I. Electronic Surveillance: Wiretapping or Pen Registers or Trap and Trace Devices

A. Introduction

- Statutes governing real-time electronic surveillance in federal criminal investigations:
  - **Wiretap statute** – 18 U.S.C. §§ 2510-2522
    - Enacted as Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (thus, known generally as “Title III”); updated by ECPA of 1986
  - **Pen Registers and Trap and Trace Devices statute** (“Pen/Trap”)
    - 18 U.S.C. §§ 3121-3127
    - Enacted in Electronic Communications Privacy Act of 1986

- Title III protects content of wire and electronic communications in transmission.

- Pen/Trap protects certain non-content information about wire and electronic communications (e.g., numbers dialed, addressing and routing information).
• “Communications”
  o “Oral” (face to face)
  o “Wire” (containing human voice)
  o “Electronic” (others, including email)


• Authorizes government attorney to apply for a court order authorizing installation of pen register and/or trap and trace device if “the information likely to be obtained is relevant to an ongoing criminal investigation.” 18 U.S.C. § 3122(b)(2)

• Key Terms
  o “Pen register” § 3127(3)
    “… a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication ….”
    ▪ Records outgoing addressing information (e.g., a number dialed from a telephone).
  o “Trap and trace device” § 3127(4)
    “… a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however that such information shall not include the contents of any communication”
    ▪ Records incoming addressing information (e.g., caller ID information).

• Providers of electronic or wire communication services may use pen/trap devices on their own networks without a court order if –
  o it relates to operation, maintenance, and testing of the communication service or to the protection of the provider’s rights or property, or to the protection of users of that service; or
  o it’s to record the fact that a wire or electronic communication was initiated or completed to protect the provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or
  o the user of that service has given consent.
  18 U.S.C. § 3121(b)

- Governs interception of the contents of wire, oral, or electronic communications – "real time" capture while the communications are in transit.
  - Accessing stored voice mail was treated as a wiretap prior to the USA PATRIOT Act of 2001 amendments.

- Key Terms
  - "Wire communication" § 2510(1)
    "… any aural transfer … of communications by … aid of wire, cable, or other like connection … furnished or operated … for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce"
    - "Aural transfer" § 2510(18)
      any "containing the human voice at any point"
    - E.g., telephone conversations are generally wire communications.
  
  - "Electronic communication" § 2510(12)
    "… any transfer of signs, signals, writing, images, sounds, data, or intelligence … by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but … not (A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device … ; or (D) electronic funds transfer information stored by a financial institution …."
    - E.g., email messages are electronic communications, as are fax transmissions, Internet chats, or any other transmission not containing the human voice.
  
  - "Intercept" § 2510(4)
    "… the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."
    - Most courts have held that the term "intercept" applies only to communications acquired contemporaneously with their transmission; not to the acquisition of stored wire or electronic communications.
  
  - "Contents" § 2510(8)
    "… any information concerning the substance, purport, or meaning of that communication"
• **Wiretap Prohibitions and Exceptions:**

  - **Prohibits:**
    - Intentional *interception* of communications
    - *Use* or *disclosure* of such intercepted contents
      - i.e., bars third parties (including the government) from wiretapping telephones or using electronic “sniffers” to read Internet traffic.

  - **Exceptions:**
    - **Court order for intercept** (aka “Title III order”) 18 U.S.C. § 2518
      - of *wire* communications in investigation of specified predicate offenses
      - of *electronic* communications in investigation of any federal felony
    - **Open to public (no reasonable expectation of privacy)**  § 2511(2)(g)(i)
    - **Computer “trespasser” communications**  § 2511(2)(i) *(new in 2001)*
      - Law enforcement may intercept a trespasser’s communications *if* all of these requirements are met:
        1. The owner or operator of the protected computer must authorize the interception of the trespasser’s communications.
        2. The person who intercepts the communications must be "lawfully engaged in an investigation."
        3. The person who intercepts the communications must have "reasonable grounds to believe that the contents of the computer trespasser’s communications will be relevant to the investigation."
        4. The interception must not acquire any communications other than those transmitted to or from the computer trespasser (unless others whose communications are also intercepted have given consent).

