Privacy

INFO/CSE 100, Autumn 2004

Fluency in Information Technology

http://www.cs.washington.edu/100

Readings and References

- Reading
  - » *Fluency with Information Technology*
    - Chapter 17, Privacy and Digital Security
- References
  - » *Harvard Law Review*
    - The Right to Privacy. Samuel Warren and Louis Brandeis. Vol. IV, December 15, 1890, No. 5
  - » Hall Health Center
    - Release of Information Questions

http://www.hallhealthcenter.com/article-detail.asp?ArticleID=176&ClinicID=1

What is Privacy?

- *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 when 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 which shall be given them.*

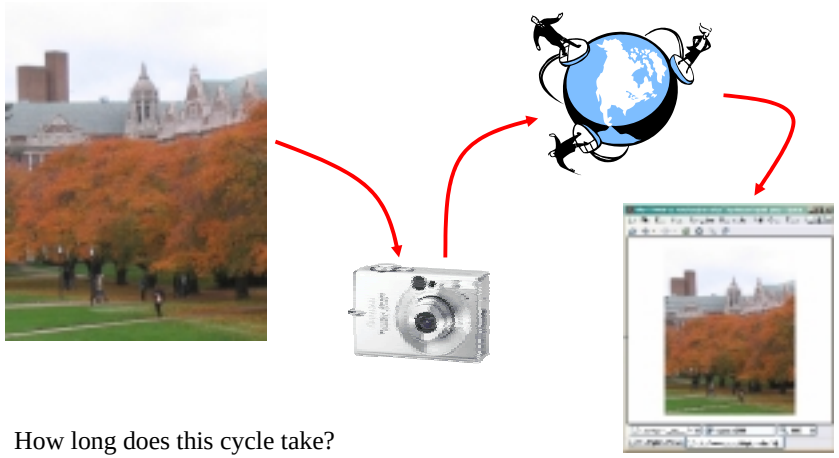
Warren and Brandeis

What is Privacy?

- *Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone". Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."*

Warren and Brandeis

"proclaimed from the housetops"



How long does this cycle take?

Are these privacy issues?

- Personal records
  - » grades, transcript
  - » payment history, personal evaluations
  - » medical exams, prescription drugs
- Buying patterns
  - » Bought airplane ticket, new skis, gasoline
- Browsing patterns
  - » Visited airline schedule page, searched for currency exchange rate for Canada

UW Privacy

- Family Educational Rights and Privacy Act
  - » "As a general rule the University will not release a student's education records to a third party without written consent of the student. This includes tuition account information."
- UW Libraries Privacy Statement
  - » "The University of Washington Libraries values the privacy of library users. The Libraries seeks to minimize the collection and retention of personally identifiable information."

Medical Records Questions

- Who owns my medical record?
  - » Your health record is the physical property of the healthcare provider/facility but you have a right to:
    - a. Review and/or have a copy of that record.
    - b. Ask to have your medical record corrected.
    - c. Not have your medical information disclosed to others unless you direct us to do so or unless the law authorizes or compels us to do so.

Hall Health

Medical Records Questions

- Can my medical record be disclosed without my authorization?
  - » Yes, there are state laws, which provide disclosure without patient authorization but every effort is made to get a written authorization from the patient prior to release. Refer to: Revised Code of Washington (RCW) 70.02.050
  - » Examples: referrals to another provider, court orders, and insurance companies for billing purposes.

Hall Health

Purchasing patterns

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.

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. Kroger also may use the data it collects to investigate and respond to customer requests, concerns, and claims.

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

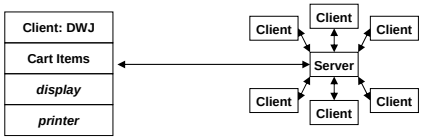
Digital Privacy

- How private is your information online?
  - » Reputable online business post Privacy Statements
  - » The statement should understandable to you and say what info they collect, what they will do with it, how to "opt-out", etc.
  - » But, there is little policing & few penalties

