Course Overview

Anupam Datta
CMU
Fall 2017
Personal Information is Everywhere
Privacy and Fairness Problems

TECH

Google’s iPhone Tracking
Web Giant, Others Bypassed Apple Browser Settings for Guarding Privacy

By JULIA ANGWIN And JENNIFER VALENTINO-DEVRIES
February 17, 2012

WHAT THEY KNOW

When the Most Personal Secrets Get Outed on Facebook

By GEOFFREY A. FOWLER

Websites Vary Prices, Deals Based on Users’ Information

By JENNIFER VALENTINO-DEVRIES, JEREMY ASHKAN SOLTANI
December 24, 2012

PERSONAL TECH

‘Right to Be Forgotten’ Online Could Spread

Farhad Manjoo
STATE OF THE ART AUG. 5, 2015
Organizing Questions

- What is privacy? What is fairness?
  - From philosophical and legal conceptions to computer science and engineering
  - Inspiration from conceptions, but greater precision often through greater specificity

- How can we protect privacy and fairness?
  - Beyond creating laws and institutions
  - Computational mechanisms
Logistics
Course Staff

- **Instructor:** Anupam Datta
  - Office: B23, 221 (SV)
  - Email: danupam@cmu.edu
  - Office hours: Mon 12-1PM Pacific at SV + Google Hangouts

- **TA:** Sophia Kovaleva
  - Office: TBD (SV)
  - Email: sophia.kovaleva@west.cmu.edu
  - Office hours: TBD + Google Hangouts

**Extra office hours on demand**
Logistics

- Lectures: Monday & Wednesday, 1:30-3:20 PM Pacific (usually 90 minutes)
- Recitation: Friday 9:30-10:20am Pacific (attend!)
- Web page:
  - [http://www.ece.cmu.edu/~ece734/](http://www.ece.cmu.edu/~ece734/) (shortly)
  - [https://www.andrew.cmu.edu/user/mkovalev/18734/](https://www.andrew.cmu.edu/user/mkovalev/18734/) (currently)
- Canvas (for grades) and Piazza (for all other communication)
  - Please enroll in Piazza; you will receive invitation shortly
- Course work and grading:
  - Homework (60%) – 4 x 15%
    - Best 4 of 5 homeworks
  - Course project (30%)
  - Class participation (10%)
Logistics (2)

- Course Project:
  - Teams of 2 (form team by end of week)
  - Project proposal: 1-2 pages + in-class presentation (Sept 25)
  - Deliverable Part I + in-class presentation (Oct 30)
  - Deliverable Part II + Written report: 5-10 pages (Dec 6)
  - In-class presentation (Dec 4, 6)
Logistics (3)

Collaboration policy:

- You are allowed to discuss homework problems and approaches for their solution with other students in the class, but are required to figure out and write out detailed solutions independently and to acknowledge any collaboration or other source.

CMU Computing Policy
CMU Academic Integrity Policy
Logistics (4)

Example Violations:

- Submission of work completed or edited in whole or in part by another person.
- Supplying or communicating unauthorized information or materials, including graded work and answer keys from previous course offerings, in any way to another student.
- Use of unauthorized information or materials, including graded work and answer keys from previous course offerings.

...not exhaustive list

If in doubt, ask me!
Prerequisites

- An undergraduate course equivalent to 15-251 is required or permission of instructor

- An introductory course in computer security such as 18-487, 18-630, or 18-730 is recommended, but not required

- If in doubt, please talk to me after class

- Quick class poll
Privacy Problems
Module I: Privacy through Accountability

- Collection
- Use
- Dissemination
Web Privacy: Online Tracking

Independent tracking mechanisms on average on top-50 sites
Healthcare Privacy

Privacy Expectations

Patient information

Physician

Nurse

Drug Company

Hospital

Analyst

Patient

Patient information
A covered entity may disclose an individual’s protected health information (phi) to law-enforcement officials for the purpose of identifying an individual if the individual made a statement admitting participating in a violent crime that the covered entity believes may have caused serious physical harm to the victim.
Example privacy policies:

- Not use detailed location (full IP address) for advertising
- Not use health information for advertising
Setting:

- Auditor has access to source code
Web Privacy: Advertising

Sensitive Information (e.g., race, health information)

Google

Confounding Inputs

Use
Module I: Privacy through Accountability

- **Formalize Privacy Policies**
  - Precise semantics of privacy concepts
    (restrictions on personal information flow)

- **Enforce Privacy Policies**
  - Accountability
    - Detect
    - Explain
    - Correct

http://www.andrew.cmu.edu/user/danupam/privacy.html
Module I: Learning Outcomes

- Understanding of real-world privacy policies and laws
- Methods for detecting privacy violations
- Experience with audit tools for healthcare privacy
- Experience with web tracking investigation tool
Module II: Protecting Privacy and Fairness in Big Data Analytics

Collection  Inference  Use  Dissemination
Database Privacy Goals

- Health records
- Census data
- Web search records

Conflicting goals:
- Provide useful information
- Protect individual privacy
AOL apologized on Monday for releasing sensitive information about subscribers that had been intended for use on the company's newly launched research site.

