet, all his personal papers, notebooks, address books, etc., on his person are taken from him as a result of the arrest. Officers will, of course, go through these items with a fine-tooth comb looking for information. These searches are permissible as searches incident to arrest. See U. S. v. Rodriguez, 995 F2d 776, 778 (7th Cir. 1993), cert. den. 114 S.Ct. 1117(1994). See also, United States v. Edwards, 415 U.S. 800 (1974); United States v. Molinaro, 877 F.2d 1341 (7th Cir. 1989) (warrantless search of arrestee's wallet, after the subject was handcuffed and placed in vehicle, valid).

The issue of searching the internal memory of a personal electronic device incident to arrest is no different than that of searching the containers, wallet, address book, notebook, etc., above. The search must occur at or near the time and place of the arrest. See U.S. v. Belton, 453 U.S. 454 (1981); U.S. v. Chan, 830 F Supp 531 (ND Cal 1993) (officers may search a pager and seize its contents incident to arrest). Again, there is no legal difference between a "list" of telephone numbers stored in a pager, cell phone or PDA, and a list of telephone numbers written on a piece of paper found in the arrestee's pocket. See United States v. Ortiz, 84 F.3d 977 (7th Cir. 1996); United States v. Lynch, 908 F.Supp. 284 (D.Virgin Islands 1995).

One other issue bears mentioning while on this topic. When officers seize a pager from someone, usually incident to an arrest, the pager will often continue to receive communications. Federal courts have held that it is permissible for officers to capture and use the data received in a pager while it is lawfully in police custody. In U.S. v. Merriweather, 717 F2d 955 (6th Cir 1990), and other cases that have followed, the courts have held that a person does not have a reasonable expectation of privacy in a phone number sent to a pager. When a person transmits a phone number (or, presumably, a text message) to a pager, he takes the chance that it will be received by whomever is in possession of the pager. There can be no legitimate expectation of privacy in a message sent to a pager over which the sender has no control and the possessor of which the sender cannot identify (by voice, for example). Additionally, as long as the officers are legally in possession of the pager, the person from whom it was seized has no standing to assert that officers improperly obtained messages from the pager. Once the officers are legally in possession of the pager and a message comes in, the seizure of that message is not considered an "interception." Needless to say, Georgia courts have not examined this particular issue. Considering the similarity of the interception statutes, however, there is no logical reason to assume the outcome would be different.

D. Search Pursuant to Search Warrant

Officers often find pagers, cell phones, PDAs, and other personal electronic devices while executing search warrants. Questions often arise about searching the internal memory of these devices. As would be the case if officers wanted to examine notebooks, address books, or other written records, the answer lies in the warrant itself. If the search warrant permits officers to search for "records of drug trafficking" or "phone numbers" or similar records, then the officers would be authorized to search the internal memory of a personal electronic device. Needless to say, there is no question if "electronic records" are specifically included in the search warrant. However, if the search warrant authorizes only a search for "controlled substances" or "weapons" or certain clothing, it will not support the search of personal electronic devices. In *Merriweather*, the court likened the seizure of a pager pursuant to a search warrant to the "seizure of a personal telephone book believed to contain the numbers of suppliers or customers."

In U.S. v. Reyes, 798 F2d 380 (10th Cir 1986), the court held that a search warrant authorizing the seizure of drug records included records contained on a cassette tape. The court stated "in this age of modern technology and commercial availability of various forms of items, the warrant could not be expected to describe with exactitude the precise form the records would take." In *Merriweather*, the court held that a search warrant "authorizing the seizure of phone numbers is specific enough to empower the executing officer to seize the numbers in whatever form they may appear as long as the officer does so within the time authorized by the warrant."

For a more detailed discussion of this topic, refer to "Searching Pagers Incident to Arrest" by Lisa A. Regini, J.D., legal instructor at the FBI Academy. This article is available from the DOJ website (http://www.usdoj.gov/criminal/publicdocs).

See *United States v. Finley*, 2007 U.S. App. LEXIS 1806 (5th Cir. 2007)

Lopez v. State, 267 Ga. App. 532, 601 S.E. 2d 116 (2004)