Electronic Searches and Surveillance
“[T]he fantastic advances in the field of electronic communication constitute a great danger to the privacy of the individual;...indiscriminant use of such devices in law enforcement raises grave constitutional questions....”

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

Before 1967...Physical Trespass Required

- **Olmstead v. U.S.,** 277 U.S. 438 (1928): OK to tap wires in the street but not inside the home.

- **Goldman v. U.S.,** 316 U.S. 129 (1942): OK to place “detectaphone” on outer wall of office to listen to conversations inside office.

- **Silverman v. U.S.,** 365 U.S. 505 (1961): Not allowed to insert “spike mike” through the wall of a house...unauthorized penetration.

- “Reasonable expectation of privacy” theory
- The 4th Amendment protects PEOPLE, not places
Katz “Privacy” Test... evolved into 2 elements

1) whether the individual manifested a subjective expectation of privacy in the object of the search, and

2) whether society is willing to recognize that expectation as reasonable.

- GPS Tracking Device on Vehicle
- Revived the “Trespass” theory
- The Katz “Privacy” theory still alive (and growing?)
“Contents” of Communications

- Protected by 4th Amendment’s “reasonable expectation of privacy”
- Contents of letters and packages
- In-person conversations and landline/cellphone calls
- Emails, text messages, etc.
- Riley v. California, __ U.S. __, 134 S.Ct. 2473, __ L.Ed.2d __ (2014) extended protection to contents of cell phones
Non-content information
NOT protected

- The outside of letters and packages
- The outgoing and incoming “numbers” dialed or called
- The “to / from” addresses on emails
Smith v. Maryland, 442 U.S. 735 (1979): The Third-Party Doctrine

- NO 4th Amendment protection in information “voluntarily turned over to a third party.”
- Outgoing numbers that were dialed...turned over to phone company
- The sending & routing of electronic information
- Subscriber records (name, addresses, numbers)
- IP addresses
- “Historical” cell site location information (CSLI)
Reason for Hope: Justice Sotomayor in Jones

- The third-party doctrine is “ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.” 132 S.Ct. at 957.
- Therefore, “it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.” Id.
- We have to press the issue...challenge it
Electronic Communications Privacy Act of 1986 (ECPA)

- In the wake of Smith v. Maryland (1979)
- 1) Title III or “Wiretapping” (interception of communications)
- 2) Stored Communications Act or “SCA” (stored electronic communications)
- 3) Pen registers and trap and trace devices (recording all incoming & outgoing numbers)
- Justice Alito wants Congress to address cell phones, GPS, real-time records, etc.
Title III or “Wiretapping” Statutes

- 18 U.S.C. 2510-2522...and...N.C.G.S. 15A-286 through 298
- “The interception of wire, oral, or electronic communications by using an electronic, mechanical, or other device”
- Only senior U.S. Justice Department officials may apply for order
- N.C. Attorney General or designee may apply to a “judicial review panel”
- Strict procedural rules for application and order like a search warrant
Interception order issued ONLY if court (or panel) finds:

- (a) there is *probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense* enumerated [in 18 U.S.C. 2516 or G.S. 15A-290]…;

- (b) there is *probable cause for belief that particular communications concerning that offense will be obtained through such interception*;

- c) *normal investigative procedures have been tried and have failed* or reasonably appear to be unlikely to succeed if tried or be too dangerous; and

- (d) [except in special applications] there is *probable cause for belief that the place from which the...communications are to be intercepted are being used...in connection with the commission of such offense*...by such person.
Stored Communications and Transactional Records

- 18 U.S.C. 2701-2712 (no N.C. counterpart)
- Stored records or “communications at rest” (emails, phone records, electronic bulletin boards, voicemails, remote computer storage, etc.)
- Includes the
  - “CONTENTS” of electronic and wire communications, and
  - “RECORDS or OTHER INFORMATION” pertaining to the communication
Obtaining CONTENTS in Electronic Storage for 180 Days or Less

- Released only pursuant to a WARRANT [based on probable cause]
- The warrant must be issued using federal or state warrant procedures
Search Warrant Procedures

- A warrant shall issue “if there is probable cause to search for and seize a person or property....” Rule 41(d)(1) [ OR ]
- “if there is probable cause to believe that...property [or information]...constitutes evidence of an offense or the identity of a person participating in an offense. 15A-242.
- Warrant must describe with particularity the property to be searched or seized
- Warrant must be executed by authorized officer within 48 hours (or 14 days and in the daytime, Rule 41)
- An itemized receipt or inventory of items seized must be prepared
- A copy must be given to the person or left at the scene
- Copies of warrant and inventory must be returned to the issuing court
Obtaining CONTENTS in Electronic Storage for Over 180 Days

- Released by warrant based on probable cause and fed/state rules, OR
- By subpoena with “notice given to customer/subscriber”, OR
- By order pursuant to 18 U.S.C. 2703(d) order with “notice to...”

“Notice” may be delayed upon a showing of exigent circumstances...i.e., notice would result in danger to the life or safety of a person, flight from prosecution, destruction/tampering with evidence, intimidation of a witness, or seriously jeopardize an investigation.
Obtaining RECORDS and OTHER INFORMATION

- Released by WARRANT based on probable cause and fed/state rules...OR
- Released by an ORDER issued pursuant to 18 U.S.C. 2703(d)...OR
- Released pursuant to SUBPOENA for subscriber, payment information, and call details records
- Prior notice is NOT required for “records and other information”
SCA Subsection 2703(d) ORDER

- Shall issue if the government “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.”