  "**Computer trespasser**” 18 U.S.C. § 2510(21)
  - a person who
    - accesses a protected computer without authorization and, thus, has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer, *and*
    - has no existing contractual relationship with the owner or operator of the protected computer for access to the protected computer

  - **Consent** 18 U.S.C. § 2511(2)(c)-(d)
    - actual or implied (e.g., by continued use after viewing network banner)
    - of either party, but of both/all parties in some states
Special privileges for communications providers

- In ordinary course of business (aka “extension telephone” exception) 18 U.S.C. § 2510(5)(a)
- As necessary to provision of service 18 U.S.C. § 2511(2)(a)(i)
- Protection of rights or property 18 U.S.C. § 2511(2)(a)(i)

(For example, system administrators generally may monitor hackers intruding into their networks and then disclose the fruits of that monitoring to law enforcement. This privilege, belonging to the provider, cannot be exercised by law enforcement. After the provider has communicated with law enforcement, they may be able to monitor under the computer trespasser exception.)

- Inadvertently obtained content pertaining to crime § 2511(3)(b)(iv)


D. Remedies for Violations of the Wiretap and Pen/Trap Statutes

- Civil cause of action for any person aggrieved by violation § 2520
  - Actual damage, up to $10,000 liquidated, & attorney fees
- Criminal penalties § 2511(4), § 3121(d)
- Good faith reliance on warrant or court order is complete defense to any civil or criminal action.
- Suppression of the evidence obtained § 2518(10)(a)
  - Statutory suppression of products of illegal wiretap of wire or oral communication, but not of electronic communications.
  - The Pen/Trap statute does not provide a statutory suppression remedy.
  - Constitutional violations may result in suppression of evidence wrongfully obtained.

Gaining Access to Stored Communications or Account Records

A. Introduction

- The Stored Wire and Electronic Communications and Transactional Records Access statute (“Stored Communications Act” or simply “SCA”) concerns access to and disclosure of stored wire and electronic communications or account records. – 18 U.S.C. §§ 2701-2712
• Enacted by the larger Electronic Communications Privacy Act of 1986.

• Prohibits intentional *access* by non-providers to wire or electronic communications *in electronic storage* in communications providers’ systems, absent consent or appropriate legal process. § 2701

• Describes when providers of *electronic communication services* or *remote computing services* may *voluntarily* disclose customer communications or records (§ 2702) and how such providers, such as ISPs, can be *compelled* to make such disclosures to a government entity (§ 2703).

• Whenever investigators seek stored email, account records, or subscriber information from such a service provider, they must comply with the SCA.

**B. Key Terms**

• **“Wire communication”** § 2510(1)
  “any aural transfer … of communications by … wire, cable, or other like connection … furnished or operated … for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce”

  o **“Aural transfer”** § 2510(18)
    any “containing the human voice at any point”

• **“Electronic communication”** § 2510(12)
  “any transfer of signs, signals, writing, images, sounds, data, or intelligence … by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but … not (A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device … ; or (D) electronic funds transfer information stored by a financial institution ….”

• **“Electronic communication service”** (ECS) § 2510(15)
  “any service which provides … users … the ability to send or receive wire or electronic communications”

  o SCA applies to *both* public and non-public ECS providers.

• **“Electronic storage”** § 2510(17)
  “any temporary, intermediate storage of a wire or electronic communication incidental to … electronic transmission …; and … any storage of such communication … for … backup protection ….”
Conventional view: An email in post-transmission storage (i.e., that has reached its intended destination) is no longer in “electronic storage” because the storage, whether on an end user’s computer or as a copy left on a service provider’s computer, is no longer “temporary” nor “incidental to ... transmission.” See, e.g., Fraser v. Nationwide Mutual Insurance Co., 135 F. Supp. 2d 623, 633 (E.D. Pa. 2001)


- “Remote computing service” (RCS) § 2711(2)
  “the provision to the public of computer storage or processing services by means of an electronic communications system”

- Only public providers of RCS are subject to the SCA.

