Internet Law

- Module 6
- Privacy Online

Privacy Protection - U.S.

- Policy overtones
  - Market regulation or legislation?
  - Economic benefits of less-intrusive regime justify privacy intrusions?
  - Should privacy online be treated differently from privacy offline?
- U.S. approach is ad hoc
- Some differences in online environment for B2C
  - Data collection
  - Capture of pre-transactional "shopping" data
  - Lack of anonymous payment mechanism
  - Shipping
- FTC: don't single out online world for data collection regulation
- Reidenberg: "private organizations now have exclusive control over the decisions regarding the collection and use of personal information . . . "

Tensions within Privacy . . .

- Values of privacy
  - Obscure identity information
  - Anonymity
- Competing interests
  - Accountability
    - Some “speech acts” bring liability
    - How does government find the speaker if privacy protection is too strong
  - Free circulation of ideas
    - Including free association
  - Efficiency
    - Targeted marketing as more cost effective marketing

Tensions within Privacy . . .

Privacy Lost: These Phones Can Find You

By LAURA M. HOLSON
Published: October 23, 2007

Two new questions arise, courtesy of the latest advancement in cellphone technology: Do you want your friends, family, or colleagues to know where you are at any given time? And do you want to know where they are?

E-MAIL
PRINT
REPRINTS
SAVE
SHARE

ARTICLE TOOLS SPONSORED BY
AN AMERICAN EMPIRICAL PICTURE BY WES ANDERSON

Obvious benefits come to mind. Parents can take advantage of the Global Positioning System chips embedded in many cellphones to track the whereabouts of their phone-toting children.

And for teenagers and 20-somethings, who are fond of sharing their comings and goings on the Internet, youth-oriented services like Loopt and Buddy Beacon are a natural next step.

Sam Altman, the 22-year-old co-founder of Loopt, said he came up with the idea in early 2005 when he walked out of a lecture hall at Stanford.

Salesgenie.com - ...

Salesgenie.com™
Unlimited Sales Leads

Where does your data come from?

Our Business Data:

- We split apart and catalogue 5,200 phone books, annual reports and other business directories to find information on nearly every business in the nation.
- Next, we hand-key each record and call every business to make sure you have the most reliable information available.
- Public record data from county courthouse filings, SEC and 10K filings, and Secretary of State data are then entered.
- Every week 50,000 new businesses are added from sources such as new business registrations and utility hookups so you can be the first to reach a hot new prospect.
- Every month, we match and clean the data with the USPS National Change of Address (NCOA), ZIP+4 and Delivery Sequence Files to standardize and keep the addresses accurate.

Our Consumer Data:

- We split apart and catalogue 4,300 telephone directories.
- Data specialists examine each listing and enhance it with buying habit and lifestyle information from real estate transactions, product registrations, magazine subscriptions, and survey responses.
- Every week we release 300,000 new movers.
- Every month we match and clean the data with the USPS National Change of Address (NCOA), ZIP+4 and Delivery Sequence Files to standardize and keep the addresses accurate.

- Waning from a historical high of privacy?

Privacy Quadrants

	Public	Private
Offline	· Government surveillance . . .	· Customer affinity programs · After-markets for aggregated customer data
Online	· Government surveillance with the enhanced power to monitor more information at lower cost due to dropping cost of information technology	· B2C transactions · Online profiling via surfing or searching · After-markets for aggregated customer data

FTC - Fair Information Practices Principles

- Notice / Awareness
- Choice / Consent
  - Internal versus external secondary uses of information
- Access / Participation
  - View and contest
- Integrity / Security
- Enforcement / Redress
  - Self-Regulation
  - Private Remedies
  - Government Enforcement
- Opt-in versus Opt-out & default rule

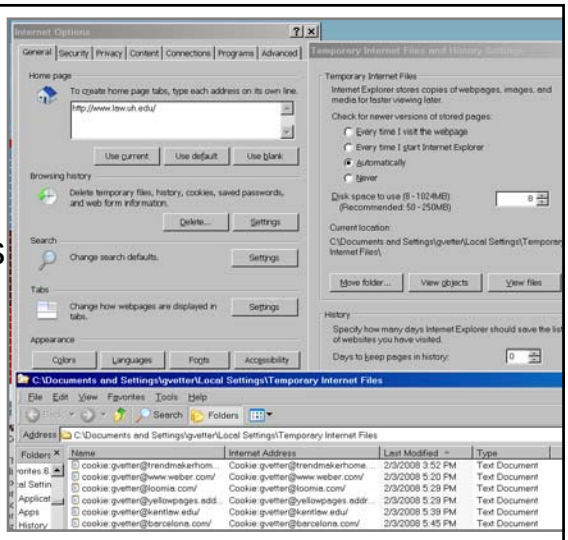
FTC - Fair Information Practices Principles – Question 1

Hypothetical Privacy Notice:

We collect and retain all of the personally identifiable information we can extract from your online activities, including all of you clickstream activity. Using a cookie, we associate this information with your online identity. We also make every effort to link this information to your real-world identity, and are usually successful. We will use the information we have gathered to target you with customized marketing materials to whatever extent we find profitable. We will also avail ourselves of every opportunity to sell, rent, share, or trade your personal information with any commercial entity if by doing so we can turn a buck.

