



Electronic Surveillance

Electronic Surveillance Issues

- Al Martinez
- Prosecuting Attorneys' Council
- Legal Services Division, Macon Office
- (478)751-6645

Topics to be Covered

- Basics of Intercepting Protected Communications
- Obtaining Stored Wire/Electronic Communications & Transactional Records
- Electronic Tracking Devices
- Searching PDAs
- Surveillance of Prisoners
- Cell Phone Location Data

Review of Materials

Statutes Governing Interception of Communications

- Title III of Omnibus Crime Control and Safe Streets Act of 1968
 - Now codified as 18 USC §§ 2510 et seq.
 - Defines protected communications
 - Originally governed interception of wire and oral communications
 - Later amended to include electronic communications
- Georgia 1967 Invasions of Privacy Act
 - Codified as OCGA §§ 16-11-60 et seq.
 - Much the same as 2510 et seq.
 - 1995 amendment applied fed law to pens/trap and trace devices
 - 2002 amendment adopted fed law to court-authorized interceptions

Electronic Surveillance Reminder

- In Electronic Surveillance cases, the rules are often very DIFFERENT from traditional Search & Seizure.
- If you are using a “device” to conduct surveillance, constitutional issues will rarely be your first concern.
- You will more often be dealing with the various statutory protections.

Another Reminder

As noted, both federal and state statutes protect communications and govern how officers may go about intercepting them.

STATE AUTHORITIES MUST COMPLY WITH **BOTH** FEDERAL AND STATE LAW!!!

Protected Communications

- Oral Communications
- Wire Communications
- Electronic Communications

“Oral Communications” Defined

18 USC §2510(2), OCGA §16-11-62(1) & (3)

- Spoken conversation
- Not transmitted in any way
 - ▶ Distinguish from wire communication
 - ▶ Phone booth example

Protection of Oral Communications

18 USCS 2519(2), OCGA §16-11-62(1) & (3)

- Federal - “Reasonable” expectation that the communication is not subject to interception
- State - “Private conversation” originating in a “private place”
 - “Private place” is where one is reasonably entitled to expect to be free from intrusion or surveillance
- Basically the same : “Reasonable expectation of non-interception”
- NOT “reasonable expectation of privacy”
 - ▶ 2 guys in open field, Gotti examples
 - ▶ Note *McKinnon, Burgeson, Quintrell*

Interception of Oral Communications

- If a “device” is to be used
- To intercept a protected communication (“private place”)
- And there is no consent - see §16-11-66(a)
- Then you must obtain an Investigation Warrant (“T-3”)
 - ▶ Body bugs, covert listening devices, covert recorders, “Bionic Ear”, etc.
 - ▶ If covert entry needed, must be included in authorization

“Wire Communications” Defined

18 USC §2510(1), OCGA §16-11-62(4)

- “Aural transfer” of communications with aid of wire, cable, or similar connection
- “Aural transfer” means a transfer containing the human voice
- Examples
 - ▶ Landline phone (POTS)
 - ▶ Cordless/wireless phones, VOIP
 - ▶ SouthernLink, Nextel, PCS, satellite phones, etc.
 - ▶ Voice pagers

“Electronic Communications” Defined

18 USC §2510(12), OCGA §16-11-62(4)

- Any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature
- Transmitted by wire, radio, electromagnetic, photoelectronic or photo-optical system
- Not including wire or oral communications (no human voice)
- Examples
 - FAX, E-mail, computer data transfers
 - Numeric/Alphanumeric pagers
 - PDA text communications
 - Accessing secure websites - Konop

Protection of Wire/Electronic Communications

18 USCS §2511, OCGA §16-11-62(4)

- Content of wire/electronic communications ALWAYS protected
 - Both federal and state law
 - Privacy Issues DO NOT apply
 - Stolen cell phone, stolen phone service
- Investigation Warrant (T-3) required to intercept content of wire/electronic communications
 - One-party consent exception **(NOT FOR MINORS)**
 - There are other federal exceptions
 - Most are probably inapplicable to state prosecutions