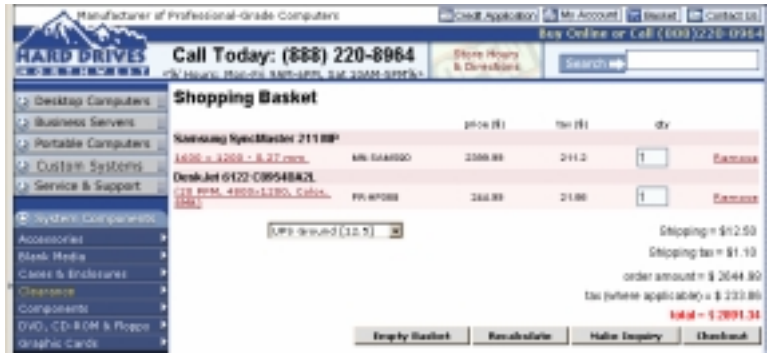
Real Networks in 1999 secretly gathered data on people's personal music tastes, encrypted the info so no one would know, didn't mention it in their privacy statement, and used TRUSTe auditor -- the day after getting caught, they improved their privacy statement … should we ever trust them???

Cookies

- Cookie: a record stored by a Web server on a client (your computer)
  - » The cookie is usually a unique ID that allows the server to remember who you are
  - » This is a well known web design idea that improves Web the web experience



A Holiday Shopping Cart



I wish!

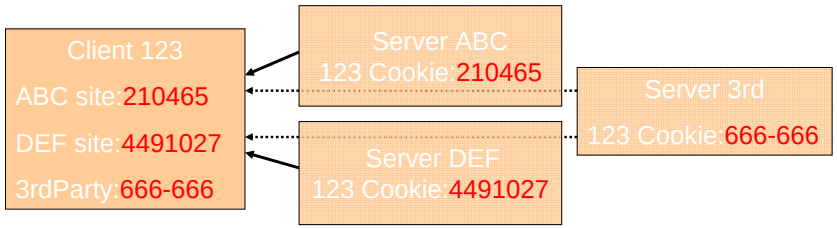
Cookies: Good

- Cookies are used by many sites and they make Web usage much better
  - » Many sites, e.g. Oxford English Dictionary use cookies
  - » Banking and credit card applications cannot be secure enough without cookies
  - » If privacy laws were truly strong and enforced, cookies would be all good and no one but computer scientists would know about them

But there are some problems …

Cookies: Bad

- Cookies can be stored in your computer by sites you have not visited: 3rd party
  - » 3rd Party Cookies come from a site in business with the site you visit, e.g. for ads
  - » 3rd party cookies allow info to be correlated



Correlating Cookies

- The 3rd party cookie becomes the key (literally, in the database sense) to join the info held by separate companies

Company ABC Database

Customer	Cookie	Ad Agcy	Data1	Data 2	...
123	210465	666-666	Nextel	360	

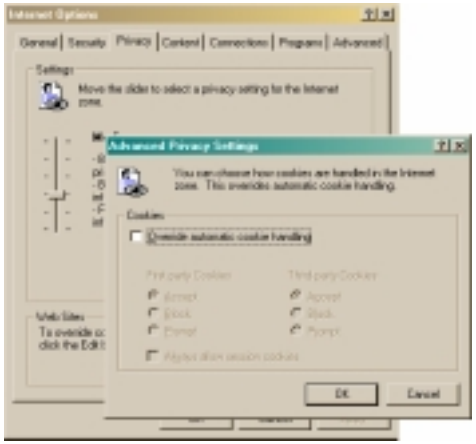
Company DEF Database

Customer	Cookie	Ad Agcy	Data1	Data 2	...
123	4491027	666-666	Dell	Samsung	

Managing Cookies

- You control whether your computer accepts cookies -- look in browser
  - » If you don't care about privacy, accept all cookies
  - » If you greatly value your privacy, accept no cookies
  - » If you want some privacy AND benefit from the useful stuff on the Web, accept cookies but reject 3rd party cookies

Setting cookie control in IE



Fair Information Practices

- To protect privacy in Information Technology, US Dept of Health, Education and Welfare created "Fair Info Principles"
- Organization of Economic Cooperation and Development (OECD) expanded these principles

Limited Collection Principle	Security Principle
Quality Principle	Openness Principle
Purpose Principle	Participation Principle
Use Limitation Principle	Accountability Principle

Europe vs America

- European Union, much of non-EU Europe, New Zealand, Hong Kong, Australia, Canada use OECD
  - » US privacy law for government has been strong
  - » US privacy law for business is "sectoral", meaning it is limited to sectors and specific business practices
  - » Many issues surrounding Opt-in/Opt-out and Enforcement