Today (10/1/20)

• Privacy Personal Essay due October 4
• Lecture – Privacy Law
• Discussion
• Student Presentations
Read for Discussion on 10/5

<table>
<thead>
<tr>
<th>Date</th>
<th>Topic</th>
<th>Speaker</th>
<th>Date</th>
<th>Topic</th>
<th>Speaker</th>
</tr>
</thead>
<tbody>
<tr>
<td>8-31</td>
<td>Introduction</td>
<td>Fran</td>
<td>9-3</td>
<td>The Data-driven world</td>
<td>Fran</td>
</tr>
<tr>
<td>9-10</td>
<td>Data and COVID-19 - models</td>
<td>Fran</td>
<td>9-14</td>
<td>Data and COVID-19 – contact tracing</td>
<td>Fran</td>
</tr>
<tr>
<td>9-17</td>
<td>Data and the Opioid Crisis</td>
<td>Liz Chiarello</td>
<td>9-21</td>
<td>Data and Privacy - Intro</td>
<td>Fran</td>
</tr>
<tr>
<td>9-24</td>
<td>Data and Privacy – Differential Privacy and the Census</td>
<td>Fran</td>
<td>9-28</td>
<td>Data and Privacy – Anonymity</td>
<td>Fran</td>
</tr>
<tr>
<td>10-1</td>
<td>Data and Privacy - Law</td>
<td>Fran</td>
<td>10-5</td>
<td>Digital rights in the EU and China</td>
<td>Fran</td>
</tr>
<tr>
<td>10-8</td>
<td>Data and Elections 1 – Cambridge Analytica and the 2016 election</td>
<td>Fran</td>
<td>10-12</td>
<td>NO CLASS – Columbus / Indigenous Peoples’ Day</td>
<td>Fran</td>
</tr>
<tr>
<td>10-15</td>
<td>Data and Elections 2</td>
<td>Todd Rogers</td>
<td>10-19</td>
<td>Data and Elections 3</td>
<td>Fran</td>
</tr>
<tr>
<td>10-22</td>
<td>Data and Discrimination 1</td>
<td>Fran</td>
<td>10-26</td>
<td>Data and Discrimination 2</td>
<td>Fran</td>
</tr>
<tr>
<td>10-29</td>
<td>Data and Research 1</td>
<td>Josh Greenberg</td>
<td>11-2</td>
<td>Data and Research 2</td>
<td>Fran</td>
</tr>
<tr>
<td>11-5</td>
<td>Data and the IoT 1</td>
<td>Fran</td>
<td>11-9</td>
<td>Data and IoT 2</td>
<td>Fran</td>
</tr>
<tr>
<td>11-12</td>
<td>Data and Ethics 1</td>
<td>Fran</td>
<td>11-15</td>
<td>Data and Ethics 2</td>
<td>Fran</td>
</tr>
<tr>
<td>11-23</td>
<td>Cybersecurity</td>
<td>Bruce Schneier</td>
<td>11-15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11-30</td>
<td>Data and Infrastructure</td>
<td>Fran</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12-3</td>
<td>Data Science</td>
<td>Fran</td>
<td>12-7</td>
<td>Data Science Careers</td>
<td>Kathy Pham</td>
</tr>
<tr>
<td>12-10</td>
<td>Wrap-up</td>
<td>Fran</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Lecture – Privacy and U.S. Law

- Federal Privacy Laws
- Bills in Congress
- State Privacy Laws
U.S. Data Privacy Landscape

• No single, comprehensive federal U.S. law regulating the collection and use of personal data.

• US has a patchwork system of federal and state laws, and regulations that can sometimes overlap, dovetail and contradict one another.

• Government agencies (e.g. FTC) provide some oversight.
U.S. Data Privacy Laws – Partial Timeline

The following are some of the laws, regulations and directives related to the protection of information systems and private information in the U.S. up to 2002 [Wikipedia]:

