Permissions

Agenda

- Announcements
- Follow-up to Identifiers
- Learning Outcomes
- Privacy
- Guest Speaker: Mayya Sharipova
- Break
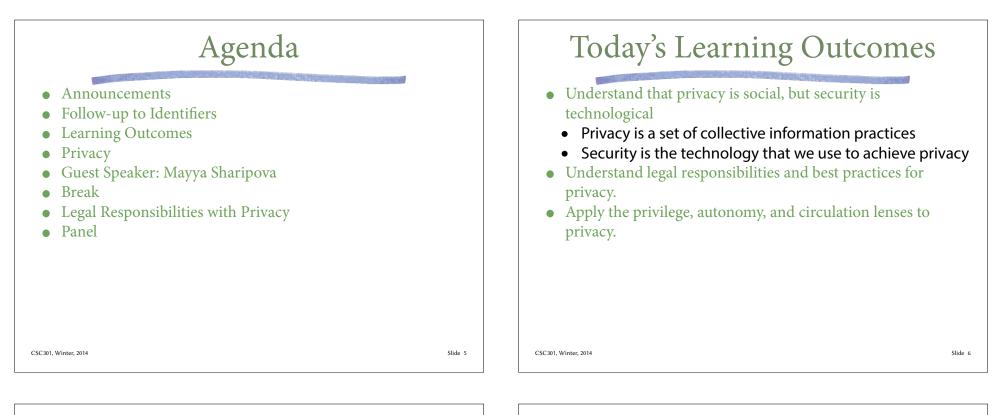- Legal Responsibilities with Privacy
- Panel

Identifiers Recap

- Identities are socially defined. They are performed for a particular social group within a specific situation.
- Within the self, the "me" is an object and represents a normative "generalized other."
- The "I" is the dominant subject and agent of novel action.
- Homunculus is not that relevant for this class.
  - Discussed as a poorly formed response to the question "Who are you talking to when you are talking to yourself?
- Sometimes an account is just an account. But other times, people are rehearsing a performance.
- Anonymous online identities lead to bad behaviour, because it allows people to avoid responsibilities.

Identifiers Recap

- Power. Who decides what identities can be portrayed?
- Privilege. What are the default assumptions? What identities are easy to portray online?
- Autonomy. Can I perform the identity of my choice online?

Agenda

- Announcements
- Follow-up to Identifiers
- Learning Outcomes
- Privacy
- Guest Speaker: Mayya Sharipova
- Break
- Legal Responsibilities with Privacy
- Panel

Today's Learning Outcomes

- Understand that privacy is social, but security is technological
  - Privacy is a set of collective information practices
  - Security is the technology that we use to achieve privacy
- Understand legal responsibilities and best practices for privacy.
- Apply the privilege, autonomy, and circulation lenses to privacy.

Quiz Question 2

- Privacy is a social consideration, while security is a technical concern.

Dourish and Anderson

- Privacy is "collective information practice"
  - Not a static set of permissions
  - More about what it does for us, rather than what is it
- Must incorporate notions of risk and danger
  - Social and cultural, as well as physical
- Information flows are markers of group membership
  - Remember identity?
- When designing, look at information practice, not just configurations and settings

Quiz Question 4

- Collective information practice includes

i) group identity and trust
ii) security configurations
iii) selective information sharing
X iv) information expiry
v) permanent information sharing

- i, iii, and v

Quiz Question 3

- Privacy is concerned with protecting secrets.

- False

Quiz Question 1

- Which one of the following is NOT a model of privacy discussed by Dourish and Anderson?

a) Discursive practice
b) Practical action
X c) Identity rehearsal
d) Economic rationality