The randomly selected data, which focused on 6,000 subscribers and posted 10 days ago, was aimed at helping Google improve its search engine. But the Internet giant has since removed the sensitive information from public view.

"This was a screw-up, and we're angry and upset," Google said in a statement, saying it was an innocent enough attempt to reach out to the community with new research tools, but it wasn't appropriately vetted, and if it had been, it would have been stopped in an instant." AOL, a unit of Time Warner, said its "top priority" was to make sure this kind of thing never happens again.
Anonymity of Netflix Prize Dataset Broken

Posted by Zonk on Tuesday November 27, 2007 @10:23AM from the there-are-degrees-of-anonymity dept.

KentuckyFC writes

"The anonymity of the Netflix Prize dataset has been broken by a pair of computer scientists from the University of Texas, according to a report from the physics arXivblog. It turns out that an individual's set of ratings and the dates on which they were made are pretty unique, particularly if the ratings involve films outside the most popular 100 movies. So it's straightforward to find a match by comparing the anonymized data against publicly available ratings on the Internet Movie Database (IMDb) (abstract on the physics arxiv). The researchers used this method to find how individuals on the IMDb privately rated films on Netflix, in the process possibly working out their political affiliation, sexual preferences and a
Google's RAPPOR aims to preserve privacy while snaring software stats

Apple's 'Differential Privacy' is about collecting your data—but not your data
Module II: Learning Outcomes

- Understanding of pitfalls in anonymizing databases
- Understanding of methods for releasing privacy-preserving statistics and their limitations
- Understanding bias in machine learning and corrective measures
- Understanding transparency (explanations) for decisions of machine learning systems
Module III: Cryptographic Mechanisms for Privacy Protection
Anonymous Communication
Anonymous Credentials

Organization

Service

Alice

Cred from Org
Name Alice
Address
Birthdate
Birthplace
Citizenship
...

“I have a cred from Org saying WA resident Age >18”

• Cannot
  • Identify Alice
  • Learn anything beyond the info she gives
• Distinguish two users with the same attributes
• Link multiple uses of the same credentials
Secure Two-Party Computation

Can Alice and Bob compute a function of their private data, without exposing anything about their data besides the result?

Bob’s Genome: ACTG...
Markers (~1000): [0,1, ..., 0]

Alice’s Genome: ACTG...
Markers (~1000): [0, 0, ..., 1]

\[ x = f(g_A, g_B) \]
Module III: Learning Outcomes

- Understanding of cryptography behind
  - Anonymous communication
  - Anonymous credentials (zero-knowledge)
  - Biometric identification (secure computation)
Fall 2014 Course Projects

- Studies of personal information usage by Web services
  - Study on Facebook ads
  - Price Discrimination
  - Recommendations for news articles
  - Effect of cookies on Google ads
- Analytics to discover information usage by Web services
  - Abstaining Machine Learning
  - Ensemble Machine Learning
- Privacy Protecting the New York Taxicab Dataset
- Defense against Canvas Fingerprinting on the Web
- Privacy and Security issues of Android ads
- ML (Lasso Regression) over Encrypted Big Data
Fall 2015 Course Projects

- Secure Modular Embedding: Comparing Signals without revealing them
- Robust Ad Collection
- Inversion Attack on Machine Learning Models
- Privacy in Election Campaigns
- Improving Usability of Private Browsing Mode
- Investigating gender discrimination in popular employment websites
- Comparing Privacy Tools
- Google Advertising Platform Case study
- The Unexpected Danger of Multiple Social Media Accounts: Instagram and Twitter Reveal More than You Think
- Effects of Browser-Type on Internet Results
An Organizing Viewpoint

Privacy as a right to restrictions on personal information flow

Collection  Inference  Use  Dissemination
Student Introductions

- Who are you?
- Why are you here?
Homework for Next Class

- Read the Fair Information Practices Principles

http://www.oecd.org/internet/ieconomy/oecdguidelinesonthe
eprotectionofprivacyandtransborderflowsofpersonaldatala.htm

- Critically read the entire privacy policy of a Web services
  company of your choice
  - Examine pairs of services owned by the same company (e.g.,
    Facebook-Whatsapp)
Homework Continued

Discussion questions:

- Try to find one example of a piece of the policy that maps to each principle.
- Can you find examples of principles that are not reflected in the policy?
- Can you find examples of policy clauses that reflect a principle that is not included in these principles?
- Are there policy clauses that could be more restrictive or less restrictive with respect to information use in order to better adhere to the principles?
- Are there parts of the policy that are too vague? If so, suggest alternatives.
- Are there conflicts in policies of service pairs owned by the same company?
Thanks! Questions?