Moral and Legal Foundations of Privacy

February 22, 2023

Recap of Last Week

- What Are the Boundaries of the Fourth Amendment?

1. Olmstead v. US – Early view that 4th Amendment only covers physical property
2. Katz v. US – Rejection of Olmstead; "reasonable expectation of privacy" test
3. Smith v. Maryland – Pen register case; third-party doctrine
4. Hardee/Kyllo case – "Search" can be done without physical intrusion
5. Thompson/Jones case – GPS tracking and "mosaic" theory
6. McCubbin/Carpenter case – digital technology issues

III. Privacy and the Government

2. Digital Searches and Seizures

Moore - Riley v. California

Search of Cell Phones

Riley v. California (2013)

- Combination of two different cases with two different fact patterns.
- One case involved David Riley; the other involved Brima Wurie.
- Court combined them because they deal with the same legal issue: whether a search of cell phones is a violation of the 4th Amendment.

Riley v. California (2013)

Riley:

- Riley stopped for traffic violation that led to arrest for weapons.
- As part of the arrest, an officer took Riley's cell phone from his pants and accessed information in the phone.
- The officer saw references to a street gang, which led to further examination of the phone by police later.
- Found images/videos that led to charges in a shooting and enhanced charges for gang affiliation.
- Riley moved to suppress phone evidence, but was denied.

Riley v. California (2013)

Wurie:

- Wurie arrested after being observed in a drug sale.
- Officers took Wurie's phone and noticed it was receiving multiple calls from "my house" on the external screen.
- Officers opened phone, searched call log and traced the "my house" number to Wurie's apartment.
- Obtained a search warrant and found drugs, guns, and money. Charged him with drug and firearm offenses as related to home search.
- Wurie moved to suppress. Appellate court vacated relevant convictions.

Riley v. California (2013)

- General rule: no warrantless search of digital information on cell phone seized from person arrested absent a specific exception to the warrant requirement.
- What exceptions are in play?
- The Court analyzes them...

Riley v. California (2013)

- Three applicable precedents:

1. A search incident to an arrest must be limited to the area within the arrestee's immediate control, where it is justified by the interests in officer safety and in preventing evidence destruction.

2. These risks of officer safety and evidence destruction are present in all custodial arrests.

Riley v. California (2013)

3. Searches of a car are OK where the arrestee is unsecured and within reaching distance of the passenger compartment, or where it is reasonable to believe that evidence of the crime of arrest might be found in the vehicle.
   - Note – The Court explains that the second point, "reasonable to believe evidence of the crime or arrest might be found in the vehicle", is based on "circumstances unique to the vehicle context," presumably the lower expectation of privacy in a vehicle than of your person.

Riley v. California (2013)

- Question: How does the "search incident to an arrest" doctrine apply to modern cell phones, which are so common that "the proverbial visitor from Mars might conclude they were an important feature of human anatomy"?
  - Technology didn't exist when earlier cases were decided.
  - Digital content on cell phones doesn't really fit with the rationales of the earlier cases where *physical* items were searched for their *physical contents*.

Riley v. California (2013)

- The Court assessed "on the one hand, the degree to which [the search of the cell phone] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."

- The Court found that a search of *digital information* on a cell phone does not further the government interests of protecting officer safety and avoiding destruction of evidence, and implicates substantially greater individual privacy interests than a brief physical search.

Riley v. California (2013)

Reasons for an insufficient legitimate government interest:

1. Digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape.
2. A general concern regarding remote wiping/encryption isn't enough. There is less concern that the arrested person will be able to conceal or destroy evidence within his reach than for *physical evidence*.
   - In addition, no indication this is a common issue, or that search incident to arrest would solve the problem.
   - Technologies exist to respond to remote wiping.

Riley v. California (2013)

- Intrusion is an issue because cellphones differ from other objects a person may carry.
  1. Capacity: Immense storage that "collects in one place many distinct types of information that reveal much more in combination than any isolated record."
  2. "…Even just one type of information to convey far more than previously possible."
  3. Longevity: Data can date back years.
  4. Pervasiveness: Many of the 90% of Americans with cell phones keep on their person a digital record of everything

Riley v. California (2013)

- The Court realizes this "will have some impact on the ability of law enforcement to combat crime," but does not mean police can never get the information:
  - They can get a warrant, which is becoming easier.
  - While this decision finds the "search incident to arrest" exception does not apply, others may allow for a warrantless search in particular cases, such as "exigent circumstances."

