Human Information Privacy
A Talk with Professor Neil Richards

- Concept of human information policy
  - Today's business and government practices are collecting and manipulating human information. Human information policy is about the rules for use of that information.
  - Privacy in the digital age is about the extent to which information about people are collected, used, and shared. Information confers power, and privacy rules are meant to constrain that power.
  - Privacy rules are important given the magnitude of information collected and the potential consequences of its use and misuse, such as security breaches and consumer electoral manipulation.
  - Updates needed in legal framework:
    - Translate constitutional protections against government to digital environment
    - Consumer protection laws regulating online privacy and data collection and use

- Constitutional protections against the government
  - Privacy protections implied in the Constitution
  - Cases
    - United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).
      - Warshak was the target of a mail fraud, wire fraud, and money laundering investigation. The government subpoenaed the ISP for Warshak's emails based on reasonable grounds to believe that information was material to the investigation, pursuant to the Stored Communications Act.
      - Sixth Circuit held that there is a reasonable expectation of privacy in emails and that a warrant based on probable cause is required to compel an ISP to turn over emails to the government.
    - United States v. Jones, 565 U.S. 400 (2012).
      - Jones was the target of a drug trafficking investigation. The government obtained a warrant to place a tracking device on a car belonging to Jones's wife within 10 days in D.C. The GPS device was installed on the 11th day in Maryland while the car was on a public street.
      - Supreme Court held that installing a GPS device on a car constitutes a search under the Fourth Amendment.
    - Riley v. California, 573 U.S. 373 (2014).

        - Riley was pulled over for expired tags and driving with a suspended license. During the arrest, the police searched Riley's cellphone without a warrant. Based in part on the information from the cellphone, Riley was convicted in connection with a shooting that involved gangs.
        - Wurie was arrested after police observed him make a drug sale. The police seized his phone, traced a number that was calling the phone to his house, secured a warrant, and found drugs and firearms.
        - Supreme Court held that the government may not conduct a warrantless search of a cell phone seized after an arrest, absent exigent circumstances.
    - Carpenter v. United States, 138 S. Ct. 2206 (2018).
        - Carpenter was arrested for multiple armed robberies in Detroit. The government obtained warrants to obtain cell site records pursuant to the Stored Communications Act, which requires showing "specific and articulable facts showing that there are reasonable grounds to believe… [the information is] relevant and material to an ongoing investigation."
        - Supreme Court held that cell-site location information constitutes a search under the Fourth Amendment and that a warrant based on probable cause is required.

- Consumer protections against private entities
    - Lack of broad privacy protections against private entities in the U.S.
        - Constitution generally protects against the government; a need in the U.S. to develop laws protecting consumers and their data.
        - U.S. lacks federal-level privacy protection.
    - Discussion of terms that technology companies and other businesses use and why it matters
        - "User"
            - Does "user" accurately describe the relationship between consumers and technology companies?
        - "Choice" and the illusion of choice
            - In a "notice and choice" regime, companies may choose to do what they want with consumers' data so long as consumers are notified in a privacy policy. Onus is on the consumer to read, opt-out, etc. Choice is overwhelming for the consumer.
            - Illusion of choice:
                - Choice is unwitting. Notices are long, inaccessible and hard to understand for the average consumer, and too ubiquitous. Choice is unwitting as to downstream consequences of information sharing.

        - Coercion: if there is one dominant technology platform, is there are actually a choice to use it?
        - Choice and capacity re. minors
      - Tech companies leverage design, use dark patterns, to lead consumers to make certain choices.
    - "Innovation"
      - What does "innovation" actually mean?
      - Is innovation and privacy a trade-off? Do privacy laws stifle "innovation"?
      - Is "innovation" a right? Tech companies increasingly make the argument that any regulation restricting data collection and use violates their First Amendment rights.
  - Discussion of how the laws should take into account cognitive biases of consumers
    - Current privacy regime of "notice and choice" does not take into account the fact that human beings are not always rational actors.
    - Technology companies design web interfaces, marketing, copy to exploit our cognitive vulnerabilities and biases.

