

A Short History of Privacy Related Case Law & Privacy Perspectives

CSC 249
April 17, 2017

Finding A Partner?

- Time at the end of class
- To seek out a classmate of similar interests
- To work together
- On the semester project

US Constitution 4th Amendment

- 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.
- "Unreasonable, probable cause, particularly describing the place to be searched"
 - From colonial days which had general warrants

Olmstead v. U.S., 1928

- Brandeis' dissent – Founders have conferred the right to be left alone
 - The most comprehensive of rights and the rights most valued by civilized people
- The right to withhold information
- Tolerance of the public disclosure of private lives is a corrupting force
- Brandeis promoted 'technology neutrality' in government ability to invade citizens' privacy

Katz v. U.S., 1967

- 4th amendment protects people not places
 - each person has an expectation of privacy
 - expectation is one that society is prepared to recognize as reasonable
- The reasonable expectation test – this is still the law today
 - An expectation of privacy, and one that society is willing to recognize
 - Led to Congress passing the *Wiretap Act*

Miller v. U.S., 1976

- Finding: There is no expectation of privacy in records held by a third party
- Example of Canceled checks: contain information voluntarily conveyed in the ordinary course of business

Smith v. U.S., 1979

- Police placed a pen register at a central phone office, recording every number dialed
- Finding: Doubt that people in general entertain any actual expectation of privacy in the numbers they dial.
 - All telephone users realize that they must “convey” phone numbers to the telephone company.
- First time the Supreme Court - drew distinction between the content and the context of a communication
 - Claim that the distinction between content and context is becoming irrelevant
 - There is some debate over URLs, which are context, but do also hold some content

Kyllo v. U.S., 2001

- Kyllo grew marijuana in his home, police use of sensors occurred prior to warrant
- Finding: Use of sensors was a search under the 4th amendment
- Kyllo won: the gov’t used a device that is not in general public use,
 - To explore details of the home that would previously have been unknowable without physical intrusions.
 - The surveillance is a search, that otherwise would have been unreasonable without a warrant.

Warshak (6th Ckt, 2010)

- Law enforcement must have a warrant to obtain email stored by email providers

Summary of Cases

- **Olmstead:** The right to be left alone
- **Katz:** Each person has an expectation of privacy, only as recognized by society to be reasonable
- **Miller:** No expectation of privacy in data freely given to 3rd party
- **Smith:** No expectation of privacy in contextual data used to establish communication
 - Distinction between *content* and *context* of a communication
- **Kyllo:** Use of advanced technology to obtain information only otherwise available through intrusion constitutes a search

Federal Laws

- Privacy act of 1974
 - Data collection must be advertised and only be used for specific agency goals...
 - Except for routine uses (!)
- Electronic communications privacy act, ECPA, 1986
 - Extend gov't restrictions on wire taps to include transmission of e-data, by computer.
 - Addressed hole in Smith case – content v. context
 - Designed to balance: the expectations of citizens and the legitimate needs of law enforcement.

See Wikipedia: [Electronic_Communications_Privacy_Act](#)

ECPA

- Title I: Wiretap Act
 - Protects wire, oral and e-communication
 - Need a warrant for communications *in transit*
- Title II: Stored Communications Act
 - Need a good argument to get data, but do not need to show probable cause – weaker than Title I
 - Email – is it “in transit” or is it “stored” in the server?
 - Need a judge approving this, or at least a legal authority
- Title III: Pen Register Act, trap and trace devices
 - Prohibits use of trap & trace devices to record context info in transmitting e-communications, w/o court order
 - Origin – devices record numbers of all those that call you
 - Destination – pen register – all numbers called are recorded
 - There is NO JUDGE deciding here

ECPA in Court

- Is email protected under Title 1 while in transient storage en route to destination?
 - 2001 – US District court ruled no
 - 2005 – First Circuit court of appeals reversed this decision
- WebcamGate – 2010 – Philadelphia school districts used cameras in school-issued laptops to monitor students at home
 - Schools settled, paying plaintiffs' legal costs

ECPA Holes

- ECPA specified when the government needs a warrant to search electronic communications
- Applied to voice communications in real-time
 - Not to data communications
 - Not to stored data – email stored on servers for more than 6 months considered abandoned property, and so no warrant needed to search
- 'Transactional data' not protected
 - dialing information
- Other Holes
 - URL visited...
 - Data stored in the cloud
 - Location/tracking data from cell phones

ECPA 2013 Amendments

- Service provider cannot voluntarily disclose contents of communications
- A search warrant is required to obtain contents of communications
- Nothing about the 'context' information (or metadata) was addressed

Perspectives...