Andersen - U.S. v. Stanley

Privacy over Electronic Communications

U.S. v. Stanley (2014)

- Erdely (investigator) suspected that a number of files on a file-sharing network were child pornography based on the file titles (and confirmed that several were).
- Erdely obtained the network's globally unique identification (GUID) and the IP address for the computer sharing the information.
- Determined ISP was from Comcast, and obtained an order for Comcast to disclose.

U.S. v. Stanley (2014)

- Conducted a search of the computers associated with the IP address, but those were not the computers.
- However, the resident used a wireless router and had an unsecured network, but had not given anyone permission to use the network.
- Resident allowed Erdely to access network and obtain private IP addresses/etc.
- Eventually obtained IP addresses.

U.S. v. Stanley (2014)

- Erdely used a free version of Moocherhunter available online.
- MH enables use of a directional antenna to find out who is improperly accessing network.
- Used "passive mode" which requires entry of a MAC address for router, as opposed to searching.
- Can then trace signal to source.

U.S. v. Stanley (2014)

- Erdely used Moocherhunter on resident's wireless router, and was able to trace the computer to its origin: Stanley's computer.
- Signal led across street to apartment complex; signal strongest at Stanley's apt.
- Erdely put all of this in a search warrant, which was granted for Stanley's residence.

U.S. v. Stanley (2014)

- A federal grand jury returned a one-count indictment charging Stanley with possession of child pornography.
- Stanley moved to suppress for improper search/seizure.
- Stanley says information obtained in violation of 4th Amendment.

U.S. v. Stanley (2014)

- Trial Court:
  - Stanley had a subjective and reasonable expectation of privacy in home under *Katz*.
  - BUT he did not for the files on his computer, especially given that he put them on a file-sharing network.
  - So, was use of Moocherhunter a search?
  - In other words, did Stanley have a legitimate expectation of privacy in his wireless signal?

U.S. v. Stanley (2014)

- No reasonable expectation of privacy in information voluntarily conveyed to third parties per *Smith* case:
  - *Smith* was use of pen registers, which include the numbers dialed.
  - Different than *Katz* where the actual content of the conversation was monitored.
  - No expectation of privacy in the numbers dialed because they are "conveyed" to a third party – the phone company.

U.S. v. Stanley (2014)

- Trial court says Stanley's wireless signal is like a pen register in *Smith.*
  - Thus, no legitimate expectation of privacy, and use of MH to track that signal was not a search.
  - *Smith* tracked phone numbers conveyed to third parties, MH tracked signal strength sent to third parties.

U.S. v. Stanley (2014)

- Stanley argued that this was a different situation than *Smith* because Moocherhunter is a tracking device.
- Court rules require a warrant for the use of a tracking device if it implicates a Fourth Amendment right.

U.S. v. Stanley (2014)

- Trial Court disagrees;
  - Even if it was a tracking device, under *Kyllo*, it was generally available.
  - Different than the heat in *Kyllo* which was not directed outside – Stanley's signal was.
  - Stanley may have wanted to remain private, but that expectation was not reasonable given that he directed his information outside the home.
    - Had he not made unauthorized access to a wireless router, he would have been known.

U.S. v. Stanley (2014)

- On appeal, the Third Circuit disagreed with the Trial Court's application of the "third-party doctrine."
  - Thought this application of the "third-party doctrine" too broad, because it would cover all Internet traffic, since all Internet traffic is shared with a third party (like a server).
  - Appeal Court was concerned that law enforcement would have "unfettered access" to Internet data without Fourth Amendment protection.

U.S. v. Stanley (2014)

- The Third Circuit still upheld the conviction, though.
- Stanley did not have a reasonable expectation of privacy because of the "dubious legality" of using his neighbor's wireless signal.

