Privacy in a Networked World: Differential Privacy, Information flow

Differential Privacy

- For detailed notes see Pages 1-5 (excluding Section 3.1) in this paper
- Cryptographer's view of privacy
- Count queries, Definition of Privacy, Attack Semantics, Sensitivity, Laplace Mechanism, Proof of Differential Privacy of Laplace mechanism
- Modification for Subset-sum queries
- Comparison with notion of incentive compatibility

Issues in applying Differential priv.

- Randomization
- Repeated queries reduce noise
  - Finite privacy budget
- Picking epsilon; still has some privacy risk, though bounded
- Far removed from current practice
- Twins paradox; see this paper
- Only impossible to tell if individual participated in database
- Loss of utility may be too strong

Google Streetview

http://www.streetviewfun.com/2012/stanford-university-visitors/

http://www.streetviewfun.com/2010/google-cameras-filming-in-your-streets/

Buzz incident

- New social network ~ 2010
- Made gmail contacts public!

Social Network Privacy

- Beacon that shared users' actions on external partner Web sites via the News Feed (Facebook, 2007)
- "Many users believed that there was a significant difference between knowing that someone changed their relationship status by regularly visiting the person's profile and seeing it listed as an action in the News Feed" Boyd 2008.

- Evolution of Facebook privacy: http://firstmonday.org/ojs/index.php/fm/article/view/3086/2589#fig2
- Point: Controls have evolved to be clearer: http://www.facebook.com/help/privacy

- But what should defaults be?

Browser privacy

- Cookies
  - Make server stateless by storing information on client (browser)
  - Used for authentication, session management, personalization ...
- Third-party cookies are problematic
- Third-party cookie set by domains that hold components of the webpage, that don't match the webpage's domain

Do Not Track

- Superficially similar to 'Do not call'
  - but not quite

- Message from browser client to server requesting that server disable tracking 'or' cross-site user tracking

- Based on honor code
- See this for a discussion: http://www.wired.com/opinion/2013/04/do-not-track/

Incognito mode

- Webpages that you open and files downloaded while you are incognito aren't recorded in your browsing and download histories.
- All new cookies are deleted after you close all incognito windows that you've opened.
- The websites you visit may still have records of your visit
  - signed-in users, IP address?
  - https://panopticlick.eff.org/

How should we think about these privacy use-cases?

Why do we need privacy?

Definitions of Privacy

- right of the individual to define his or her essence as a human being
- moral freedom of the individual to engage in his or her own thoughts, actions and decisions
- right to decide "when, how, and to what extent information about them is communicated to others"
- secrecy, anonymity and solitude

Contextual Integrity(Nissenbaum'04)

Norms of appropriateness

What information is revealed in what context?

Norms of flow

What information is transmitted in what context?

Norms evolve over time

My view of privacy

- We make decisions that affect people based on their personal information
- Assuming honesty and competence, of the decision-maker, possibly no need for privacy
  - privacy laws and other laws
- Assuming honest and competence of the individual everything can be on a 'need to know basis'
  - examinations or reputation systems
- Make this a basic right
- Rely on the past to establish norms for each context

Contd.

- For new contexts, past is not a good indicator of norms
- So tread carefully, transparently, and offer control
- In practice, 'free-riding' could be an issue