Online Surveillance

- Cookies
  - Session versus persistent
- Hardware identifiers
- Web bugs
  - Potent because it can transmit to other servers
- Email and document bugs
- Spyware & adware



Online Profiling

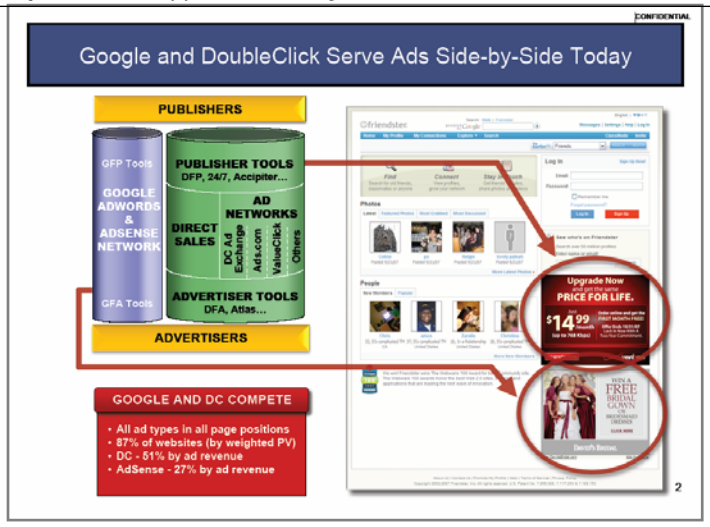
- Non-PII or PII

If you select a DART opt-out cookie, ads delivered to your browser on behalf of clients using DoubleClick's ad-serving technology will be targeted based only on the non-personally-identifiable information that is automatically transmitted in the Internet environment when an ad request is received by our ad servers, and your DART cookie will not be uniquely identified. The non-personally identifiable information that is automatically transmitted includes your browser type, Internet service provider, information about the general content of the site or page displayed on your browser and other non-personally identifiable information provided by the site.

	Before Opting Out	After Opting Out
Cookie Value	Unique, e.g., **id=** 8000002cd6f0880	Generic, **id** = OPT_OUT
Targeting Criteria	**Cookie-derived information:** • Ad frequency limitation • Ad sequencing • User list	Not Applicable
	Ad Tag information: • Site name • Web page • Key values	**Ad Tag information:** • Site name • Web page • Key values
	Header fields information: • Operating System type • Windows version • User's local time • Location information from IP address	**Header fields information:** • Operating System type • Windows version • User's local time • Location information from IP address
Will You Still See Ads?	Yes	Yes

Online Profiling – Microsoft on the Google / DoubleClick merger

"By acquiring the dominant provider of ad-serving tools that publishers use to manage and make their inventory available to advertisers, Google will force other online ad networks to build and market their own ad-serving tools. Unless and until Google's competitors are able to obtain access to competitively neutral and unbiased ad-serving tools like those currently provided by DoubleClick, the ability of Google's rivals to create viable alternative pipelines will be very difficult, if possible at all. Moreover, by the time competitors are able to assemble their own pipelines, given the network economics that characterize online advertising, Google likely will have obtained in non-search advertising the same unbeatable market position that it now enjoys in search advertising."



Online Privacy Policies

- Uses and Abuses
  - Conscious failure to honor
  - Inadvertent disclosure when privacy policy says information is securely held
  - Customer list and associated PII as asset in bankruptcy
  - Other questions about disclosure: related entities
  - Modifying a privacy policy
- State Law Requirements to Post
  - California example

Security Breaches

- In re BJ's Wholesale Club, Inc (FTC, 2005)
  - Failure to encrypt in-transit or when stored in-store
  - Information stored in files accessible via default user id and password
  - Failure to use readily available wireless access point security measures
  - Insufficient security investigations and detection of unauthorized access
  - Storage of information locally longer than needed
- Security Breach Notification Legislation

Piercing Online Anonymity – Columbia Ins. v. Seescandy.com (ND Cal.1999)

- Suits for purpose of unmasking a critic?
- Subpoena compliance by ISP with or without notice to holder of pseudonym?