Investigation Warrants

OCGA §16-11-64, 18 USCS §2518

- Requires written application, under oath
 - Usually based on investigator’s affidavit
 - Must involve “predicate offense” - 18 USC §2516(2)
 - Most serious felonies and drug cases are included
- By the AG or a DA with jurisdiction to prosecute offenses being investigated
 - See 18 USCS §2516(2)
- Before Superior Court Judge
- Application must meet requirements of §2518

Requirements for Issuance of Investigation Warrant ("T3")

18 USCS §2518

- P/C that "predicate crime" involved
- P/C that named targets using target device or place in furtherance thereof
- P/C that communications concerning predicate offenses will be intercepted
- P/C that conventional means exhausted, useless, or too dangerous
- Must ID all previous applications
- Note - numerous other technical requirements

Effect of Investigation Warrant

- Authorizes interception of protected communications:
 - ▶ Oral communications in "private place"
 - Covert mikes, bugs, etc.
 - Also authorizes entry to install, maintain, remove
 - ▶ Wire/electronic communications
 - Wiretaps
 - Interception of text msg, FAX, etc.
- Authorizes observation, photography, video of activities in protected area
 - ▶ Note: GA law only
 - ▶ Feds only require search warrant for this

Investigation Warrants - Execution

- Once authorized, surveillance must comply with federal law
 - ▶ Minimization
 - ▶ Privilege
 - ▶ Sealing
 - ▶ Other technical requirements
- Order is good for no more than 30 days
 - ▶ Unlimited extensions
 - ▶ Each must meet original §2518 conditions, plus:
 - Set forth results obtained so far
 - AND/OR explain failure to achieve results

Pens/Traps - Definitions

OCGA §§16-11-60

- GA Definitions rewritten in 2002
 - ▶ Dumped “instrument or apparatus” attached to phone line wording - no longer always applicable
 - ▶ Adopted federal 2001 USA Patriot Act definitions
 - “device or process” which records, captures or decodes
 - Takes into account new technology
- Pens record numbers dialed from target device
- Traps record phone number of devices calling to target device
 - ▶ “Caller ID”

Pens/Traps - Requirements

OCGA 16-11-64.1, 18 USCS 3121-3124

- GA adopted federal requirements in 1995
- Application must be by:
 - ▶ DA with jurisdiction over prosecution of offense, or
 - ▶ Attorney General
- To Superior Court Judge in:
 - ▶ DA’s Judicial Circuit, or
 - ▶ AG: Any judicial circuit

Pens/Traps - Application

18 USCS §3122

- Application must be in writing, under oath
- Application must comply with 18 USCS 3122
- Application must certify three things:
 - ▶ Information “likely to be obtained”
 - ▶ Is “relevant”
 - ▶ To an ongoing criminal investigation
- Must contain all info required for order in §3123
- NOT LIMITED TO “PREDICATE CRIMES”

Pens/Traps - Order

18 USCS §3123

- Order “shall issue” if Ct finds applicant has certified that information “likely” to be obtained is “relevant” to ongoing criminal investigation
- Federal Courts have found that issuing court has no discretion to deny
- Order is good for 60 days
- Unlimited 60-day extensions

Access to stored wire/electronic communications and records in GA

OCGA §§16-9-109 & 16-11-66.1, 18 USCS §§2701 *et seq.*

- Protected by federal law - 18 USCS §2701 *et seq.*
- In 2002 GA adopted federal law - §16-11-66.1
- In 2005 GA added §16-9-109
 - Note that 16-9-109 is limited in application
 - 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

Stored Wire/Electronic Communications & Records

OCGA §§16-11-66.1 & 16-9-109, 18 USC §§ 2510(17), 2701 *et seq.*

- Contents/Records of wire/electronic communications in electronic storage
 - Content in remote electronic storage
 - E-mail, Voice-mail, text messages, Western Union
 - Records (Transactional Data)
 - Toll records, Call detail records, Subscriber information, Historical cell-site information
- Defined, protected by 18 USCS §2701 *et seq.*
- Gvt. Access governed by 18 USCS §2703