- 1970 U.S. Fair Credit Reporting Act
- 1970 U.S. Racketeer Influenced and Corrupt Organization (RICO) Act
- 1974 Family Educational Rights and Privacy Act (FERPA)
- 1974 U.S. Privacy Act
- 1980 Organization for Economic Cooperation and Development (OECD) Guidelines
- 1984 U.S. Medical Computer Crime Act
- 1986 U.S. Electronic Communications Privacy Act (ECPA)
- 1988 U.S. Video Privacy Protection Act
- 1990 United Kingdom Computer Misuse Act
- 1992 OECD Guidelines to Serve as a Total Security Framework
- 1994 Communications Assistance for Law Enforcement Act
- 1996 U.S. Economic and Protection of Proprietary Information Act
- 1996 Health Insurance Portability and Accountability Act (HIPAA) (requirement added in December 2000)
- 1998 U.S. Digital Millennium Copyright Act (DMCA)
- 1999 U.S. Uniform Computer Information Transactions Act (UCITA)
- 2000 U.S. Congress Electronic Signatures in Global National Commerce Act ("ESIGN")
- 2001 Uniting and Strengthening America by Providing Appropriate Tools to Restrict, Intercept and Obstruct Terrorism (USA PATRIOT) Act
- 2002 Homeland Security Act (HSA)
Key U.S. Data Privacy Laws -- HIPAA

Health Insurance Portability and Accountability Act (HIPAA) (42 U.S.C. §1301 et seq.) Regulates medical information. Can apply broadly to health care providers, data processors, pharmacies and other entities that come into contact with medical information.

- HIPAA enacted by Congress in 1996.

- **Basic idea of HIPAA** is that an individual who is a subject of individually identifiable health information should have:
  - Established procedures for the exercise of individual health information privacy rights.
  - The use and disclosure of individual health information should be authorized or required.
COPPA

• Children's Online Privacy Protection Act (COPPA) passed in 1998 and effective in 2000 is a U.S. federal law that applies to the online collection of personal information by U.S. children under 13.

• Children–focused websites must protect children's privacy and safety online including restrictions on the marketing of those under 13.
  
  – Applies to commercial websites and on-line services either directed towards children under 13 or have knowledge that children under 13 are providing information on-line
  
  – Website operators must have privacy policies and seek verifiable consent from a parent or guardian
  
  – FTC enforces COPPA
FCRA

• The 1970 *Fair Credit Reporting Act (FCRA)* is a federal law that promotes accuracy, fairness, and privacy of consumer information contained in the files of consumer reporting agencies.
  
  − Intended to protect consumers from the willful and/or negligent inclusion of inaccurate information in their credit reports.
  
  − Updated in 2003 as FACTA (Fair and Accurate Credit Transaction Act). FACTA allows affiliate sharing of credit reports, “prescreening” of credit reports (unsolicited offers of credit to certain customers) and limited preemption of stronger state credit laws.

• **FCRA regulates the collection, dissemination, and use of consumer credit information.**

  − Enforced by the US Federal Trade Commission, the Consumer Financial Protection Bureau and private litigants.

• Credit reports used for background checks, insurance, employment, credit checks, etc.
FERPA

- The **Family Educational Rights and Privacy Act** of 1974 (FERPA or the Buckley Amendment) governs the access of educational information and records to public entities such as potential employers, publicly funded educational institutions, and foreign governments.

- The law applies only to educational agencies and institutions that receive funding under a program administered by the U.S. Department of Education.

**FERPA protects “educational records”:**
- Grades
- Class lists
- Student course schedules
- Disciplinary records
- Student financial records
- Payroll records for employees who are employed as a result of their status as students (RAs, TAs, Resident Assts, etc.)

**FERPA doesn’t protect**
- “Sole possession” records made by faculty and staff for their own use and not shared
- Personal observations
- University law enforcement records
- Medical and mental health records used to treat students
- Alumni records
- Peer-graded papers and exams prior to the grade being recorded
Role of the Federal Trade Commission

- The **Federal Trade Commission Act** (15 USC § 41 *et seq.*) has broad jurisdiction over commercial entities under its authority to prevent unfair or "deceptive trade practices." While the FTC does not explicitly regulate what information should be included in website privacy policies, it uses its authority to issue regulations, enforces privacy laws, and take enforcement actions to protect consumers. For example, the FTC might take action against organizations for:
  - Failing to implement and maintain reasonable data security measures.
  - Failing to abide by any applicable self-regulatory principles of the organization's industry.
  - Failing to follow a published privacy policy.
  - Transferring personal information in a manner not disclosed on the privacy policy.
  - Making inaccurate privacy and security representations (lying) to consumers and in privacy policies.
  - Failing to provide sufficient security for personal data.
  - Violating consumer data privacy rights by collecting, processing, or sharing consumer information is a violation of the FTC's consumer privacy framework or national privacy laws and regulations.
  - Engaging in misleading advertising practices.
Current Privacy Bills in Congress

State Privacy Laws

• There are many laws at the state level that regulate the collection and use of personal data, and the number grows each year.
  
