

## Privacy

---

Info 344 Winter 2007

## Administrivia

---

- r Lab 8 due today at end of day
- r Project 3 (Model and View Classes) due Thursday
- r Project meetings continue today
  - λ ~20 to go @ 3-4 minutes each
- r Changes to Discussion Forum
  - λ New section: PHP and MySQL Tips
  - λ POST YOUR PROJECTS!
- r PHPS files

## Looking Ahead

---

- r Thursday: Kirk Bailey, UW CISO
- r Tuesday, Douglas McDavid, IBM
- r Two labs: RSS and Web Services
- r Project 4 (Database Access) due Thursday Feb 22
- r Writing Assignment on Security and Privacy up Thursday, due March 8
- r Final Project: DUE 10:00am March 16

## And now...

---

- r Linda Lane on Privacy

Views on Privacy

### Dr. Jakob Nielsen

[http://www.digital-web.com/articles/jakob\\_nielsen/](http://www.digital-web.com/articles/jakob_nielsen/)

**JN:** Trust is a huge problem. Users are justifiably very cynical about their privacy and about the extent to which they can trust Web sites. In our recent study of newsletter usability, we saw a lot of people being very hesitant to sign up for a totally honest and legitimate newsletter because they were afraid of spam and shady marketing. It's going to be a big challenge to find ways to reaffirm the credibility of honorable websites that respect users' rights.

## Privacy Information

---

What we will briefly cover -

1. Historical roots of the concept of privacy: Privacy protection in tort and constitutional law
  - Responses reduce privacy to other interests
  - Coherent concept with fundamental values
2. Critiques of privacy as a right.
3. Array of philosophical definitions / defenses of privacy as a concept, with meaning and value.
- 4. Challenges to privacy in technology.**
5. What to consider as best practices.

## History of Privacy

- r Aristotle's distinction
  - λ **public** sphere of political activity
  - λ the **private** sphere associated with family and domestic life
- r American Law
  - λ Treatises in 1890's privacy protection
  - λ *descriptive* accounts of privacy
  - λ *normative* accounts of privacy defending its value
  - λ moral or legal *right* that ought to be protected by society or the law

## Privacy Skeptical & Critical Accounts

- r No right to privacy - nothing special about privacy
  - λ Equally well explained and protected by other interests or rights, notably **rights to property and bodily security** (Thomson, 1975).
  - λ **Economically inefficient** (Posner, 1981)
  - λ Inadequate **legal** doctrine (Bork, 1990)
  - λ Detrimental to women because it is used as a shield to dominate, control, silence and cover up abuse (Mackinnon, 1989).

## Privacy Meaningful & Valuable

- r **Control over personal information** (Parent, 1983)
- r Required for **human dignity** (Bloustein, 1964)
- r **Crucial for intimacy** (Gerstein, 1978; Inness, 1992)
- r **Ability to control access others have to us** (Gavison, 1980; Allen, 1988; Moore, 2003)
- r Enhance personal expression and choice (Schoeman, 1992)

## Defining privacy

- r Warren and Brandeis, Harvard Law Review, 1890:

"The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments and emotions shall be communicated to others. Under our system of government he can never be compelled to express them (except upon the witness stand); and even if he has chosen to give them expression, he generally retains the power to fix the limits of the publicity that shall be given them."

## Modern definition of privacy

From modern US tort law, four types of *invasion of privacy*:

1. Intrusion of solitude (unwanted publicity)
2. Public disclosure of private or embarrassing facts
3. Portrayal in false light
4. Appropriation of another person's identity

We have intuitive moral ideas about what "privacy" means

## Ethics in a Free Society, Why is this Case Important?

- r "Nussenzweig, an Orthodox Jew, claimed that diCorcia, a photographer using his image violated his First Amendment right to religion on the grounds that his image constituted a graven image that was exhibited and consumed commercially.
- r Multiple prints of Nussenzweig's photo sold for about \$20,000 each and published in "Heads," a book that sold several thousand copies
- r Justice Judith J. Gische said that Nussenzweig's claim to **privacy was not valid**, finding that diCorcia created the photograph for **artistic purposes**."

