Foundations of Privacy

- Constitutional Privacy
- Privacy Torts
- Statutory Privacy

Constitutional Privacy

“The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man’s spiritual nature, of his feelings, and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, ***the right to be let alone*** — the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth.”

- Justice Louis D. Brandeis, dissenting [emphasis added]

Olmstead v. United States, 277 U.S. 438 (1928)

Griswold v. Connecticut, 381 U.S. 479 (1965)

- Planned Parenthood/contraceptives case
- Majority = Privacy is a fundamental right
- Implicit within the Bill of Rights (1st, 3rd, 4th and 5th Amendments)
- "Penumbra" = zones of privacy
- Dissent:

- "I like my privacy as well as the next one, but I am nevertheless compelled to admit that government has a right to invade it unless prohibited by some specific constitutional provision." Justice Black, *Id.* At 509-10.

***Katz v. United States*, 389 U.S. 347 (1967)**

- FBI recording device placed on phone booth
- Holding = electronically listening violated defendant's reasonable expectation of privacy

- This constitutes an illegal “search and seizure”
- J. Harlan, concurring
- 4th Amendment protects people, not places
- Public phone booth can temporarily become a private place with reasonable expectation of freedom from intrusion
- Now a test for 4th Amendment protection

***Smith v. Maryland*, 442 U.S. 735 (1979)**

- Use of a pen register on a phone line
- A person has a legitimate expectation of privacy when:
- (1) he "exhibited an actual (subjective) expectation of privacy" and
- (2) his subjective expectation of privacy was justifiable under the circumstances
- Contrast with *Katz*?

***US v. Maxwell*, 42 M.J. 568 (U.S.A.F. Ct. Crim. App. 1995)**

- Indecent language, distribution of obscene material, knowingly transporting/receiving child pornography via personal AOL email account
- Court notes that the Constitution requires probable cause to enter into a personal/private computer BUT this expectation of privacy diminishes as messages are sent over the Internet
- Email = a letter in a sealed envelope sent via post?

- Holding = a subscriber to an online computer service had an objectively reasonable expectation of privacy in stored email transmissions

***O'Connor v. Ortega*, 480 U.S. 709 (1987)**

- State hospital MD's office searched, items seized while on administrative leave, pending investigation of possible improprieties

- Does a state employee have a reasonable expectation of privacy in workplace or “private office”?
- Decided on a case by case basis – here, defendant has a reasonable expectation of privacy in his desk and file cabinets
- With a reasonable expectation of privacy, what is the standard for conducting searches?

Constitutional Privacy

U.S. v. Jones (US Supreme Court 2012)

- Government attaches GPS device to vehicle owned by spouse
- Obtained warrant for DC within 10 days
- Device installed on 11th day not in DC in a public parking lot
- Device sends more than 2,000 pages of data over 4 weeks
- District Court suppresses some data which obtained while vehicle was in garage adjoining Jones's residence
- Jury convicts ($850K in cash, 97 kilos of cocaine, 1 kilo of cocaine base)
- Court of Appeals reverses conviction because of admission of evidence, obtained by warrantless use of GPS device data

Constitutional Privacy

U.S. v. Jones (cont.)

- Is the installation of the GPS to monitor vehicle's movements a search?
- How important is the concept of "trespass" to assertions of privacy? Is this a useful test for privacy?
- Does *Katz* apply?
- Is the underbody of the chassis of the Jeep where Jones can have a reasonable expectation of privacy?
- Do you look at the degree of privacy expected with the Constitution was adopted?
- Scalia says mere visual observation is not a search

Constitutional Privacy

Riley Supreme Court Case history

- Trial court denied motion to suppress evidence and Riley was convicted on all 3 counts with an enhanced sentence of 15 years to life in prison after findings of smart phone search admitted into evidence
- California Court of Appeal affirmed
- California Supreme Court denied Riley's petition for review
- U.S. Supreme Court accepts petition for certiorari

Constitutional Privacy

Brima Wurie Supreme Court Case History

- Wurie was charged and he moved to suppress the evidence obtained from the search of the apartment, arguing that it was the fruit of an unconstitutional search of the cell phone
- District Court denied the motion to suppress and he was convicted on 3 counts and sentence to 262 months in prison
- Divided First Circuit Court of Appeals reversed and vacated his convictions
- U.S. Supreme Court grants certiorari