  – Some federal privacy laws pre-empt state privacy laws on the same topic. Companies may find themselves in the position of complying with both.

• Most states have enacted some form of privacy legislation, however California leads the way in the privacy arena, having enacted multiple privacy laws, some of which have far-reaching effects at a national level. Unlike many federal privacy laws in the US, California's privacy laws resemble the European approach to privacy protection.

• Resource for privacy laws by state: https://www.epic.org/privacy/consumer/states.html
California has a constitutional right to privacy

Right to privacy guaranteed in California State Constitution:

• **ARTICLE I DECLARATION OF RIGHTS [SECTION 1 - SEC. 32]** (Article 1 adopted 1879.)

• **SECTION 1.** All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy. *(Sec. 1 added Nov. 5, 1974, by Proposition 7. Resolution Chapter 90, 1974.)*
California Consumer Privacy Act of 2018

- Act gives “consumers” (defined as natural persons who are California residents) four basic rights in relation to their personal information:
  1. The right to know, through a general privacy policy and with more specifics available upon request, what personal information a business has collected about them, where it was sourced from, what it is being used for, whether it is being disclosed or sold, and to whom it is being disclosed or sold;
  2. The right to “opt out” of allowing a business to sell their personal information to third parties (or, for consumers who are under 16 years old, the right not to have their personal information sold absent their, or their parent’s, opt-in);
  3. The right to have a business delete their personal information, with some exceptions; and
  4. The right to receive equal service and pricing from a business, even if they exercise their privacy rights under the Act.

- The Act’s provisions are designed to put these rights into practice.
- Goes into effect 2020.
CCPA Status

• Much discussion about feasibility and power of clauses in CCPA
• Final revisions modified
  – Notice of collection of personal information changed to *not* require explicit consent for *new uses* of personal information
  – Businesses that operate offline may require customers to *opt out via an online form*
  – *Removal* of a section requiring that customer opt-out may be “easy for consumers to execute” and require “minimal steps” to execute
• CCPA is more restrictive than EU’s GDPR but provides substantial consumer protections compared to federal law.
• California will provide important experience with consumer privacy law within the U.S.
Vermont Data Broker Law (H.764)
(from https://www.lexology.com/library/detail.aspx?g=5398e04c-f672-428e-b8f6-707538072acf)

• **Data broker** = a business that "knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship."

• Goal of the law is to regulate businesses that collect, aggregate, and sell data about consumers with whom the business **does not** have a relationship.
  – Businesses that collect, share, or sell their own consumers' data are not affected by this law, so long as they have a direct business relationship with those consumers.
  – Applies to Vermont residents (consumers) and businesses from anywhere

• **Law is the first of its kind in the United States**, became effective January 1, 2019.
First Vermont data broker enforcement action on Clearview

- State alleges that Clearview violated the data broker law by fraudulently acquiring brokered personal information through *screen scraping photographs* without consent and in violation of website terms of use, and exposing sensitive personal data to *theft* by foreign actors and criminals.

- State requests injunctive relief, restitution, disgorgement of Clearview’s profits, and *penalties of $10,000 for each violation*.

Lecture 9 References (not already on slides)

- COPPA, FCRA, FERPA, Wikipedia
- Fair Credit Reporting Act, EPIC, https://www.epic.org/privacy/fcra/
- “You need to understand your educational privacy rights”, Forbes, https://www.forbes.com/sites/willarddix/2018/05/16/you-need-to-understand-your-educational-privacy-rights/#7807ed576b93
- California approves final CCPA regulations, https://www.crowell.com/NewsEvents/AlertsNewsletters/all/California-Approves-Final-CCPA-Regulations

Fran Berman, Data and Society, CSCI 4370/6370
• Presentations for October 5


• Presentations for October 8


Need Volunteers – Presentations for October 15


• “Democrats are slight favorites to take back the Senate”, 538, https://fivethirtyeight.com/features/democrats-are-slight-favorites-to-take-back-the-senate/ (Zachary S.)
Presentations for Today

• “Nobody reads privacy policies. This senator wants lawmakers to stop pretending we do.”, Washington Post, https://www.washingtonpost.com/technology/2020/06/18/data-privacy-law-sherrod-brown/ (John)