

TO SEARCH AND SEIZE

Deborah W. Hemdal
Attorney at Law
deborah@attyhemdal.com

PRESENTER

- ▶ Deborah W. Hemdal, Esq.
 - ▶ Solo practitioner
 - ▶ Adjunct Faculty at Newbury College
 - ▶ Teaches classes in cybercrime and cyber security
 - ▶ Adjunct Faculty at Brandeis University
 - ▶ Teaches introductory classes in health care law and intellectual property law

OBJECTIVES

- ▶ Introduce basic concepts of search and seizure
- ▶ Present road search and seizure principles that apply to all searches and seizures.
- ▶ Introduce laws and cases important to search and seizure
- ▶ Focus on issues for colleges and universities
 - ▶ Computers and Computer-Related Offenses
 - ▶ Searches of students and of employees

THE FOURTH AMENDMENT

- ▶ Amendment IV
- ▶ The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.
 - ▶ https://www.law.cornell.edu/constitution/fourth_amendment

PROBABLE CAUSE

- ▶ What is probable cause?
 - ▶ Reasonable basis to believe a crime has been committed
 - ▶ Warrant Searches: Obtained by law enforcement personnel upon presentation of probable cause to a judge or magistrate
 - ▶ Warrantless Searches:
 - ▶ Plain view: The authorities don't need to shade their eyes from obvious contraband visible to the public.
 - ▶ Exigent circumstances: There is an immediate need to act and no time to get a warrant before the evidence will be lost - the aftermath of a crime, an obvious threat to safety, etc.
 - ▶ *Terry* Stop & Frisk: Law enforcement stops someone to question and has reasonable suspicion that the person has a weapon or has just or is about to engage in criminal conduct.
 - ▶ Consent searches: Law enforcement asks permission to search someone or somewhere and a person who has control of the object or place agrees.
 - ▶ Private searches by employers or schools (must still be based on reasonable suspicion).

PRIVACY IN SEARCHES

- ▶ Why is the idea of privacy important in searches?
 - ▶ The Supreme Court has ruled that people have an expectation of privacy in certain areas of their lives. Both private searches such as those done by an employer or public searches such as those done by law enforcement must respect this privacy.
 - ▶ The searchers, whether private or public, must justify their intrusion of a person's privacy. This goes back to probable cause.
 - ▶ Scope of the privacy right depends on location
 - ▶ Protection of the physical person and their personal property
 - ▶ Home/Dorm v. Office v. Shared Communal Spaces v. Public Spaces
 - ▶ Automobile Exception

WHAT IS PRIVACY? WHERE DO WE FIND IT?

- ▶ Oddly enough, it is not mentioned in the Constitution.
- ▶ Ninth Amendment: The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.
- ▶ Applied to the states through the Fourteenth Amendment.
- ▶ Amendment XIV
 - ▶ Section 1.
 - ▶ All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the state wherein they reside. No state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

REASONABLE EXPECTATION OF PRIVACY

- ▶ *Olmstead v. U.S.* (1928) - Olmstead's privacy was not violated - wiretapping was done on "public" property
- ▶ *Katz v. U.S.* (1967) - When does a person have a reasonable expectation of privacy?
- ▶ *Kyllo v. U.S.* established a two-prong test to determine whether or not there is a reasonable expectation of privacy:
 - ▶ Two prong test:
 - ▶ Does the person believe that his words/actions would be private?
 - ▶ Is the subjective privacy an expectation that society is prepared to recognize as reasonable?

COMPUTER FRAUD AND ABUSE ACT

- ▶ 18 U.S.C. § 1030 defines computer fraud and abuse
 - ▶ (1) as knowingly gaining unauthorized access to a computer or exceeding authorized access to a computer;
 - ▶ (2) intentionally gaining unauthorized access to a computer or exceeding authorized access to a computer and thereby
 - ▶ Accesses financial information
 - ▶ Information from or on any U.S. government agency or department
 - ▶ Accesses information on a protected computer
 - ▶ (3) intentionally and without authorization accesses a nonpublic computer of the U.S. government;

CFAA, cont'd

- ▶ (4) knowingly and with intent to defraud accesses or exceeds authorized access to a protected computer;
- ▶ (5)
 - ▶ (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
 - ▶ (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
 - ▶ (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.