- Whether an entity is a provider of “electronic communication service,” a “remote computing service” provider, or neither, depends on the nature of the particular communication sought.

- A provider can simultaneously provide “electronic communication service” with respect to one communication and “remote computing service” with respect to another communication, or a public provider can consecutively provide such services with respect to the same communication.

C. Types of Information Obtainable from Service Providers

- Basic Subscriber Information § 2703(c)(2)
  “(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)”

- Relating to identity, relationship with provider, and basic session connection records.
• **Records or Other Information Pertaining to a Customer or Subscriber**  
  § 2703(c)(1)  
  “a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)”
  
  o Referred to as “transactional records”
  
  o Includes basic subscriber information, but also includes, for example:
    * Logs that record detailed account usage
    * Logs showing sites visited and browsing patterns
    * Logs identifying email correspondents
    * Buddy list information
    * Cell-site data for wireless phone calls
    * Anything else revealing on-line usage

• **“Contents”**  
  § 2510(8)  
  “any information concerning the substance, purport, or meaning of that communication”
  
  o May be
    * In “electronic storage”, or
    * Stored by provider of “remote computing service”, or
    * Electronically stored but, technically, neither in “electronic storage” nor stored by a provider of “remote computing service.”

D. **Voluntary Disclosure by Providers**  
  § 2702

  • Providers of services not available “to the public” (i.e., private, non-subscription-based providers) may freely disclose both contents and other records relating to stored communications.

  • Disclosure **prohibitions** applying to providers of RCS or ECS services to the public  
    § 2702(a)

    o **Content** – Cannot knowingly divulge to anybody communications that are stored by the RCS or by the ECS in electronic storage.

    o **Non-content** – Cannot knowingly divulge to government.

  • **Exceptions** to content disclosure prohibitions  
    § 2702(b)

    o Public provider of ECS or RCS may divulge communication contents
      * to addressee or intended recipient, or his/her agent.
      * as authorized under Wiretap Act or compelled under § 2703.
      * with consent of originator, addressee or intended recipient, or subscriber.
• to forward the communication to its destination.
• as necessary to provide service or protect the provider’s rights or property.
• to NCMEC if mandated report of child pornography.
• to a law enforcement agency if inadvertently obtained and appear to pertain to commission of crime.
• to a government entity if provider believes, in good faith, that a related emergency involving danger of death or serious physical injury requires disclosure without delay.

• Exceptions to non-content disclosure prohibitions § 2702(c)
  o Public provider of ECS or RCS may divulge a subscriber or customer record or other information (other than communication contents)
    ▪ if served with appropriate legal process, per § 2703.
    ▪ with customer consent.
    ▪ as necessary to provide service or protect the provider’s rights or property.
    ▪ to a government entity if provider believes, in good faith, that a related emergency involving danger of death or serious physical injury requires disclosure without delay.
    ▪ to NCMEC if in connection with report of child pornography.
    ▪ to any person other than a government entity, for any reason.

E. Compelling Disclosure § 2703

• When providers are not allowed or do not choose to voluntarily disclose content or records, government can compel public or non-public providers to disclose the contents or records through appropriate legal process, depending on the nature of the communication storage.

• With Subpoena (no prior notice required)
  o Investigators can subpoena basic subscriber information.
  o Can also subpoena opened messages and other files in non-RCS storage (because the SCA does not apply to such storage by non-public providers).

