Privacy and Anonymity in Data
Lecture 0

School of Computer Science
Carnegie Mellon University
latanya@privacy.cs.cmu.edu

Question Addressed in this Course

The emergence of many new technologies becomes increasingly hampered by privacy concerns because these technologies leave society vulnerable to privacy abuses.

Current situation.
Let society choose between benefiting from the technology and maintaining privacy protections.

Our solution.
To proactively construct privacy technology (and integrated policy) with provable guarantees of privacy protection while allowing society to collect and share person-specific information for many worthy purposes .

An Objective – data detective

In this course, you will learn how to exploit existing data collections and how to reason about vulnerabilities in publicly available information.

An Objective – data protector

In this course, you will also learn how to render person-specific information available such that the ability to identify individuals contained in the released data is controlled, yet the data remain practically useful.

Privacy and Anonymity in Data

Course begins officially Tues 9/14
because of SCS Graduate IC

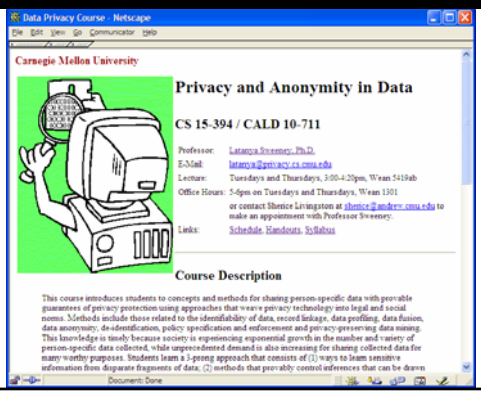
15-394 undergraduate /17-802, graduate version

Meets in Wean 5419ab

Highlights: importance of topic,
research effort,
programming requirement,
privacy technology emphasis,
term project

http://privacy.cs.cmu.edu/courses/pad1/index.html

http://privacy.cs.cmu.edu/courses/pad1/index.html



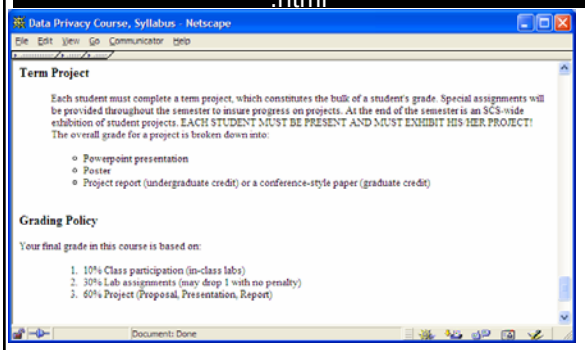
Overview of Course Requirements

1. Weekly lectures and discussions 10%
2. Weekly labs and homework assignments (grad students do more) 30%
3. Term Project, faculty showing at end of term. 60%
   -Powerpoint presentation
   -Poster
   -Project Report (undergrad)
   Conference-style paper (grad)

No exams.

Term project has a steady flow of deliverables to move you through the process: proposal abstract, introduction, methods, experiments, discussion

http://privacy.cs.cmu.edu/courses/pad1/syllabus.html



Background for Labs and Projects

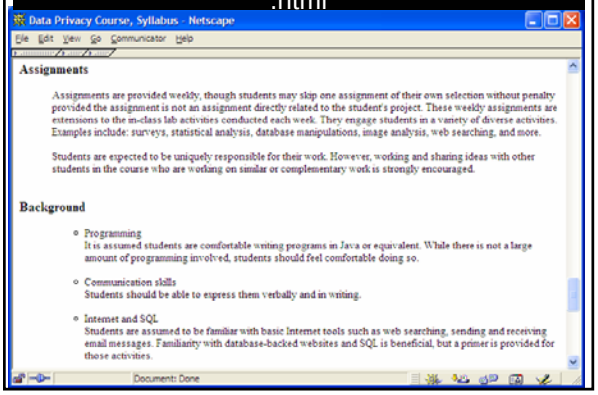
1. Programming (Java or equivalent)
2. Ability to express yourself in writing
3. Web searching beneficial

SQL beneficial, but there will be a primer provided.

Projects involve (data detective & data protective):
given a stated problem in a setting,

provide a programming or technical solution
a synthesis of solution into the social/policy setting
analysis of result

http://privacy.cs.cmu.edu/courses/pad1/syllabus.html



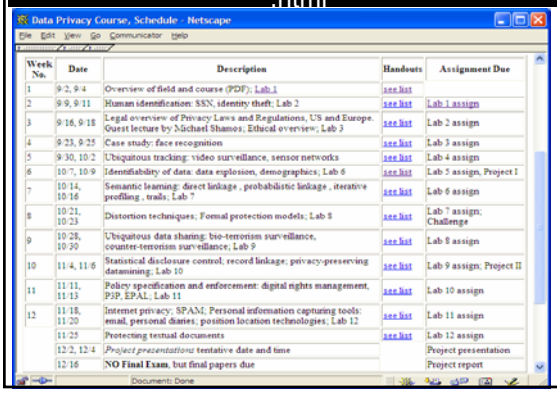
Course Materials

There are no books to purchase. We will provide you with copies of the materials you will need.

The basic text this term will be Prof. Sweeney's manuscript:

The Science of Privacy

http://privacy.cs.cmu.edu/courses/pad1/schedule.html



Emerging Technologies with Privacy Concerns

1. Face recognition, Biometrics (DNA, fingerprints, iris, gait)
2. Video Surveillance, Ubiquitous Networks (Sensors)
3. Semantic Web, Data Mining, Bio-Terrorism Surveillance
4. Professional Assistants (email and scheduling), Lifelog recording
5. E911 Cell Phones, IR Tags, GPS
6. Personal Robots, Intelligent Spaces, CareMedia
7. Peer to peer Sharing, Spam, Instant Messaging
8. Tutoring Systems, Classroom Recording, Cheating Detectors
9. DNA sequences, Genomic data, Pharmaco-genomics

Some Privacy Technology Solutions

- Face de-identification
- Self-controlling data
- Video abstraction
- CertBox ("privacy appliance")
- Reasonable cause ("selective revelation")
- Distributed surveillance
- Privacy and context awareness
- Data valuation by simulation
- Networks of people
- Video and sound opt-out
- Text anonymizer
- Privacy agent
- Blocking devices
- Query restriction