CFAA, cont'd

- ▶ (6) knowingly and with intent to defraud traffics in any password or similar information through which a computer may be accessed without authorization, if—
 - ▶ (A) such trafficking affects interstate or foreign commerce; or
 - ▶ (B) such computer is used by or for the Government of the United States;
- ▶ (7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any—
 - ▶ (A) threat to cause damage to a protected computer;
 - ▶ (B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or
 - ▶ (C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;

WHAT IS A COMPUTER?

- ▶ **18 U.S.C. §1030 Fraud and related activity in connection with computers**
- ▶ **(e)**As used in this section—
- ▶ **(1)**the term “computer” means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;
- ▶ U.S. v. Kramer, 631 F. 3d 900 (2011)

ELECTRONIC COMMUNICATIONS PRIVACY ACT (ECPA)

- ▶ Title I - Wiretap Act: prohibits the intentional actual or attempted interception, use, disclosure, or "procure[ment] [of] any other person to intercept or endeavor to intercept any wire, oral, or electronic communication." Title I also prohibits the use of illegally obtained communications as evidence. [18 U.S.C. § 2515](#).
- ▶ Exceptions. [O]perators and service providers for uses "in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service" and for "persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act ([FISA](#)) of 1978." [18 U.S.C. § 2511](#). It provides procedures for Federal, State, and other government officers to obtain judicial authorization for intercepting such communications, and regulates the use and disclosure of information obtained through authorized wiretapping. [18 U.S.C. § 2516-18](#). A judge may issue a warrant authorizing interception of communications for up to 30 days upon a showing of probable cause that the interception will reveal evidence that an individual is committing, has committed, or is about to commit a "particular offense" listed in § 2516. [18 U.S.C. § 2518](#).

STORED COMMUNICATIONS ACT

Title II of the ECPA

- ▶ 18 USC §§ 2701 - 2712 -
 - ▶ Criminal liability applies to those who:
 - ▶ Intentionally access without authorization a facility through which an electronic communication service is provided; or
 - ▶ Intentionally exceed an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system

TITLE III OF THE ECPA

- ▶ Addresses pen registers and trace and trap devices installed by law enforcement under a warrant.

SPECIAL ISSUES IN COMPUTER SEARCHES

- ▶ How much data should you collect?
- ▶ Just exactly what does it mean to “search” a computer?
 - ▶ Separate warrants are needed for cell phones, pagers, thumb drives

CASE LAW PERTAINING TO CELL PHONE SEARCHES

- ▶ *Riley v. California* and *U.S. v. Wurie*, 573 U.S. ____ (2014): The Court has held that a warrantless search of a person and the immediate area may be carried out pursuant to a lawful arrest. In this pair of cases, the Court ruled that it was illegal to conduct a warrantless search of cell phones. Police must get a warrant to search a suspect's cellphone.
- ▶ *U.S. v. Carpenter*, 585 U.S. ____ (2018): The Court held that a person has an expectation of privacy in his cell phone records that indicate his physical location. Law enforcement must now obtain a warrant to get third-party cell phone data. Before this, law enforcement could request any and all cell phone records from a provider without a warrant. They were considered property of the provider. The cell phone owner had no privacy expectation in them.

COLLEGES

- ▶ Private colleges will be treated as private employers.
- ▶ Public colleges will be considered a state entity.
- ▶ For purposes of certain laws, particularly drug laws, campuses are considered federal property.

COLLEGE SEARCHES

- ▶ As an employer, a college can conduct some searches of employees' workspaces, computers and cell phones. These can be done either as a matter of policy or if there is probable cause.
- ▶ As a school, operating under the theory of in loco parentis, it may conduct certain searches of a student's room and electronics. These can be done either as a matter of policy or if there is probable cause.