Obtaining Stored Wire/Electronic Communications Records

OCGA §§16-11-66.1 & 16-9-109, 18 USCS §2703

- **Content** - Voicemail, e-mail, text messages
 - ▶ Less than 6 months old = SW only
 - ▶ More than 6 months old = SW or Ct order
- **Records (Transactional data)**
 - ▶ Subscriber info, telephone number, tolls = subpoena, SW, Ct Order
 - ▶ All other records: SW, Ct Order, consent of subscriber
- **Court Order must be by Superior Court Judge**
 - ▶ “Specific and articulable facts” showing that
 - ▶ Contents/Records sought are “relevant”
 - ▶ To ongoing criminal investigation

Electronic Tracking Devices

- **Device attached to or installed on target article**
- **Permits tracking movement of target**
 - ▶ Proximity (older technology)
 - ▶ GPS (all modern tracking devices)
- **Transmits and/or records location**
 - ▶ Homing beeper
 - ▶ Built-in memory
 - ▶ Cellular transmitter

Electronic Tracking Devices - Federal

18 USCA §3117, Rule 41 FRCP

- **Now specifically authorized by Rule 41 FRCP**
 - ▶ Rule was amended to add tracking devices in 2006
 - ▶ Prior to 2006 amendment:
 - Feds used 28 USCS 1651, the All Writs Act, as authority
 - Obtained a search warrant under previous Rule 41
- **See also 18 USCA §3117**
 - ▶ If Court is authorized to issue order for ETD
 - Court can order use of device w/i its jurisdiction
 - AND outside court’s jurisdiction if installed w/i court’s jurisdiction
 - ▶ Has been applied to fed AND state courts

Tracking Devices - GA

Note that there is
NO STATUTORY AUTHORITY
for a GA court to issue an order or a
search warrant authorizing the use of
an electronic tracking device.

Legal Justification for Tracking Device Order in GA

- See Dunivant, 155 Ga. App. 884
- Federal Authorities
 - ▶ Had no statutory authority prior to 2006
 - ▶ Used 28 USCS 1651, the All Writs Act
- Compare GA Law
 - ▶ OCGA §15-6-9(4)
 - ▶ GA Const Art VI, § I, ¶ IV Exercise of Judicial Power
 - ▶ GA Const Art VI, § IV, ¶ I Jurisdiction of Superior Courts

Use of Tracking Devices in GA

- Dunivant Court cited federal cases as authority
- Use of tracking devices is treated much like a search
 - ▶ If no trespass, no entry, no monitoring in private area, then no authorization is needed
 - ▶ Otherwise, a SW should be obtained
 - Dicta in Dunivant
 - Suggest getting a SW in any case
 - Suggest compliance with Rule 41 as much as possible
 - Note implications of 3117 - applicable to states

Searching Personal Data Devices

Accessing internal memory of cell phones, pagers, PDA's etc.

- Accessing internal memory, not intercepting transmissions to/from
- Not covered by specific statute - constitutional rules apply
- Think of them as a "little black book," or contents of defendant's wallet
- If you would be justified in looking thru one, you would the other
- Search incident to arrest, execution of s/w, etc.

Surveillance of Prisoners

- **Electronic Observation**
 - ▶ Jails specifically exempted by statute - 16-11-62(2)
- **Oral communications**
 - ▶ A jail is not a "private place" - no reasonable expectation of privacy
 - ▶ No protection from surveillance
- **Wire Communications**
 - ▶ Always protected, even in jail
 - ▶ One-party consent - express or implied
 - NOTE: Implied Consent Rule adopted by GA
 - *Smith v. State*, 254 Ga. App. 107

Cell Phone Location Data

U.S. DIST. CT., E.D.N.Y., 2008 U.S. Dist. LEXIS 97359, November 22, 2008,
Decided

- **UNRESOLVED ISSUE!!!**
- **Federal District Courts Are Split**
 - ▶ "Hybrid" Orders
 - Pen + 2703
 - Minority of Districts
 - ▶ Probable Cause Rule
 - Now in majority
- **Will Likely Remain Unresolved Until Legislation**

Questions