• With Subpoena with Prior Government Notice to Subscriber or Customer
  o Investigators can subpoena opened email from a public provider if they comply with the notice provisions of §§ 2703(b)(1)(B) and 2705.
  o May obtain
    ▪ Basic subscriber information.
    ▪ Contents in RCS storage (including opened email).
    ▪ Contents in electronic storage more than 180 days.
• With § 2703(d) Order (no prior notice)
  o Agents need at least a § 2703(d) court order to obtain most account logs and transactional records.
  o May obtain
    ▪ Basic subscriber information.
    ▪ Transactional records.
  o May be issued
    ▪ by court of competent jurisdiction
    ▪ on specific and articulable facts
    ▪ showing reasonable grounds to believe communications or records
    ▪ are relevant and material to criminal investigation.
  o “Court of competent jurisdiction” § 2711(3)
    “has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographic limitation.”
    ▪ “Court of competent jurisdiction” § 3127(2)
      “(A) any district court of the United States (including a magistrate …) or any United States court of appeals having jurisdiction over the offense being investigated; or
      (B) a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device”
    ▪ Orders by federal courts are conferred extraterritorial effect by the statute but such orders by state courts are not.
  o Court may quash or modify order, on provider’s motion, if information or records sought unusually voluminous or compliance would cause provider undue burden.

• With § 2703(d) Order with Prior Government Notice to Subscriber or Customer
  o Investigators can obtain everything in an account except for unopened email or voicemail stored with a provider for 180 days or less using a § 2703(d) court order that complies with the notice provisions of § 2705.
  o May obtain
    ▪ Basic subscriber information.
    ▪ Transactional records.
    ▪ Contents in RCS storage (including opened email).
    ▪ Contents in electronic storage more than 180 days.
• With Search Warrant
  
  o Investigators can obtain the full contents of an account with a search warrant. The SCA does not require the government to notify the customer or subscriber when it obtains information from a provider using a search warrant.

  o May obtain
    - Basic subscriber information.
    - Transactional records.
    - Contents in RCS storage (including opened email).
    - Contents in electronic storage more than 180 days.
    - Contents in electronic storage for 180 days or less.

  o Presence of an officer is not required for service or execution of the warrant. § 2703(g)

F. Working with Providers

• In general, investigators should communicate with network service providers before issuing subpoenas or obtaining court orders that compel the providers to disclose information.

• Preservation of evidence § 2703(f)

  o Agents may direct providers to preserve existing records pending issuance of compulsory legal process.
    
    - Such requests have no prospective effect.
    
    - Such records and evidence are to be retained for up to 90 days (plus another 90 days if the request is renewed).

• Orders not to disclose existence of legal process § 2705(b)

  o Permits agents to apply for court order directing service provider not to disclose the existence of the legal process by which disclosure is compelled whenever the government itself has no legal duty to notify the customer or subscriber of the process.

  o If the relevant process is a § 2703(d) order or § 2703(a) warrant, agents can include appropriate language in the application and proposed order or warrant.

  o If agents instead seek to compel information using a subpoena, they must apply separately for this order.
Cost reimbursement § 2706

- Government entity may be required to pay a responding provider “a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in” responding to compulsory process for content or records.
  - Amount of fee is to be
    - “as mutually agreed” by the government and the provider, or
    - “as determined by the court which issued the order” in the absence of an agreement.

The Cable Act 47 U.S.C. § 551

- Restricts government access to cable operator records only when the records relate to ordinary cable services. It does not restrict SCA access by government to records relating to Internet access or telephone service provided by a cable operator.

G. Remedies

- Suppression
  - The SCA does not provide a suppression remedy for non-constitutional violations.

- Criminal penalty (for unlawful access to stored communications) § 2701(b)
  - A 5-year felony, or a 10-year felony for a repeat offense, if committed for “commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act….”
  - Otherwise a misdemeanor, or a 5-year felony for a repeat offense.

- Civil penalties
  - If civil action against the “person or entity, other than the United States, which engaged in that violation”
    - Relief can include money damages no less than $1,000 per person, equitable or declaratory relief, and a reasonable attorney's fee plus other reasonable litigation costs.
    - Willful or intentional violations can also result in punitive damages.
    - Employees of the United States may be subject to disciplinary action for willful or intentional violations.
- A good faith reliance on a court order or warrant, grand jury subpoena, legislative authorization, or statutory authorization provides a complete defense to any civil (or criminal) action.
- Qualified immunity may also be available.

  - Suits may be brought against the United States for willful violations of the SCA, Title III, or specified sections of the Foreign Intelligence Surveillance Act (50 U.S.C. § 1801).