Solove and Schwartz – Digital Searches and Seizures

Searches and Seizures in a Digital World

Digital Searches & Seizures

- A collection of various topics and cases that relate to those topics, along with questions to stretch your thinking on each topic.
  1. Searching Computer Contents
  2. Encryption
  3. E-mail
  4. ISP Records
  5. IP Addresses and URLs
  6. Key Logging Devices

Digital Searches & Seizures

- 1. Searching Computer Contents:
  - Generally, a generic search warrant for an entire computer system is enough for the government to find the "needle in a haystack."
  - It is no different than a search of an entire house for drugs.
  - *US v. Campos* (2000): a warrant to look for one set of images found others. Court allowed the search because of the nature of searching computers.

Digital Searches & Seizures

- There are limits to search warrants
  - In *US v. Carey* (1999), a warrant to search a computer for drug information was not enough to search for pornography.
  - Is copying a search and seizure under the 4th Amendment?
    - *US v. Gorshkov* (2001) did not think so.
    - Some commentators do.

Digital Searches & Seizures

- What about password protection?
  - *Trulock v. Freeh* (2001) only allowed the search of the password-protected part of the computer consented for search
  - *US v. Andrus* (2007) allowed the search of an entire password-protected computer without consent
  - Compare *Trulock* and *Andrus*.

Digital Searches & Seizures

- 2. Encryption:
  - *Junger v. Daly* (2000): encryption is protected free speech, at least in source code form.
  - *But see Karn v. US* (1996): regulation of encryption source code through export controls is a valid government purpose.

Digital Searches & Seizures

- 3. E-mail:
  - *Steve Jackson Games v. US Secret Service* (1994): electronic BBS (a store and forward e-mail system). Warrant to search SJG and Blankenship residence; SJG warrant for computer data.
  - Was the unread e-mail obtained from the BBS an intercept without a court order?
  - No, because the e-mails were in storage, not in transmission, when obtained.
  - It was a violation of 18 USC 2701, though.

Digital Searches & Seizures

- Carnivore:
  - FBI mechanism to intercept e-mail and IMs from ISP and capable of analyzing the entire e-mail traffic at an ISP.
  - Programmed only to search to/from (like pen register), but could do more if instructed.
  - Government said it was only searching pursuant to warrants, but who knows?
  - 2001 Patriot Act authorized Carnivore subject to some limitations.

Digital Searches & Seizures

- 4. ISP Records:
  - *US v. Hambrick* (1999)
    - An adult sought to entice minor online (the "minor" was a police officer).
    - Officers served subpoena on the adult's ISP (Mindspring) to get his name. Mindspring complied.
    - Warrant was invalid because of interested judge.
    - Should the information be suppressed for violation of the Fourth Amendment?

Digital Searches & Seizures

- Court looks to see if defendant had a "reasonable expectation of privacy":
  - 1. Subjective expectation of privacy
  - 2. Objectively reasonable expectation of privacy
- Key in this case is whether there was "objectively reasonable" expectation.
- Court says no. Hambrick was not completely anonymous because the ISP knew who he was. Nothing in their agreement to the contrary.

Digital Searches & Seizures

- "Where such dissemination of information to nongovernment entities is not prohibited, there can be no reasonable expectation of privacy in that information."
- The Court relies on *Smith v. Maryland* and the third party doctrine to come to this conclusion.

Digital Searches & Seizures

- 5. IP Addresses/URLs:
  - *US v. Forrester* (2008): Defendants convicted of running ecstasy lab appeal because use of a "mirror port" to monitor e-mail and tracking Internet activity violated the 4th Amendment.
  - The Court relies on *Smith v. Maryland*, finding use of pen registers for phone numbers is not a search, because no reasonable expectation of privacy in that kind of information.

Digital Searches & Seizures

- Court says that "mirror ports" and pen registers are constitutionally the same, and thus no expectation of privacy –
  - (1) users know the to/from information in an e-mail will be given to third parties to convey the information; and
  - (2) it provides no information about the substance of the transmission.
- After this case, the 2001 Patriot Act confirmed that the Pen Register Act applied to e-mails.

Digital Searches & Seizures

- 6. Key Logging Devices
  - US v. Scarfo (2001): during a search, government found computer with encrypted "Factors" file, and installed a "Key Logger System" to gain access information.
    - Court was concerned that government intercepted information over telephone wires without applying for a wiretap.
    - Scarfo said it was a violation because it collected data on all keystrokes, not just the passphrase to the "Factors" file.