Models of Privacy

- Economic rationality
  - Exchange value (information as a commodity)
  - Rational actor (trade off between risk and reward)
- Practical Action
  - Security is practical, ad hoc, in the moment accomplishments by social actors
  - Continual and ongoing production and reproduction
  - Everyday settings
- Discursive Practice
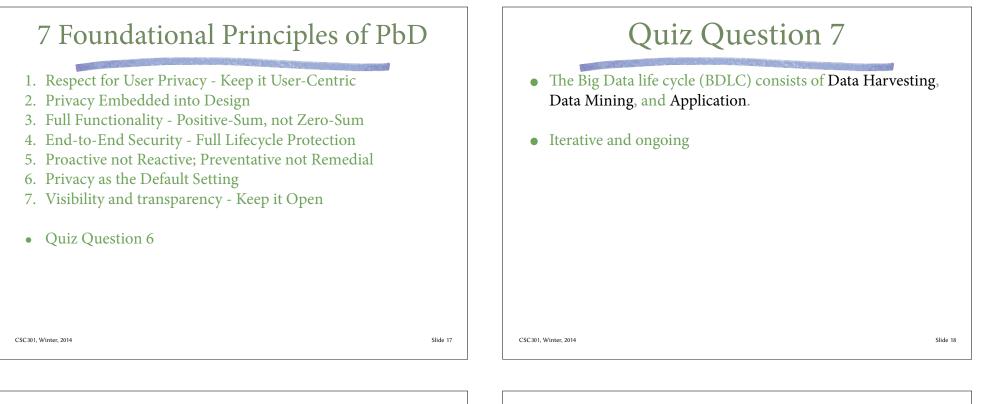 - Establishing categories of safe and unsafe through language = world shaping, defining

Quiz Question 5

- Risk assessments are as much about **rational criteria**, as they are about **moral judgements**.

Safety

- "The Righteous Mind: Why Good People are Divided by Politics and Religion" by Jonathan Haidt
- Uses the metaphor of the rider and the elephant to explain moral judgements
  - Elephant = emotions
  - Rider = reason
- Emotions react first, rational justifications come later
- Five Foundations for Moral Reasoning
  - Care/harm
  - Fairness/cheating
  - Loyalty/betrayal
  - Authority/subversion
  - Sanctity/degradation

Theory vs. Practice

- Dourish and Anderson give the theory
- Big Privacy and ACM are two sets of recommendations for best practices
  - How well do they fit? Or not?
  - Where do they converge? Where do they diverge?

Big Privacy

- Project by the Ontario Information and Privacy Commission, Anne Cavoukian
- Rooted in Privacy by Design (PbD) Principles
  - Privacy must be built in
- Big privacy is an application of PbD to big data

7 Foundational Principles of PbD

1. Respect for User Privacy - Keep it User-Centric
2. Privacy Embedded into Design
3. Full Functionality - Positive-Sum, not Zero-Sum
4. End-to-End Security - Full Lifecycle Protection
5. Proactive not Reactive; Preventative not Remedial
6. Privacy as the Default Setting
7. Visibility and transparency - Keep it Open

- Quiz Question 6

Quiz Question 7

- The Big Data life cycle (BDLC) consists of Data Harvesting, Data Mining, and Application.
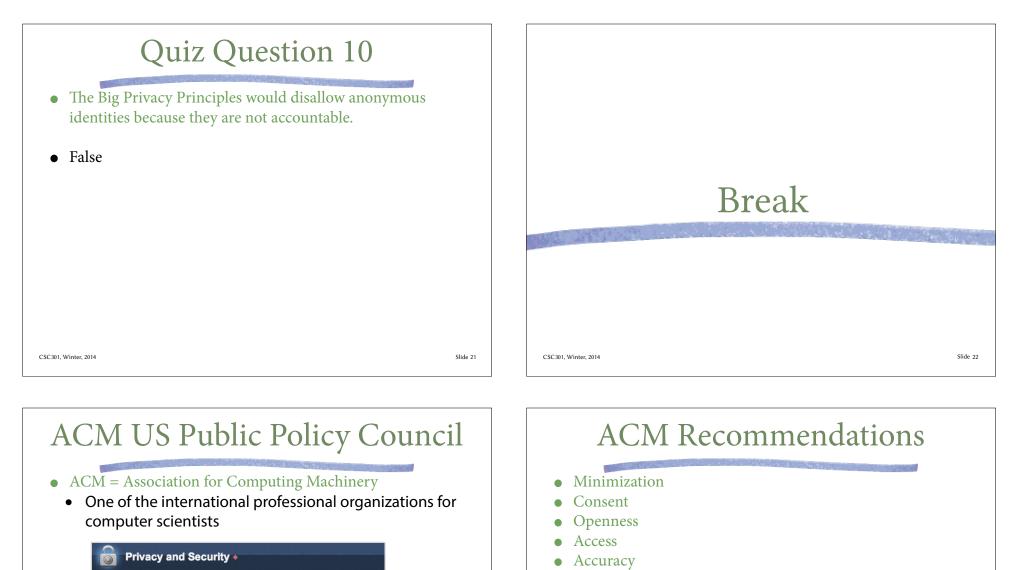
- Iterative and ongoing