- Protecting privacy from government intervention
- Protecting privacy from corporate and private entity control

Helen Nissenbaum

- Contextual Integrity – privacy in context
 - Different situations require different value structures
 - A zone of seclusion
 - A given context defines what we consider to be private

•

•

Center for Democracy & Technology: Suggested for ECPA

- Email
 - Protect stored > 180 days, and not dependent upon whether or not it has been opened
 - Coalition Letter Supporting Email Privacy Act in 115th Congress, ([January 30, 2017](#))
- Mobile location
 - Need to clearly specify a standard for when the government can access this info, and require agents to have a warrant
- Cloud computing
 - All data on the cloud must be protected
- Social networking
 - Government should need a warrant to access private data
- Tracking and logging of online activity
 - Currently government files blanket subpoenas for everyone who has visited a given site, rather than specific and targeted subpoenas.

•

•

CDT: Suggested for ECPA

- Technology and platform neutrality
- Assurance of law enforcement access
- Equality between transit and storage
- Consistency in access to communication
 - voice vs. data
 - whether 'opened' or not
- Simplicity and clarity
- Recognize all existing exceptions

Bentham & Foucault

- Jeremy Bentham
 - No such thing as natural rights
 - Discussed the Panopticon (prison)
 - A new mode of obtaining power of mind over mind
 - Big brother syndrome – when you believe you are being watched all the time you become more passive
- Foucault – the metaphor of panoptical a state of surveillance
 - Feeling you are being watched all the time induces a sense of being watched all the time

Data & Marketing

- Deleuze – feedback mechanism
 - As get information about a person, modulate the additional information you provide/send, in order to get the response you want from the person
 - Very powerful for advertising
- When a technology collects information, there will be a “market” for that information,
 - Market could be government, law enforcement –
 - **AND** once the market is there, it is very hard to do away with it.

Data & Marketing

- Privacy vs. Autonomy
- The right to indeterminacy → somewhat an economic/marketing use now
 - To be truly autonomous depends on an underdetermined environment
 - vs. Direct marketers seeking to make us respond in certain ways

IRB: Nuremberg Code

- Informed consent is essential.
- Research on human subjects should be based on prior animal work.
- The risks should be justified by the anticipated benefits.
- Only qualified scientists should be allowed to conduct research with human subjects.
- Physical and mental suffering must be avoided.
- Research in which death or disabling injury is expected should not be conducted.

IRB Principle: Autonomy

- This principle requires researchers to treat individuals as autonomous human beings, capable of making their own decisions, and not to use people as a means to an end. Elements of autonomy include:
 - Mental capacity (the ability to understand and process information)
 - Voluntariness (freedom from undue control or influence of others)

IRB Principle: Autonomy

- Subjects have autonomy when they have the capacity to understand and process information, and the freedom to volunteer for or withdraw from research without coercion or undue influence from others.
- In practice, this involves creating a meaningful consent process.
 - Provide prospective subjects with all the information they need to make a decision to participate in research
 - Allow subjects to withdraw from research without any adverse consequences if they change their minds.

IRB Principle: Beneficence

- This principle requires researchers to minimize the risks of harm and to maximize the potential benefits of their research.
- The term "risk" refers to a possibility that harm may occur.
 - However, the assessment of risk requires evaluating both the magnitude of the possible harm and the likelihood that the harm will occur.

Identifiable private information

- As defined in the regulations, private information includes:
 - Information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place
 - Information which has been provided for specific purposes by an individual and which the individual can reasonably expect will not be made public (for example, a school record).
- The regulations further state that for data to be “private information” it must be individually identifiable
 - *i.e.*, the identity of the subject is or may be readily ascertained by the researcher or associated with the information

Invasion of Privacy

- Invasions of privacy can occur if personal information is accessed or collected without the subjects' knowledge or consent.
 - For example, if a researcher studying interaction patterns in an online support group joins the group and does not reveal her true identity online, the support group participants could feel that their privacy had been invaded by the researcher, if or when her true identity is revealed to the group.
- Invasions of privacy can also occur if a subject's participation in a study is revealed despite assurances that this would not happen.
 - For example, a researcher is studying Another university staff person sees an acquaintance entering the meeting room and therefore discovers that his acquaintance is part of that study.

Breach of Confidentiality

- Perhaps the primary source of risk in the social and behavioral sciences is that information obtained by researchers could harm subjects if disclosed outside the research setting.
- Confidentiality can be compromised through an unauthorized release of data, which could have a negative impact on the subjects' psychological, social, or economic status.

