- Searches of **Electronically stored information (ESI)** governed by 4th Amendment
- **Computer Forensics** concerns: use of scientifically derived and proven methods toward preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for purpose of facilitating or furthering reconstruction of events found to be criminal.
    - **Antiforensics:** tools for hiding, destroying, or counterfeiting the information on which digital forensics experts rely and by extension, undermining evidentiary reliability of the information.
- To ensure compliance with the 4th Amendment's particularity requirement, officers should specify the following in their applications for search warrants of ESI:
    - Crimes for which evidence is being sought for
    - Reasons why there is probable cause to believe the computer will contain such evidence
    - Dates/time frame that are relevant to the investigation
    - Relevant search strategy in practical, nontechnical terms to ensure that search doesn't become general rummaging expedition
- **Minimization** requirements: effort must be reasonably made to limit whose communication is intercepted.
- **Electronic Surveillance** by agents of government is a search and seizure governed by 4th amendment and extensive statutory requirements.
    - Permissible only of conducted pursuant to the authority of an interception order affording protections similar to those present in the use of conventional warrants
    - Application for warrant must particularly describe the search in nature, scope, and duration.
- Title III prohibits interception of wire, oral, or electronic communications by both private persons and state actors unless such interceptions were conducted with the procedures duly authorized under law.
    - **Title III** balances need to use electronic surveillance for effective law enforcement against the need to protect the privacy rights by providing for judicial supervision of all aspects of it and establishing warrant procedures based on probable cause.
    - Special **exigent circumstances** provision, allow for emergency interceptions that must be judicially supervised within 48 hours after interception has occurred or begins to occur.
        - When an emergency situation exists
        - An interception order cannot be obtained in sufficient time
- Judicially authorized interception order NOT required to covertly enter and install listening device on premise.
- Judicially authorized interceptions must terminate on attainment of authorized objective, or on expiration of order.
- Information gained must be kept confidential unless one of specific provisions of Title III authorizes disclosure.
    - Judge will put information under seal.

- Within reasonable time, but no later than 90 days, an **Inventory must be served on the persons** named in the order and on such other parties to intercepted communications as judge determines in interest of justice.
    - Can be delayed under certain circumstances.
- States are free to superimpose more rigorous requirements for electronic surveillance than those mandated by Congress in Title III, but must not water down the federally mandated safeguards of Title III.
- **Violations of oral/wire communications** result in broad suppression of illegally obtained evidence far beyond that normally prescribed.
- **Violations of electronic communications** have remedies including criminal penalties and civil suits.
- **Aggrieved person:** a person who was a party to any intercepted wire or oral communication or a person against whom interception was directed.
- Title III does NOT cover wire/oral/electronic communications when there is no reasonable expectation of privacy.
    - Surveillance when one party consents
    - Interceptions of computer trespasser
    - Willful and voluntary disclosure
    - Eavesdropping
    - Provider exemption- employee of service provider may intercept/disclose communications to protect rights or property of provider as part of ordinary course of business
    - Computer trespasser exemption
    - Public access exemption
    - Trap-and-trace devices: records incoming addressing information and Pen registers: records outgoing addressing information
    - Tracking devices
    - Tracking beepers
    - Tone-only pagers- officers can activate the pager to see suspects location or confirm identity
    - Cell phones, cell sites, GPS
        - Devices for electronic tracking are not covered by Title III b/c they do NOT "intercept" a communication.
        - Rulings on use of GPS, real-time, cell sites data searching to track suspects has been inconsistent, but generally it requires warrant before either if these tracking methods may be used.
            - **Mosaic Theory:** "detailed patchwork of information reveals so called 'mosaic' of an individual's life- a profile not simply of where they go, but also of their associations- the implications of which conjure protections of the 1st/4th amendment.
    - E-mail and Voice mail

        - **Stored Communications Act (SCA):** stored communication may be obtained by law enforcement; 1st 180 w/ a warrant, after 180 days government may access stored communications either using warrant of after giving notice to the subscriber, a subpoena.
- Title III does NOT regulate foreign intelligence surveillance. Rather **Foreign Intelligence Surveillance Act (FISA)** authorizes and regulates the electronic surveillance and physical searches of foreign powers as well as any individual/group that is not linked to foreign government but who "engages in international terrorism or activities in preparation thereof."
- FISA does NOT regulate U.S. governmental intelligence operations outside the U.S.
    - Extraterritorial investigations remain within scope of national security exemption to warrant requirement of 4th amendment.
- Any federal agent may apply for FISA warrant, but each **application must be approved by the U.S. attorney general.**
    - Unlike normal search warrants or Title III intercept orders, FISA warrants may be issued w/o any showing of probable cause to believe that crime has been or is being committed.
        - FISA only requires probable cause that surveillance is of an authorized person/group and that "significant purpose" of surveillance relates to gathering foreign intelligence or preventing harm.
- **Foreign Intelligence Surveillance Court (FISC)**: special Article III court to review FISA applications.
    - If FISC denies an application, denial may be appealed by the U.S. Department of Justice to the Foreign Intelligence Surveillance Court of Review.
    - The President, through the U.S. attorney general, is authorized to approve an application for FISA surveillance for periods up to 1 year w/o FISC approval under certain circumstances.
        - Namely, to gather intelligence from foreign governments in U.S.
        - If this is used, attorney general must certify that he/she has made requisite statutory findings and has followed all procedures mandated by FISA.
        - Certification must be provided to intelligence committees of BOTH the House of Representatives and Senate, as well as filed under seal with the FISC.
- Any judge reviewing a FISA warrant is authorized to do so ***ex parte, in camera***: judge may review relevant information on their own, w/o all of the information being disclosed to defense counsel or being revealed in open court.
    - May be done if U.S. attorney general certifies under oath that "disclosure or an adversary hearing would harm the national security of the United States."