- Supreme Court hears 2 cases together
  - Riley and U.S. v. Brima Wurie – both of which involve cell phone evidence

- 8 Supreme Court Justices joined majority opinion plus 1 Justice wrote separate opinion concurring in judgment

Riley and Brima Wurie Decided Together

Common question of the 2 cases: Whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested

Riley contends the searches of his smart phone violated the 4th Amendment because the police performed the search without a warrant and were not otherwise justified by exigent circumstances

Constitutional Privacy

Riley Facts

- Riley was stopped by police officer for driving with expired tags
- In course of the stop, the officer learned that Riley's driver's license had been suspended
- Officer impounded Riley's car pursuant to department policy
- Another officer conducted an inventory search of Riley's car
- Riley was arrested for possession of concealed weapons and loaded firearms

when 2 handguns were found under the hood of Riley's car

Riley Fact (cont.)

- Cell phone was a "smart" phone
- Officer looking at phone saw the letters "CK" preceded words on the phone – presumably in text messages or contacts
- Letters "CK" believed by officers to be referring to "Crip Killers" – slang term for members of the Bloods gang
- At police station, 2 hrs after arrest, detective specializing in gangs further examined the smart phone

- Detective, noted among “lots of stuff” on the phone, videos of young men sparring while someone yelled encouragement using the moniker “Blood”
- Also on the phone were photos of Riley in front of a vehicle that had been involved in a shooting a few weeks earlier

Constitutional Privacy

Brima Wurie Facts

- Police officer doing routine surveillance observed Wurie make an apparent drug sale from a car
- Wurie arrested and taken to police station
- At police station, 2 cell phones seized from Wurie

- The one in issue was “flip phone” which was receiving phone calls from a source shown as “my house” on the phone’s external screen
- When officers “flipped open” the phone, they saw a photo of a woman and a baby as the wallpaper
- They pressed the button to see the call log
- Then pressed another button to determine the phone number
- Then with the phone number they traced it via online directory to an apartment building

Brima Wurie Facts *(cont.)*

- Going to the apartment building, they find Wurie's name on a mailbox and observed through a window a woman resembling the woman in the photo wallpaper on Wurie's phone
- They secured the apartment while obtaining a search warrant
- With the warrant they searched the apartment and found 215 grams of crack cocaine, marijuana, drug paraphernalia, a firearm, ammunition and cash

Riley and Wurie Analysis

- Without a warrant, the search is reasonable only if it falls within a specific exception to the warrant requirement (e.g. incident to a lawful arrest)
- *Chimel (1969)* authorizes police to search a vehicle "only when the arrestee is unsecured and within reaching distance of the passenger compartment at time of search"
- *Robinson* (1973) OK'd pat down which found a cigarette package in pocket containing heroin capsules – search incident to arrest requires no additional justification even without concern about loss of evidence or concern Robinson was armed
- *Gant* (2009) adds exception when it is reasonable to believe evidence relevant to the crime of arrest may be found in the vehicle
- Factors:

- Harm to officers
- Destruction of evidence
- Is a search acceptable because a person is in custody?
- Are cell phones different than a cigarette package?

***United States v. Stanley*, 753 F.3d 114 (3d Cir. 2014)**

- "MoocherHunter" case
- Background:
- Pennsylvania State Police investigating online distribution of child pornography through Gnutella
- Identified IP address and its user ("Neighbor")

- Upon warrant and search, no evidence of child pornography or Gnutella on Neighbor's computers – non-password protected WiFi
- "Mooching" computer private IP address identified
- MoocherHunter used to find Stanley
- Issue = warrant required to use MoocherHunter?

United States v. Stanley – Appellate Court

- When does a search occur?
- What test does the Third Circuit use? (Hint – *Smith v. Maryland*)

- Subjective expectation of privacy; and
- Whether expectation is objectively justifiable under the circumstances
- NOT a rational expectation by an individual – consider whether society recognizes as a legitimate expectation of privacy
- How is this different from *Kyllo?*

United States v. Stanley – District Court

- Stanley's response:
- Warrantless search occurred, per *Kyllo v. United States*, 533 U.S. 27 (2001)

- District court:
- No reasonable expectation of privacy in wireless signal
- Distinguished from *Kyllo* case
- If Stanley had been using his own connection, Penn State Police would've followed same warrant procedure to find his information
- Otherwise, incentivize the stealing of WiFi?
- "That [Stanley] established an unauthorized connection does not convert his subjective expectation of privacy into a reasonable one."

