Study Sheet for Exam 2, CPSC 457/557, Fall 2011

Exam 2 will be based on the material covered in class between October 11, 2011 and November 17, 2011 (inclusive) and in the reading assignments for these class sessions. It will be a 1.25-hour, closed-book exam.

This "study sheet" specifies, for each topic that's in scope, the main points that you should focus on in preparing for this exam.

Anonymity on the Internet (Margot Kaminski, Wendy Seltzer, and Anton Petrov)

- The legal argument that anonymity is a free-speech/free-press right and the arguments for and against treating Internet- and print-based communication identically
- The main points of the Tor approach to anonymous communication on the Internet
- Narayanan and Shmatikov's approach to re-identification of NetFlix data

The National Strategy for Trusted Identities in Cyberspace – NSTIC (Aaron Segal)

- The goals and basic technical approach of the NSTIC
- Typical use cases for the NSTIC
- The strengths and weaknesses of this approach that are explicated by Mayer and Narayanan

Privacy Implications of Ad Targeting (John Langhauser)

- The approach of the EU "Privacy and Electronic Communications Directive"
- The approach of the US "Commercial Privacy Bill of Rights" proposed by Senators Kerry and McCain
- Privacy advocates' objections to the Kerry-McCain bill
- The design, findings, and implications of the Goldfarb-Tucker experiment

Location-based advertising (Matt Gaba)

- The government and regulatory approach covered by Desai *et al.*
- The main points of US Patent 7,668,832 (awarded to Google for location-based advertising); see, in particular, "Summary of Invention" and "Related Art"
- The main points of the Gedik-Liu approach that Matt presented in class

Gmail and Privacy (Ben Silver)

- How ad targeting works (technically) in Gmail
- Google privacy policies that are applicable to Gmail
- Arguments for and against the "reasonableness" of Gmail's ad-targeting approach and the claim that it does not "lessen the reasonable expectation of privacy" in email

Differential privacy

See the CACM paper “A firm foundation for private data analysis,” by Cynthia Dwork

- Naïve approaches that do not work and why they do not work
- Dalenius’s goal and why it is unattainable
- The (technical) definition and (intuitive) meaning of differential privacy
- Examples of differential-privacy solutions to datamining problems: “how-many-rows” and histogram queries

“Traditional” digital cash (based on cryptographic signatures)

See Section 12.5 of “Lecture notes on cryptography,” by Shafi Goldwasser and Mihir Bellare

- The four properties required of a digital-cash scheme
- The basic protocols that achieve these properties
- The roles of digital signatures, blinding, cut-and-choose, and one-way hashing in achieving these properties

Hashcash

See the paper “Hashcash: A Denial of Service Counter-Measure,” by Adam Back

- The basic Hashcash protocol and why it works
- The canonical use case for Hashcash: spam fighting; why Hashcash is more appealing in this use case than “traditional” digital cash

The BitCoin Digital-Currency System (Max Uhlenhuth)

- The main (technical) points of the BitCoin approach to digital currency
- The major ways in which BitCoin differs from earlier approaches to digital currency; BitCoin’s comparative strengths and weaknesses