

Computer Science 199r

Special Topics in Computer Science

Privacy and Technology

Course Information -- Spring 2007

Case studies of areas in which there are perceived conflicts between individual privacy and computer technology. Which of these conflicts are real? Which could reasonably be addressed through changes in policy and technology? Areas include RFID, surveillance, biometrics, data aggregation and data mining.

A defining goal of the course is to bring together students from disparate disciplines so that each can learn from the other while tackling problems where technology and policy are deeply tangled. The course is designed around a case-study approach; we will create inter-disciplinary teams of students for discussing and studying the various cases.

The specific focus of the proposed course is to study several areas in which privacy and technology are thought to be in conflict, decide if these conflicts are real and, if so, discuss what could reasonably be done about them in the areas of both technology and policy. The subtext of this thrust is that much of the current debate over the privacy-invasiveness of technology rests on misunderstandings of what is really possible with technology and which technologies constitute the most potent threats to individual privacy. We will look at a number of current controversies having to do with the use of technology and the effects of that use on individual privacy, along with the laws and regulations that have been designed or interpreted as relevant to these issues.

1 Administrative Details

Class hours: TuTh from 2:30-4pm in Maxwell Dworkin G115

Course page: <http://www.eecs.harvard.edu/cs199r>

Instructors: Mike Smith -- MD 329 -- 6-5661 -- smith [at] eecs.harvard.edu
Jim Waldo -- waldo [at] eecs.harvard.edu
Alon Rosen -- alon [at] eecs.harvard.edu
Allan Friedman -- allan_friedman [at] ksgphd.harvard.edu

Administrative Assistant: Tristen Hubbard -- MD 239 -- tristen [at] eecs.harvard.edu

2 Prerequisites

None. The course is open to all students.

3 Course Requirements

Each two-week unit in the course will comprise two lectures and two discussion sections. In support of each unit, each student will be asked to read a number of papers on the topic of the unit, write a short position paper (2-3 pages) responding to a couple of open-ended questions, prepare for and participate in the discussion sections, and work together with a handful of classmates to produce a final briefing

document proposing several specific action items addressing the one problematic aspect of the unit's topic. Late assignments will not be accepted; attendance at all course meetings will be expected.

The final project will be to prepare a briefing book for a high-level interdisciplinary task force discussing some new technology and its privacy implications. Student groups will summarize the technology and key aspects of its implementation and potential use, and present a detailed list of critical discussion questions for this task force. The briefing should contain an annotated list of readings, discuss historical analogs, and recommend one or two potential experts to interview. Students will be asked to present a summary of the briefing book and defend their choices during the first week of reading period. A more detailed description of the final project will be distributed before spring break. Students will be expected to hand in a project proposal on April 13, 2007, and a completed briefing book on May 14, 2007, at 5pm.

There will not be any examinations given in this course.

4 Cooperation

Due to the interdisciplinary nature of the course topic, the students will be expected to work with each other and learn from each others' perspectives and backgrounds.

5 Grading

25% Class participation
25% Personal writings
10% Group writings
40% Final project/paper

6 Textbooks and Other Readings

There is no required text for this course. All reading material will be distributed in class or will be available on the Internet. The foundational aspects of the course will be based on an about-to-be-published study from the National Academies on privacy. This material will be supplemented with technical, academic, and popular-press readings from the Internet, including the web sites for the Electronic Frontier Foundation and the Electronic Privacy Information Center. Outside speakers will also be invited to shed light (or generate heat) on some of the topics.

7 Envisioned Schedule

2/6-2/16 What is Privacy?
2/20-3/1 RFID
3/6-3/15 Public Surveillance and Identification from a distance
3/20-4/5 Data Aggregation, Data Mining and Linking information
4/10-4/19 Anonymity
4/24-5/3 Medical privacy
5/8-5/10 Presentations (Reading period)