PRIVATE EMPLOYER SEARCHES

- ▶ Can you search your employees' computers?
- ▶ 18 U.S.C. §§ 2701 - 2712 - Stored Communications Act
 - ▶ Those storing electronic communications shall not divulge them without authorization or other lawful request
- ▶ 18 U.S.C. §§ 2510 - 2522 - Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited
 - ▶ Electronic communications cannot be intercepted or disclosed without a warrant

PARAMETERS OF SEARCH

- ▶ Search must be work related - cannot be done to look for wrongdoing
- ▶ Search must be justified and permissible in scope
- ▶ *Note Bene: A government employer may not consent to a law enforcement search that he could not conduct himself

EMPLOYER SEARCHES

continued

- ▶ *United States v. Ziegler*, 474 F.3d 1184 (___ Cir. 2007) - an employer could consent to a search of a work-issued computer
- ▶ *United States v. Buettner-Janusch*, 646 F.2d 759 (2d Cir.1981) - a co-worker who shares space may consent to a search of the shared space
- ▶ *United States v. Simons*, 206 F.3d 392 (4th Cir. 2000) - if an employer has a policy stating that files will be subject to periodic searches then employee should expect those searches

PUBLIC EMPLOYER SEARCHES

- ▶ Can your employer search your workspace?
 - ▶ It depends.
 - ▶ Are the areas to be searched “public?” This means do others have access to it.
 - ▶ Does the employer retain control over the computer, files, etc?
 - ▶ *O’Connor v. Ortega*, 480 U.S. 709 (1987): While the employee may have a reasonable expectation in his workspace, employers may conduct searches if they are work-related and justified.
 - ▶ *City of Ontario, Cal. v. Quon*, 560 U.S. 746 (2010): Narrowly decided on the issue that an employer can perform warrantless searches texts on employer-issued pagers.

CAMPUS POLICE SEARCHES

- ▶ Campus Police are special state police. Campus is their jurisdiction.
 - ▶ *Commonwealth v. Smeaton*, 465 Mass. 752 (2013)

SCHOOL SEARCHES (in general)

- ▶ *New Jersey v. T.L.O.*, 469 U.S. 325 (1985): In high school settings, the same prohibitions that the 4th Amendment places on law enforcement are placed on school officials operating under color of state statute.
- ▶ This theory can be expanded to include colleges and searches of dorm rooms and backpacks.

DORM ROOMS

- ▶ General searches of dorm rooms are allowed under the same circumstances as an apartment.
 - ▶ But see *State v. Houvener*, 145 Wash. App. 408, 186 P.3d 370 (2008) (privacy protections for dorm corridors/hallways).
- ▶ In addition, colleges may have a policy stating that rooms will be periodically searched for health and safety reasons.
 - ▶ Search must be limited to health and safety concerns. See *Platteville Area Apartment v. City of Platteville*, 19 F.3d 574, 579 (7th Cir. 1999) (“if you are looking for an adult elephant, searching for it in a chest of drawers is not reasonable.”) See also *Arizona v. Hicks*, 480 U.S. 321, 325 (1987) (police searching for shooter and weapons could not turn over electronic device and record its serial number).
- ▶ *Medlock v. Indiana University*, 783 F.3d 867 (___ Cir. 2013): Resident advisors may search a dorm room with notice. This does not constitute an illegal search.

APARTMENT SEARCHES

- ▶ Generally, if there are two or more roommates, one roommate can consent to a search of common areas of an apartment or house. BUT not to private bedroom spaces or closed containers.
- ▶ HOWEVER, if one roommate objects, the police must get a warrant before searching. (*Georgia v. Randolph*, 547 U.S. 103 (2006); *Fernandez v. Cal.*, 571 U.S. ____ (2017))

AUTOMOBILE SEARCHES

- ▶ *Carroll v. U.S.* (1925) - search of automobile without warrant permissible on basis of probable cause
- ▶ *California v. Acevedo* (1991) - search of closed container in car permissible if there is probable cause
- ▶ Other factors:
 - ▶ Cars are mobile
 - ▶ Lower expectation of privacy in car

EVIDENTIARY ISSUES

- ▶ Investigative problems:
 - ▶ Expensive and time consuming
 - ▶ Make sure the searches are legal

CONCLUSION

- ▶ Electronic search law is constantly changing
- ▶ When in doubt, consult a lawyer