Digital Searches & Seizures

- Court looks at the search warrant and said it was very specific.
  - Moreover, that KLS recorded other kinds of keystrokes doesn't turn the limited search into a general exploratory search.
  - Compares to searching in a closet or filing cabinet.
- Court said no wiretap issue because the software was designed not to record keystrokes when the modem was operating, so the KLS could not "intercept" communications.

III. Privacy and the Government

3. National Security

Solove – I've Got Nothing to Hide

The "I've Got Nothing to Hide" Argument Against Privacy

Solove – Nothing to Hide

- The government's surveillance over you continues to grow as part of the war on terror:
  - NSA warrantless wiretapping
  - Total Information Awareness (TIA)
  - NSA review of phone and bank records
- There has been some public outcry, but most just shrug and say "I've got nothing to hide"
- Is that a sufficient answer?

Solove – Nothing to Hide

- This is not limited to the US; in the UK, CCTV is everywhere, and the government markets it using the "nothing to hide" argument:
  - "If you've got nothing to hide, you've got nothing to fear"
- To someone like Solzhenitsyn, though, "Everyone is guilty of something or has something to conceal. All one has to do is look hard enough to find what it is."

Solove – Nothing to Hide

- But many people are willing to exchange "a small amount of privacy for a potential national security gain."
- The "nothing to hide" argument is then just a balance of the relative values of privacy and security, and favors security over privacy.
- Does it make a difference in your mind if it is just a computer doing the collecting and analysis? It limits human eyes on information.

Solove – Nothing to Hide

- Solove thinks the "nothing to hide" argument is flawed.
  - This stems, in part, from his belief that the "third-party doctrine" in the Fourth Amendment cases is incorrect and should be changed.
    - "[T]he lack of Fourth Amendment protection of third party records results in the government's ability to access an extensive amount of personal information with minimal limitation or oversight."

Solove – Nothing to Hide

- "Surveillance can create chilling effects on free speech, free association, and other First Amendment rights essential for democracy. Even surveillance of legal activities can inhibit people from engaging in them."
- "Chilling effects harm society because, among other things, they reduce the range of viewpoints expressed and the degree of freedom with which to engage in political activity."

Solove – Nothing to Hide

- To Solove, aggregation surveillance (like what the NSA does) is a problem because it is "suffocating" and "aims to be predictive of behavior, striving to prognosticate about our future actions."
- The other problem is "exclusion," that this collection and these programs are kept secret from us.
- What else will the government do with the information in the future as yet unrevealed to us?

Solove – Nothing to Hide

- Some critics believe that privacy problems are not very compelling because they do not have "enough dead bodies."
  - But what about Rebecca Shaeffer and Amy Boyer? Both killed by stalkers who gained personal information about them from databases.
- Solove says this objection is similar to the "nothing to hide" argument. He believes there is still a harm worth addressing, even if it is not sensational.

Solove – Nothing to Hide

- To Solove, a general security interest should not be weighed against a general privacy interest.
- Instead, we should limit the government collection by "judicial oversight" and "minimization procedures."
- "Only in cases where such procedures will completely impair the government program should the security interest be weighed in total, rather than in the marginal difference between an unencumbered program versus a limited one."

Global Relief Foundation v. O'Neill

FISA and the FISC

Global Relief v. O'Neill (2002)

- Background facts:
  - Global Relief is a non-profit and claims to support humanitarian relief programs throughout the world.
  - After the 9/11 attacks, the FBI looked to Global Relief and its potential connections to the terrorists who carried out the attacks.
  - The FBI searched Global Relief's HQ pursuant to the Foreign Intelligence Surveillance Act ("FISA").
  - Global Relief challenged the search as illegal and in violation of the Fourth Amendment.

Global Relief v. O'Neill (2002)

- FISA:
  - Law passed by Congress in 1978 to create a framework in which the government can conduct "legitimate electronic surveillance for foreign intelligence purposes" while recognizing "privacy and individual rights."
  - The FISA created an oversight special court called the Foreign Intelligence Surveillance Court ("FISC"), which reviews applications for authorization of electronic surveillance (similar to a search warrant).
  - The FISA requires the government to provide certain information in support of its application for surveillance.