Traft v. Commonwealth, 593 SW.3d 647 (2018)

- Background:

- License plate reader used by sheriff's deputy
- Defendant Traft stopped, arrested for DUI and active warrant
- Trial court, Court of Appeals = denied Traft's motion to suppress
- *Katz*, 4th Amendment cited
- Reasonable expectation of privacy…
- In license plate?
- In information connected to license plate?
- Reasonable reason for stopping Traft?

***U.S. v. Riley*, 858 F.3d 1012 (6th Cir. Tenn. June 5, 2017)**

- Background:
- Police officers obtained warrant to arrest Riley for armed robbery
- Two days later, Riley's girlfriend gave police his cell phone number
- Next day, officers obtain a court order, compelling AT&T to provide a record of Riley's cell-site location information, phone calls and real time GPS tracking
- Within hours, Riley is found at the Airport Inn in Memphis, TN
- Riley is arrested and charged with being a felon in possession of a firearm

- Issue:
- 4th Amendment search occur when government tracked defendant's public movements using real-time GPS cell phone data?

U.S. v. Riley (cont.)

- Riley's response:
- Government was required to obtain a warrant based on probable cause to obtain cell phone records, GPS location
- Sounds like…*Kyllo*?
- Use of a tracking device to obtain information from inside a dwelling that could not be observed by visual surveillance is a Fourth Amendment search

- BUT, the court held that the government learned no more about Riley's whereabouts from tracking GPS data than what Riley exposed to public view by travelling to

  motel "along public thoroughfares"

- Tracking didn't reveal his exact room, after all…

***Carpenter v. US*, 585 U.S. ____ (2018)**

- Background:
- In 2011, four men arrested in connection with robberies of Radio Shack and T-Mobile stores in Detroit area
- One claimed that a group of 15 robbed stores in Michigan and Ohio

- Gave his phone to the FBI
- FBI requested transactional records from federal magistrate judge under Stored Communications Act
- No warrant
- Found Carpenter through use of cell-site records, was within two miles of four robberies
- Jury convicted Carpenter of aiding and abetting robbery, sentenced to over 116 years in federal prison
- Issue = is use of cell-site records a 4th Amendment search?

***Carpenter v. US*, 585 U.S. ____ (2018)**

Holding:

- Yes, the acquisition of Carpenter's cell-site records was a 4th

Amendment search

- *Katz, Smith* cited
- Data = at intersection of expectation of privacy in physical location, movements and expectation of privacy in information voluntarily turned over to third parties
- Narrow decision – prior decisions undisturbed
- Also, warrant supported by probable cause not obtained
- "A warrant is required only in the rare case where the suspect has ***a legitimate privacy interest*** in records held by third party."

Privacy Torts

Privacy Torts

Restatement (Second) of Torts, §§ 652 A-E (1977)

- Four types of actionable privacy invasions:
- Intrusion upon one's seclusion
  - Publicity that places one in a false light
  - Misappropriation of one's name or likeness for commercial purposes
  - **Public disclosure of private facts**

Privacy Torts

Public Disclosure of Private Facts

- Restatement (Second) of Torts § 652D:
- One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that
- (a) would be highly offensive to a reasonable person, and
- (b) is not of legitimate concern to the public.
- *Sipple v. Chronicle Publishing*, 154 Cal. App. 3d 1044 (1984)
- Ex-Marine Oliver Sipple helped thwart assassination attempt of President Gerald Ford
- Sued two newspapers for revealing his sexual orientation in stories related to attempt
- Sipple was unsuccessful – evidence sufficiently established that his sexual orientation was readily known by many members of public