## Legal precedents

- ⌞ In US, Warren and Brandeis set the stage for civil privacy protection
  - ⌘ Fourth Amendment protects against govt's "unreasonable search and seizure"
  - ⌘ No specific discussion of privacy in Constitution
  - ⌘ HIPAA protects privacy of health information
  - ⌘ SOX exposes SDLC process declaring funds
- ⌞ EU supports stronger privacy regulations
  - ⌘ Organization for Economic Cooperation and Development (OECD)
- ⌞ For private US organizations, privacy protection is good practice, *but what does this really mean...*

## Who controls information about you?

- ⌞ The Web raises some interesting issues related to privacy
  - ⌘ Information lasts forever
  - ⌘ Easily searchable
  - ⌘ Anyone may publish
- ⌞ Many types of personal information stored online
  - ⌘ Credit cards
  - ⌘ Student information
  - ⌘ Photos
  - ⌘ Blogs, MySpace, etc...

## Privacy and Technology

- ⌞ Massive databases and Internet records of information, individual financial and credit history, medical records, purchases, and telephone calls
- ⌞ People do not know what information is stored or who has access
- ⌞ Access to databases? few controls on how they use, share, or exploit the information
- ⌞ Makes individual control over information about oneself difficult

## Information Tools

Caller ID, smart cards  
RFID leaks privacy information through DNS  
Mandatory drug tests  
Surveillance photos, Face scanning  
Global Positioning System (GPS)  
Satellites  
Electronic trackers  
FBI Web Carnivore surveillance system  
Echelon covert global satellite network - intercepts all phone, fax, and e-mail messages in the world, up to 20 international listening posts  
Biometric identification using faces, eyes, fingerprints, and other body parts

**Technology for matching the information with other databases Such as cross referencing cookies from divergent sources**

## Some scenarios to consider

- ⌞ Red Square webcam
- ⌞ Job interview searching MySpace
- ⌞ Sharing a computer with a housemate
- ⌞ Many possible scenarios
  - ⌘ Guidelines alone not enough

## Opt in vs. opt out

- ⌞ *Opt in:* choose to allow the site to collect or use personal data
- ⌞ *Opt out:* By default, site may use data, unless you explicitly tell them not to

## Some best practices

---

- r Opt in vs. opt out
- r Security
- r Allow deletion of personal data
- r Privacy policy

## Opt in or opt out

---

### Good

Click here to be added to our e-mail newsletter

### Bad

Click here if you do not wish to be added to our list

### Worse

If you wish to be removed from our list, send an e-mail to [service@badguys.com](mailto:service@badguys.com)

By signing up you agree to allow us to share your data with our partners

## Security = privacy

---

- r Private data can only be protected as long as it is stored securely
- r Take security precautions when handling personal data
- r Disclose security risks in privacy policy

## Deleting data

---

- r The user should be able to *delete* any personal data that he or she does not want stored anymore
- r This can be a problem if information ends up in many places
  - λ Google caches *forever*
  - λ Public or private archive
  - λ Copied to other sites
    - Wayback Machine is just one public site that does

## Privacy policies

---

- r A *privacy policy* document describes how information will be collected and used by an organization
- r Should describe
  - λ What information will be collected
  - λ What this information will be used for
  - λ Who will have access to information
  - λ Retention and deletion policies, etc.
- r Privacy policy should be easily accessible from any page that collects data (or from every page)

## Privacy policy: QFC

---

The information gathered by QFC will be used to give you, our valued customer, our very best. You have our word on that!  
**We pledge that QFC will not release your name to any list service or manufacturer, and that such information will be held in the strictest of confidence—even within our company.**

## Privacy policy: continued

---

***Kroger and its affiliates may use personal customer information to create merchandising and promotional programs tailored around specific purchases, the frequency of store visits, volume of purchases, and other data...***

***We may share personal customer information with our subsidiaries, affiliates, agents, representatives and trusted partners for the limited purpose of providing services or information to Kroger or our customers at our discretion.***

## Designing for privacy

---

- r How can we design our web applications to support users' right (or desire) for privacy?
- r Best approach takes into account multiple viewpoints
  - λ Draw from guidelines, laws
  - λ Interview and test with users
  - λ Draw from our own thoughts and experiences
- r Let's talk about our own experiences related to privacy

## Microsoft's Privacy Statement

---

### Exercise

- r <http://privacy.microsoft.com/en-us/fullnotice.aspx>
- r What is Trust-e?
- r What about your Privacy?
- r What Benefit