Global Relief v. O'Neill (2002)

- The government must provide:
  - Facts to justify belief that the target of the search is a foreign power or an agent of a foreign power.
  - Premises to be searched contains foreign intelligence information.
  - Information sought is foreign intelligence information that could not reasonably be obtained through normal investigative means.
- If the target of the search is a "United States person," there must also be probable cause and procedures to minimalize intrusion.

Global Relief v. O'Neill (2002)

- FISA also allows for surveillance without a warrant in "emergency situations" as long as the government later applies for a warrant within 72 hours of the initial search.
- In this case, the Court found that the US Attorney General had declared such an "emergency situation" and had later applied for a warrant within the 72-hour window.
- Thus, the search of Global Relief's HQ was authorized under FISA.

Global Relief v. O'Neill (2002)

- The Court also found no Fourth Amendment concern.
- "FISA's safeguards provide sufficient protection for the rights guaranteed by the Fourth Amendment in the context of foreign intelligence activities."
- Because the government followed the FISA requirements, the Fourth Amendment was not violated.

Klayman v. Obama

NSA Surveillance and Telephone Metadata

Klayman v. Obama (2013)

- Background facts:
  - 2013 Snowden revelations that the NSA was conducting widespread wiretapping and data collection of the public. The government was:
  - (1) Targeting non-US persons outside the US by surveillance occurring in the US.
  - (2) Collecting telephone metadata.
  - (3) Spying on foreign countries and their leaders.
  - (4) Attempting to weaken encryption standards.

Klayman v. Obama (2013)

- Under the Obama administration, "the communication records of millions of US citizens [were] being collected indiscriminately and in bulk—regardless of whether they are suspected in any wrongdoing."
- The plaintiffs filed this case against the government for violating various constitutional rights, including the Fourth Amendment and for violating FISA.
- After reviewing the history of FISA and the FISC, the court reviews the facts of the case.

Klayman v. Obama (2013)

- The government's "Bulk Telephony Metadata Program" collected information about the phone numbers used to make and receive calls, when the calls took place, and how long the calls lasted.
- The government did not collect any information about the contents of the calls or the name, address, or other information about the parties to the calls (other than their phone numbers).
- The government used this information to attempt to identify connections between terrorists.

Klayman v. Obama (2013)

- The government's collection had been happening for more than 7 years (2006-2013) and had been collecting from many telecom companies.
- The NSA then aggregated all the information into a single database to create a "historical repository that permits retrospective analysis."
- The FISC had authorized this program, but only for "counterterrorism purposes."
- The NSA limited its searches to three "hops" from a seed.

Klayman v. Obama (2013)

- Fourth Amendment Analysis
  - Threshold issue is whether the plaintiffs had a "reasonable expectation of privacy."
  - The Court starts with *Smith v. Maryland* and the third-party doctrine.
  - The *Smith* case is much different than these facts, though.
  - "When present-day circumstances—the evolutions in the Government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies—become so thoroughly unlike those considered by the Supreme Court 34 years ago," does *Smith* still apply?

Klayman v. Obama (2013)

- The Court believes the metadata collection "almost certainly does violate a reasonable expectation of privacy" for several reasons:
  1. Pen register in *Smith* was only for a few days and no expectation the government would retain the records.
  2. Relationship between the police and the telephone company in *Smith* is "*nothing* compared to the relationship that has apparently evolved over the last seven years between the Government and telecom companies."

Klayman v. Obama (2013)

3. The technology enables the government to "store and analyze the phone metadata of every telephone user in the US" and that makes it "unlike anything that could have been conceived in 1979."
4. "[N]ot only is the government's ability to collect, store, and analyze phone data greater now than it was in 1979, but the nature and quantity of the information contained in people's telephony metadata is much greater, as well."

Klayman v. Obama (2013)

- "This rapid and monumental shift towards a cell phone-centric culture means that the metadata from each person's phone 'reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.'"
- "Whereas some may assume that these cultural changes will force people to 'reconcile themselves' to an 'inevitable' 'diminution of privacy that new technology entails,'… I think it is more likely that these trends have resulted in a *greater* expectation of privacy and a recognition that society views that expectation as reasonable."

Klayman v. Obama (2013)

- Court also finds the metadata collection an "unreasonable" search because the government does not have an immediate concern and the collection has not met any such terrorism concern.
- The government could not cite a single instance where the metadata collection stopped an imminent attack or aided a time-sensitive government objective.