Statutory Privacy

Statutory Privacy

Examples

- Electronic Communications Privacy Act, 18 U.S.C. § 2510 et seq.
- Federal Educational Rights & Privacy Act, 20 U.S.C. § 1232g
- Illegal Access to a Computer
- Federal – Computer Fraud & Abuse Act, 18 U.S.C. § 1030
- Kentucky – KRS 434.840 - .860
- Disclosure of Video Tape Rentals, 18 U.S.C. § 2710
- Privacy Act of 1974, 5 U.S.C. § 552
- Privacy Protection Act of 1980, 42 U.S.C. § 2000aa - aa-12
- Kentucky Open Records Act, KRS 61.870-.884

- Health Insurance Portability and Accountability Act, 45 CFR 160, 164

Web-Based Privacy Issues

- Internet Privacy
- Consumer Online Privacy
- Social Networking Privacy
- Cell Phone Privacy
- Email Privacy
- Cybersecurity
- Location Tracking
- Surveillance Technologies
- Consumer Privacy
- Workplace Privacy

International Privacy

See http://ec.europa.eu/justice/data-protection/reform/index_en.htm

- European Union General Data Directive Regulation (GDPR)
  - Regulation 2016/679 effective May 25, 2018
  - http://eur-lex.europa.eu/legalcontent/en/TXT/?uri=CELEX%3A32016R0679
  - Directive 2016/680 to be implemented by member states by May 6, 2018
  - http://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG

- Other countries adopting GDPR like statutes & regulations

EU Privacy Fundamentals

Background

- Data Privacy is a fundamental right that cannot be easily bargained away
- There must be a lawful basis for all processing (e.g. consent, required by law, needed to perform a contract)
- This basis should be balanced against the impact on individuals
- Processing is subject to **principles** (*See definitions on later slide*)
- Scope of data protected is broader than in the US

- Certain categories or types of data have additional rules (e.g. political opinions, genetics or biometrics, criminal background, sexual orientation, health data, religious beliefs or philosophies)

Scope of the GDPR

Impacts more than just citizens of the EU

- EU law always provides protection of a **natural person** who is in the EU, irrespective of nationality
- For US institutions, **natural persons** could be:
- Students going to study abroad programs in the EU
- Faculty & staff who are hired in the EU or who work in the EU
- Other 3rd parties like a contractor or vendor in the EU

- Could also impact international students, located in the EU, applying and then enrolling to the US university or to online courses provided by the US university

GDPR (cont.)

Who Does It Apply To?

- Applies to the processing of personal data by a controller or processor **established in the EU**, regardless of whether the processing takes place in the EU or not
- Applies to the processing of personal data of individuals in the EU by a controller or processor not established in the EU if:
- **Related to the offering of goods or services** to the individuals in the EU, or

- The **monitoring of the individual's behavior takes place in the EU**
- Applies to the processing of personal data by a controller not established in the EU but in a place where an EU member state

(country) law applies by virtue of public international law

GDPR (cont.)

Definitions

- **Controller**: the entity that determines the purposes and means of the processing of personal data
- **Processor**: an entity that processes personal data only on behalf of and on the instructions of the controller (e.g. a service provider)

- *The rules and obligations and penalties/fines vary dependent upon your organization's role as a controller or a processor*
- *More processor obligations will be contractual rather than legal/regulatory*

GDPR (cont.)

Definitions (cont.)

- **Personal data**: any information relating to an identified or identifiable person (e.g. name, id number, IP address, image, location data)
- **Processing**: any operation(s) which are performed on personal data (automated or not) such as collecting, recording, organizing, structuring, storing, retrieving,

disclosing, disseminating, altering, destroying, erasing or otherwise making available

- Processing is subject to **principles**: must be lawful, for specified purposes, adequate, relevant, proportionate, accurate, secure and retained only as long as necessary

Other Countries

A sample

- Saudi Arabia Personal Data Protection Law (PDPL) implemented by Royal Decree effective March 13, 2022 and will cover personal data of Saudis outside Saudi Arabia
- Australia and New Zealand – Some similarities and both have potential fines for data breach and require consent for personal info
- Canada Scope expanded to private businesses in 2000 and consent required for personal info

- Brazil 2018 adopted and consent required for personal info but fines & penalties not effective until Aug 2021
- India Personal Data Protection Bill introduced in 2019 and mirrors the GDPR in many aspects but had not been passed as of early 2021
- Mexico Adopted personal info protection in 2010. It does not apply to the government, credit reporting companies, or individuals carrying out data collection solely for their own personal use and not disclosed for commercial use.

Questions?