Privacy vs. Government Tech
A talk with Jeffrey Rosen

I. Fourth Amendment and Government Surveillance

A. Privacy origins
   1. The Fourth Amendment was penned with the case of John Wilkes in mind. In 1767, Wilkes, an Englishman, was arrested in his home for authoring a pamphlet criticizing the government.
   2. Wilkes sued for trespass on the grounds that the pamphlets were searched and seized under a general warrant – it identified neither the specific place to be searched nor the particular thing to be seized.
   3. Wilkes won a large sum in a verdict written by Lord Camden.
   4. The opinion stands for the proposition that paper searches for evidence of seditious libel were a violation of the common law rights of Englishmen.

B. Olmstead v. United States (1928)[1]
   1. Olmstead, a bootlegger, argued that the US government could not, according to the exclusionary rule, lawfully use information gained from a wiretap of his home phone.
   2. SCOTUS, in a 5-4 decision with a majority opinion led by Chief Justice Taft, ruled in favor of US: The Fourth Amendment did not forbid what was done because there was no entry into the home or office of Olmstead -- the wires were placed under public property (sidewalks outside of his office).
   3. This decision would eventually be overturned in Katz v. United States, 389 U.S. 347 (1967).
   4. Justice Brandeis writes the dissent in Olmstead: Because wiretapping allows an observer to listen to both ends of a conversation, it is actually a greater invasion of privacy than breaking and entering.
   5. Brandeis also anticipates future privacy-related legal issues as technology develops: “Ways may someday be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions.”

C. United States v. Jones (2012)[2]

---

[1] 277 U.S. 438 (1928): https://scholar.google.com/scholar_case?case=5577544660194763070&hl=en&as_sdt=6&as_vis=1&oi=scholarr

1. Jones was arrested for drug trafficking based off of information collected from a police GPS tracking device attached to his car. He argued that his Fourth Amendment rights were violated as the GPS was used to follow him beyond the geographical and temporal bounds of a valid search warrant.
2. Deputy Solicitor General Dreeben argued that citizens can have no expectation of privacy in public. When we're in public, we're assuming the risk that we're being tracked. 24/7 tracking with GPS technology, therefore, does not violate the Fourth Amendment.
3. SCOTUS unanimously rejected Dreeben's arguments:
    a. Scalia authors majority opinion: The act of trespassing onto Jones' driveway and putting a GPS device on his car was an invasion of his property rights, and thus a violation of the Fourth Amendment.
    b. Alito's concurrence: questions the focus on physical trespass. The police could have obtained the same geo-location information by subpoenaing Jones' cell phone to reconstruct his movements. But Jones has a subjective idea of privacy -- a "reasonable expectation of privacy"-- that he's not being tracked 24/7.
    c. Justice Sotomayor concurrence: questions the Third Party Doctrine: "It may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."

D. Third Party Doctrine: when individuals share information to third parties, there is no "reasonable expectation of privacy" of that information under the Fourth Amendment.

II. Cell phone search incident to arrest: Riley v. California (2014)[3]

A. The court considered two cases presenting a common question. In the first case, Riley, a Lincoln Park gang member in San Diego, was the driver in a drive-by shooting of a rival gang. 20 days later, the police pulled over Riley driving a different car, which had expired registration. Because he was driving with expired license, the car was impounded. As part of its inventory search, the police searched the impounded car, found 2 guns, and arrested Riley for possession of firearms. During the arrest, the police searched his phone, saw videos and photos that showed him making

---

[2] 565 U.S. 400 (2012): https://supreme.justia.com/cases/federal/us/565/10-1259/
[3] 134 S. Ct. 2473 (2014): https://scholar.google.com/scholar_case?case=9647156672357738355&hl=en&as_sdt=6&as_vis=1&oi=scholarr

gang signs, and determined he was gang affiliated. Ballistics tests subsequently tied Riley to the drive-by shooting. Riley sought to suppress the cell phone evidence. The motion was denied. He was convicted of assault with a semiautomatic weapon, shooting at an occupied vehicle, and attempted murder.

B. The California Court of Appeal affirmed.
C. The Supreme Court reversed the California Court of Appeal. It held that the police must secure a warrant before conducting a cell phone search incident to arrest. The Court used a balancing analysis. Digital contents, unlike physical objects, cannot directly endanger the police. Evidence preservation and the concern there could be remote wiping or data encryption can be addressed via other means. The defendant's privacy interests – cell phones have immense storage capacity and it can reveal detailed information about all aspects of a person's life.

III. Carpenter v. U.S[4]

A. Over a 2-year period, there were several armed robberies of Radio Shack and T-Mobile stores in the Detroit area. Timothy Carpenter was the lead organizer of the conspiracy, supplying the guns, acting as lookout, and signaling when each robbery would begin. One of co-conspirators confessed and gave up the cell phone numbers of the conspirators.
B. The government applied for 3 different court orders for the cell-site records associated with the numbers, seeking "cell site information" "at call origination and at call termination for incoming and outgoing calls," under the Stored Communications Act (SCA). The statute requires only reasonable suspicion (and not probable cause).
    1. SCA permits the government to obtain records where "specific and articulable facts show that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."
C. The records showed that conspirators were within 2 miles of the robberies at the time they occurred and that Carpenter's phone was using cell towers near 4 robberies over a 5-month window.
D. Carpenter was charged with aiding and abetting robbery affecting interstate commerce and the user or carriage of a firearm in violation of the Hobbs Act.

[4] Argued on November 29, 2017.

E. The Court will consider whether the warrantless seizure and search of the cell phone records revealing and location and movements of the user over 172 days is permitted by the 4th Amendment.
F. Third party doctrine – information voluntarily given to third parties are not protected by the 4th Amendment.
    1. In *Jones,* Justice Sotomayor noted in her concurrence the impracticability of the third party doctrine in the digital age in which people reveal a lot of data about themselves to third parties.

IV. ECPA

Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act, commonly referred together as the Electronic Communications Privacy Act (ECPA) of 1986

A. Applies to email, telephone conversations, and data stored electronically.
B. Title II, the Stored Communications Act (SCA), protects the privacy of the contents of files stored by service providers and of records held about the subscriber by service providers, such as name, billing records, or IP addresses.[5]

[5] 18 U.S.C. §§ 2701-12: http://www.law.cornell.edu/uscode/html/uscode18/usc_sup_01_18_10_I_20_121.html