- Applies to “contents” in storage over 180 days and “records and other information”
North Carolina Equivalent to the SCA

- There is NONE
- State orders will cite 18 U.S.C. 2701-2712
- The only relevant statute is N.C.G.S. 15A-298 that provides the SBI Director or designee may issue an administrative subpoena to a communications common carrier for **toll records or subscriber information that “are material to an active criminal investigation being conducted by the SBI.”**
Pen Registers and Trap and Trace Devices

- 18 U.S.C. 3121-3127...and...N.C.G.S. 15A-260 through 264
- Captures telephone incoming/outgoing numbers and sender/addrressee information in electronic communications
- Except may intercept “post-cut-through dialed digits”...digits that are transmitted (other than telephone numbers) such as credit card numbers, bank account numbers, Social Security numbers, or prescription numbers which constitute “content” communication. If this is the case, officials must use a Title III (“wiretap”) order based on probable cause to obtain that information.
- Since no content information is generally involved, a low standard for a PR/T&T device order...
Legal Standard for PR/T&T Device Order

- A [federal] court shall enter an order authorizing the installation and use of a PR/T&T device, if the court finds...that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. (18 U.S.C. 3123(a)(1)).

- An order authorizing the installation and use...of the device within the State shall issue if a N.C. superior court judge finds: 1) there is reasonable grounds to believe that a felony offense, or a Class A1 or Class 1 misdemeanor offense has been committed; 2) that there are reasonable grounds to suspect that the person named or described...committed the offense...; and 3) that the results of procedures involving pen registers or trap and trace devices will be of material aid in determining whether the person named...committed the offense. (N.C.G.S. 15A-263).
What to Look for in Orders Authorizing Electronic Records or Searches

- Types of Records or Searches Covered by the Order
- Lack of Jurisdiction
- Substitution of the Wrong Legal Standards
- Lack of Particularity (for orders requiring probable cause)
- Lack of Procedural Protections (for orders requiring PC)
- Review the Records for “Content Information”
Types of Records / Searches Covered by Order

- What exactly does the order seek to obtain...see sample orders (4A-E)
- Use Glossary of Technical Terminology to define (Attachment 5)
- Protected by 4th Amendment: contents of communications, GPS tracking, real-time location records...all require “probable cause”
- Unprotected, non-content records requiring “reasonable suspicion”
- Mere numbers or addresses “likely to be obtained and relevant”
Look for Lack of Jurisdiction

- GPS tracking device requires warrant based on PC (Jones)
- Search warrant issued by Superior Court judge is valid within the State (15A-243(a))
- Superior Court judge may issue order allowing use of a PR/T&T device within the State (15A-263(a))
- Federal court has jurisdiction to order searches in other states (18 U.S.C. 3117(a))
- State court may issue federal search warrant in absence of federal judge but only for searches within its district. (Rule 41(b)(1))
Lack of Jurisdiction Example: Attachment 4B and 4C

- Detective’s application and State judge’s order states:

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

Does this exceed State judge’s jurisdiction?
Substitution of the Wrong Legal Standards

- “Probable cause” is required for 4th Amendment searches (GPS tracking, cell phone searches, some content information, and maybe real-time location records)

- “Reasonable grounds to believe that some contents and records of communications are relevant and material to an ongoing criminal investigation.” (18 U.S.C. 2703(d)).

- “The information likely to be obtained...is relevant to an ongoing criminal investigation.” (18 U.S.C. 3123 for PR/T&T devices)
Example of Wrong Standard: GPS Order (4C)

“The officer has offered specific and articulable facts showing that there is probable cause to believe that above referenced vehicle(s) are being used/operated by Mr. E and that the placement, monitoring of and records obtained from the electronic tracking device...are relevant and material to an ongoing criminal investigation conducted by the Raleigh Police Department.”

Proper standard: “There was probable cause to believe that the information obtained by the installation and use of a GPS tracking device constituted evidence of an offense or would lead to the identification of a person(s) participating in the offense.”  Jones and 15A-242.
Lack of Particularity 
(for warrants/PC orders)

- Search warrants “must particularly describe the place to be searched or the things to be seized.”
- Court orders being substituted for a warrant “must contain all the indicia of a warrant” (including particularity requirements).
- The purpose of the particularity to prevent “general warrants”
- “[G]eneral warrants, whereby any officer or other person may be commanded to search suspected places without evidence of the act committed, or to seize any person or persons not named, whose offense is not particularly described and supported by the evidence, are dangerous to liberty and shall not be granted.” N.C. Const. I, 20.
Particularity Requirements

- A particularized description of the place to be searched
- A particularized description of the crime to which the search and seizure is related;
- A particularized description of the [information] to be seized;
- The order should not provide the officer with discretion in the execution of the warrant...“Nothing is left to the discretion of the officer executing the warrant.”
- The order should lay down “precise and discriminate” requirements to prevent the indiscriminant use of electronic devices to conduct a “general search.”
Procedural Safeguards (for PC orders)

- Termination of the interception when the [information] sought has been seized
- Prompt execution of the order
- A copy of the order and inventory must be given to the person or left at the scene
- A showing of exigent circumstances to overcome the want of prior notice.
- Return to the issuing court detailing the items seized
- Look at SAMPLE ORDERS...
Issues Ripe for Challenges

- Anything seized from a cellphone without a valid warrant *(Riley)*
  - Anything related to “reasonable expectation of privacy” in a gadget
  - Private Facebook postings
  - Remote electronic storage...the Cloud, etc.
- “Real-time” cellphone location records vs. “historical” CSLI *(pp. 18-19)*
  - GPS tracking (by itself) may be a “trespass”
  - Short-term GPS tracking may be a violation of “expectation of privacy”
  - Rule 41 requirements for GPS tracking
THE END.