- Consumer protection laws
  - U.S. does not have comprehensive data protection regs
    - Federal Trade Commission (FTC)
      - In the U.S., the FTC is largely tasked with enforcing competition and consumer protection laws.
      - Bolstering FTC
        - One of its biggest challenges is resources. For such a broad and increasingly important mandate in today's digital age, the FTC is a comparatively small agency with a budget to match.
        - Strengthening existing authorities
      - Federal Trade Commission Act of 1914 § 5 (15 U.S.C. § 45): prohibits unfair or deceptive trade practices in commerce.
  - International privacy regulations
    - EU: General Data Protection Regulation (GDPR)
      - EU regulation on collecting, storing, and processing of personal data. Scope is broad: generally applies to any entity that processes EU residents' data.
      - Focus is on giving consumers the right to control how their data is used, including providing right to object to processing, right to access personal data, right to delete.
    - China: Personal Information Protection Law of the People's Republic of China (2021)
    - Argentina: Personal Data Protection Act (2000)

        - Canada: The Personal Information Protection and Electronic Documents Act (2000)
        - South Korea: Personal Information Protection Act (2011)
    - State privacy laws
        - California Consumer Privacy Act of 2018 (CCPA)
            - Applies to all for-profit entities that collect data from California residents that: 1) generates over $25 mill in annual gross revenue, 2) buys, receives, sells, or shares personal information of 50,000 or more CA residents; or 3) derive 50% of more of annual revenue from selling CA residents' personal information.
            - Grants consumers right to access or delete personal information; grants ability to opt out of sale of personal information.
            - Remains rooted in consent, control and choice; consumers have to choose to exercise their rights.
        - States have begun taking more action in protecting consumer privacy, enacting more comprehensive privacy laws (e.g., CA, CO, and VA) and attorneys general focusing on enforcement.

- Areas for reform
    - Deception and unfairness
        - Expand the definition of "deception" to prohibit services from being marketed as "free."
            - Are "free" internet and "free" apps and services actually free?
                - Consumers pay with their personal information. For tech companies, consumer data is the asset.
                - Consumers have to pay in other ways, e.g. electricity to power their device, internet connection, device itself, etc.
    - Abusiveness
        - Practice of designing interfaces and products to take advantage of human cognitive biases, to steer and manipulate consumers to behave in certain ways. Examples of practices include:
            - Bait and switch: user takes action expecting a certain outcome but a different outcome results (e.g., clicking "close ad" which brings up additional options).
            - Misdirection: designing interfaces to focus consumers' attention elsewhere (e.g., canceling a subscription brings up a page highlighting benefits of the subscription and a small button to cancel).
    - Amend FTC Act §5(n)
        - For practice to be unlawful on grounds of unfairness, requires showing that the practice causes substantial injury to consumers, injury is not reasonably avoidable by consumers themselves, and injury is not outweighed by benefits to consumers or competition. (FTC Act §5(n)).

        - Is the threshold too high?
            - As the unfairness test stands, the threshold does not target abusive or manipulative tactics.
            - The practices that companies employ are not outright deceptive and do not cause the type of significant harm contemplated in the rules. Rather, they leverage human behavior to get consumers to behave in certain ways, whether it's to give up more data or continue to play an addicting game.
    - Discussion of surveillance-based advertising and concept of "free"
        - Whether surveillance-based advertising is necessary or whether it's unnecessary or harmful
        - Model of "free" based on advertising
        - Duty of loyalty
            - Should a duty of loyalty be imposed on data collectors?
            - Duty to act in the best interests of consumers, with whom the company is in an information-sharing relationship.
            - When duty of loyalty may be imposed: 1) trust is invited by company, whether through design or words, that information will not be used in some that harms them, 2) large power imbalance between the parties, 3) company has control over the data, and 4) consumer exposes their vulnerabilities, i.e., gives up information/data, based on trust.

Additional Resource:

- Neil Richards, Why Privacy Matters (Oxford Press 2021)