Quiz Question 8

- Big Privacy includes
  - systemic protection of personal data
  - radical personal control over collection
  - protection applied to entire networks, value chains, and ecosystems
  - selective information sharing

- All of the above

7 Architectural Elements of Big Privacy

1. Accountable Pseudonyms
2. Identity and Data Portability
3. Trust Frameworks
4. Data-By-Reference
5. Semantic Data Interchange
6. Contractual Data Anonymization
7. Personal Clouds

- Quiz Question 9

Quiz Question 10

- The Big Privacy Principles would disallow anonymous identities because they are not accountable.

- False

Break

ACM US Public Policy Council

- ACM = Association for Computing Machinery
  - One of the international professional organizations for computer scientists

Privacy and Security ◆

Privacy and Security | Privacy Overview | Security Overview | Cybersecurity | Real ID | E-Verify | Social Security Numbers | Archives

ACM Recommendations

- Minimization
- Consent
- Openness
- Access
- Accuracy
- Security
- Accountability

PIPEDA

- Personal Information Protection and Electronic Documents Act (PIPEDA)
  - Applies private companies
  - The Privacy Act applies to government agencies
- Personal information = anything that can be used to identify a person
  - Especially health information
- Places electronic documents on same footing as paper

- For details, see the Privacy Commissioner of Canada
  - http://www.priv.gc.ca/leg_c/r_o_p_e.asp

PIPEDA

- Businesses must obtain consent when collect, use, or disclose personal information
  - Except in case of emergency where lives or safety at risk
- Information can only be used for the purpose for which it was collected
- Business are responsible for:
  - Protecting personal information
  - Ensuring accuracy
  - Openness about policies
- Individuals can see own data
- Data must be destroyed, erased, or made anonymous when original purpose has been served

Electronic Signatures

- The electronic signature must be unique to the person using it;
- The person whose electronic signature is on the document must have control of the use of the technology to attach the signature;
- The technology must be used to identify the person using the electronic signature; and
- The electronic signature must be linked to an electronic document to determine if the document has been changed after the electronic signature was attached to it.

Best Practice: Privacy Policy

- Your web site should have a Privacy Policy
  - Especially if you collect data
- Tell people
  - When you are collecting data
  - When you are installing a cookie
  - What you are going to do with the data collected
  - Who you're going to share the data with

Privacy and the Census

- Census is not subject to the same privacy constraints as rest of government data
  - Do not need to have purpose decided in advance
- Gold standard for privacy protection
  - Aggregation
  - Suppression
  - Physical protection

- Census privacy and this course

Today's Learning Outcomes

- Understand that privacy is social, but security is technological
  - Privacy is a set of collective information practices
  - Security is the technology that we use to achieve privacy
- Understand legal responsibilities and best practices for privacy.
- Apply the privilege, autonomy, and circulation lenses to privacy.

Up Next: Intellectual Property

- Sim and Stenberg gives an overview of current law (US-centric)
  - Standard view of intellectual "property" as a trade between disclosure and exclusivity
- Lessig is a Professor of law at the Berkman Center at Harvard
  - Video is his criticism of current copyright law (in the US)
  - Trade has gone too far in favour of creators
- Creative Commons podcast gives an alternative view of intellectual "property"
  - Creativity belongs to all, because it comes from all
  - Circulation lens