




Law Enforcement Access to
Records of Electronic
Communications

Jeff Welty
October 2010




Terminology

- Content vs. non-content/“envelope”
- Historical vs. prospective/“real time”



Non-Content Records



Protection of Records

- Service providers' records aren't protected by the Fourth Amendment.
 - Smith v. Maryland, 442 U.S. 735 (1979)
- They are protected by federal statute: “A provider of . . . electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber . . . to any governmental entity.”
 - 18 U.S.C. § 2702(a)(3).



Permitted Disclosure

- Service provider may disclose records “if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency.”
 - 18 U.S.C. § 2702(c)(4)



Compulsory Disclosure

Process	Showing	Information Available
Subpoena	None	Basic subscriber information
Court order	Specific facts showing reasonable grounds	All
Search warrant	Probable cause	All



Compulsory Disclosure

- Administrative or trial subpoena gets basic subscriber information.
 - 18 U.S.C. § 2703(c)(2)
 - Name, address, phone number or IP address, “telephone connection records, or records of session times and durations,” payment details
 - Does not include detailed subscriber profile information, e.g., user’s DOB, email address associated with a Facebook account
 - Does not include email logs



Compulsory Disclosure

- Court order gets any non-content “record or other information pertaining to a subscriber.”
 - 18 U.S.C. § 2703(c)(1)
- Requires “specific and articulable facts showing . . . reasonable grounds to believe that . . . the records or other information sought[] are relevant and material to a[] . . . criminal investigation.”
 - 18 U.S.C. § 2703(d)



I, the undersigned applicant, first being duly sworn, say that:

1. Subscriber account information, to include IP connection logs, dates and times of login, Facebook mobile information, e-mail address(es) provided by user for Facebook profile ID [REDACTED], is believed to be material and relevant to an on-going criminal investigation being conducted by the Durham Police Department involving identity theft and fraud committed using an address in Durham, North Carolina.
2. The information sought by the Durham Police Department is believed to be material and relevant to this investigation as the user profile is associated with the suspect in the identity theft. The time frame of IP connection information requested is the most recent sixty (60) days of connection history.
3. It is in the best interest of the enforcement of the law and the administration of justice in the State of North Carolina to have this information disclosed.



Compulsory Disclosure

- Search warrant gets any non-content “record or other information pertaining to a subscriber.”
 - 18 U.S.C. § 2703(c)(1)
 - Same as a court order
- Issued “using State warrant procedures.”
 - 18 U.S.C. § 2703(c)(1)(A)
- Requires a showing of probable cause.



Cell Site Location Information

- Historical CSLI is just an example of non-content records.
- As such, it is available with a court order (or a search warrant).
- Prospective information, i.e., real-time tracking, is different.



Content

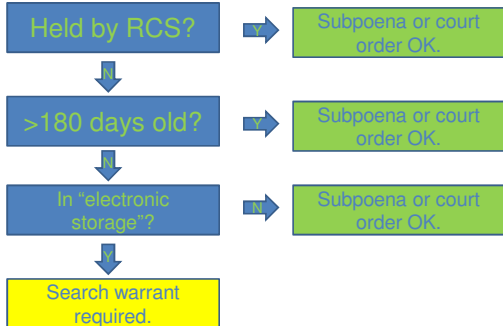


Content Is Complicated

- Depends on type of service provider
 - Electronic communication service
 - Remote computing service
- Depends on age of communication
 - Rules may be different after 180 days
- May depend on whether the communication has been “opened”
- 4th Amendment may protect content



Content Flow Chart



Practice and Procedure



Who May Seek?

- Statute says a “governmental entity.”
 - 18 U.S.C. § 2703(c)
- Appears to include officers and prosecutors.
 - My sense: mostly officers.
 - Your experience?
- Contents of a typical application.



Who May Issue?

- Court orders/search warrants may be issued only by a “court of competent jurisdiction.”
 - 18 U.S.C. § 2703(c)(1)(A), (d)
- Meaning “a court of general criminal jurisdiction . . . authorized by [state] law . . . to issue search warrants.”
 - 18 U.S.C. § 2711(3)(B)
- Includes superior courts, not clear whether district courts have “general” jurisdiction.



Notice

- Governmental entity need not notify subscriber.
 - 18 U.S.C. § 2703(c)(3)
- Order may command service provider not to notify subscriber, on showing that notification would “seriously jeopardiz[e] an investigation.”
 - 18 U.S.C. § 2705(b)



7. Applicant requests that the Court Order direct AT&T Southeast, its agents and employees, not to disclose the existence of this order or of this investigation to the subscriber, or to any other person unless otherwise directed by the Court.



Filing

- Must be filed.
 - G.S. 7A-109(a)(1)
 - If no case yet, similar to search warrant?
 - If a pending case, under seal?
- Ex parte application once charges are pending?



Discovery

- Information obtained from service provider is part of the “files of all law enforcement . . . agencies.”
 - G.S. 15A-903(a)(1)



Suppression?

- 18 U.S.C. § 2707 provides a civil cause of action against service providers for improper disclosure.
- 18 U.S.C. § 2708 states that the statutory remedies are the “only judicial remedies and sanctions for nonconstitutional violations of this chapter.”
- So, no suppression for statutory violations.



Law Enforcement Access to Records of Electronic Communications

Jeff Welty
October 2010



UNC
SCHOOL OF GOVERNMENT

www.sog.unc.edu