Overview of Informed Consent

- Providing specific information about the study to subjects in a way that is understandable to them.
- Answering questions to better ensure subjects understand the research and their role in it
- Giving subjects adequate time to consider their decisions
- Obtaining the voluntary agreement of subjects to take part in the study.
 - The agreement is only to enter the study, as subjects may withdraw at any time, or decline to answer specific questions or complete specific tasks at any time during the research

Frameworks for Discussion

- Why do we care about privacy?
- Right to not have information on yourself collected
- The right to control the spread and use of your information
 - Commoditization of information
- The right to be anonymous
 - Privacy vs. Autonomy
 - Historical context of privacy (living in a village v. a city...)
- The inequality of access to information
 - To information gathered on you (gov't has it and you don't know)
 - Information for economic (shopping) decisions
- The costs of privacy

• Martin Kaste, NPR, Smith College Kahn Privacy project •

MOVING FORWARD:

- Privacy Aware Design
 - Onion Routing
 - Block Chain
 - Authentication

Privacy Aware Design

- Limit collection of data in the first place
 - ...then to
- Design principles:
 - a) Provide full disclosure of data collection
 - b) Require consent to data collection
 - c) Minimize collect of personal data
 - d) Minimize identification of data with individuals, the opportunity to anonymize data
 - e) Minimize and secure retained data

Privacy Aware Design

- Provide full disclosure of data collection
 - Description requirement
 - Fine print user agreements from software companies
 - Enforceability requirement
 - FTC privacy statements
 - Irrevocability requirement.
 - *i.e.*, Facebook rules changes weekly, but we don't really have the chance to change our 'agreeing'
 - Intelligibility requirement
 - Must be able to be understood by regular people

Privacy Aware Design

- Require consent to data collection
 - Acknowledgement requirement
 - Opt-in requirement – vs. opt-out
 - Consent should be opt-in
 - It is very hard to get people to care enough to read the agreements.
 - Who really looks at these ridiculous agreements
 - The company putting them out
 - The FTC – Microsoft was sued, by the FTC, on some of its privacy requirements

Privacy Aware Design

- Minimize collection of personal data
 - For data to be collected, it must be **matched to the mission**
 - Establish **functional requirement** for the collection
 - No data collection simply because it might be useful
 - Collection must be necessary to the functionality of the communication system, the technology
 - **Distributed processing** requirement
 - Process close to collection location, and so DO NOT centralize data collection or processing
 - Aggregation prior to centralized collection
 - Destroy the data once it is no longer needed or useful
 - Limits re-use of the data, as well as hacking opportunities
 - **Technical problems possible**
 - Demand response w/o centralized data collection

Privacy Aware Design

- Minimize identification of data with individuals
 - Anonymize data
 - Note that this is not part of "Fair Information Practices"
 - Data collection (bills, cell phone, etc.) is/should be identified with the equipment, and not to the person
 - Cellular Privacy Overlay (Wicker article)
 - Use public key encryption to bind equipment to person
 - Non-attribution requirement
 - Track equipment, not user
 - Does the technology require association of data with individual or with his/her equipment?
 - Technical problem
 - Private use of public service
 - How show you are a valid user without public disclosure?

Privacy Aware Design

- Minimize and secure retained data
 - Destroy all/most data after its immediate and intended use is done
 - Functional requirement for retention
 - Convenience conflicts with security/privacy
 - Basic security requirement
 - Non-reusability requirement
 - Inadvertent use not allowed

Onion Routing

- The Tor network is a group of volunteer-operated servers that allows people to improve their privacy and security on the Internet.
- Tor's users employ this network by connecting through a series of virtual tunnels rather than making a direct connection, thus allowing both organizations and individuals to share information over public networks without compromising their privacy.
- Tor is an effective censorship circumvention tool, allowing users to reach otherwise blocked destinations or content.
- <https://www.torproject.org/about/overview.html.en>
-

Cryptography

- Block Chain & Bitcoin
 - Blockchain is a shared immutable ledger for recording the history of transactions. A business blockchain provides a permissioned network with known identities.
 - Blockchain for dummies: <https://www.ibm.com/account/reg/us-en/signup?formid=urx-16905>
- Elliptical curves
 - An approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC requires smaller keys compared to non-ECC cryptography to provide equivalent security. (wikipedia)

Authentication

- FIDO Alliance
 - The FIDO Alliance enable an interoperable ecosystem of hardware-, mobile- and biometrics-based authenticators that can be used with many apps and websites.
 - This ecosystem enables users to deploy strong authentication solutions that reduce reliance on passwords and protect against phishing, man-in-the-middle and replay attacks using stolen passwords.
 - <https://fidoalliance.org/about/overview/>

Summary

- Legal history of privacy protections
- Discussion of defining privacy
- Increased vulnerability of our privacy with data collection and storage on the Internet
- Solutions for protecting privacy

Find a Partner?

- 1000 word project + ~250-300 for each additional person,
- We are in the 'knowledge age' and so you should practice creating new knowledge,
- Research your topic and propose something new – a new idea, some new knowledge,
- Your project must be presented in a way that it is clear how it relates to course material,
- Presentation is of a single, interesting thing you learned and want to share,
- Due May 10 by 4pm.
-