- Columbia (TM assignee w/ license back to candy manufacturer) sues D for TM infringement
- Issue whether to allow discovery to find identity
  - Good faith exhaustion of traditional avenues to identify a D pre-service
  - Prevent use of identity discovery to harass or intimidate
  - Limiting principles
    - Specificity for court to know entity or person who can be sued in Federal court
    - Describe all previous steps taken to identify
    - Show suit can withstand motion to dismiss
    - File discovery request

Piercing Online Anonymity

- Other standards for pre-service discovery:
  - good faith
  - prima facie (4 elements, 4th is balancing)
  - withstand S/J (notice requirement, including on same online facility)
- Virginia regulation of subpoenas to discover online speakers' identity
- Anonymous third-party witness
  - More stringent standard

Models for Privacy

- Self Regulation
  - Inherently raises the question of technological tools to express privacy preferences
  - As a response to the threat of government regulation
- 3rd Party Certification
- Technological Tools
  - Email encryption
  - Anonymous surfing
  - Banner ad / popup blocking
  - Cookie managers
  - File encryption
  - Anonymous remailers
  - Hard drive erasers
  - Firewalls
  - Spam filters
  - Spyware detectors
- P3P

Models for Privacy - More on P3P . . .

- W3C P3P 1.0 Spec
  - The Platform for Privacy Preferences 1.0 (P3P1.0) Specification
- Website operators incentives to adhere to the standard
- Users browsing habits and inclination to "tune" browser settings for heightened privacy

The Platform for Privacy Preferences Project (P3P) enables Web sites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents. P3P user agents will allow users to be informed of site practices (in both machine- and human-readable formats) and to automate decision-making based on these practices when appropriate. Thus users need not read the privacy policies at every site they visit.

Although P3P provides a technical mechanism for ensuring that users can be informed about privacy policies before they release personal information, it does not provide a technical mechanism for making sure sites act according to their policies. Products implementing this specification MAY provide some assistance in that regard, but that is up to specific implementations and outside the scope of this specification. However, P3P is complementary to laws and self-regulatory programs that can provide enforcement mechanisms. In addition, P3P does not include mechanisms for transferring data or for securing personal data in transit or storage. P3P may be built into tools designed to facilitate data transfer. These tools should include appropriate security safeguards.

Models for Privacy - More on P3P . . .

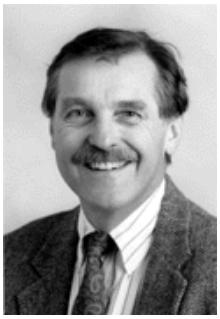
The EC Directive

- Directive (what's a Directive? Transposition?)
  - Limits on "processing" "personal data"
    - Applies to non-automatic processing when part of a "filing system" (accessible by criteria)
  - "data controller" is one w/ a role in determining purposes and means of processing
- Various limits on the data controller
  - What collected, how maintained, quantity not excessive, integrity, identifiable on as long as necessary
  - Consent, w/ 5 exceptions, direct marketing right to object
  - No processing of sensitive personal data, w/ 6 exceptions, limited anti-automatic-characterizing right
  - Disclosures to the data subject about the data controller
  - Right to regular reports (3 elements) on data processing and right to correct inaccurate data
  - Assure confidentiality and security
  - Notify national supervisory authority before automatic processing of data, including whether any data transferred to non-EU countries; the authority must examine for operations "likely to present specific risks to the rights and freedoms of data subjects"
  - Limits on transfer outside EU, third country must have "adequate level of protection", w/ 6 exceptions or with adequate safeguards imposed by data controller on recipient in third country

U.S. Safe Harbor

- Notice
- Choice
  - Opt-out must be available, opt-in for sensitive if to be disclosed to third-parties or uses for other purposes
- Onward Transfer – obligate receiver
- Security
- Data Integrity
  - Relevant for purposes; reliable, accurate, current
- Access
- Enforcement

Privacy Commodified? - Laudon



- Problem is that the "property right" is in the wrong place
- Put it with the individual to whom the information refers
  - Then, the price won't be "too low"
- Otherwise, market is "dominated by privacy-invading institutions"
- Inefficient market in information has "coping" costs
  - Junk mail
  - Attention spreading
  - Loss of "serenity, privacy and solitude"

Responses to Laudon

- Litman
  - Pervasive clicking on “I accept” always transfers the information as alienable personal property to the web site / aggregator
  - Value of privacy is underestimated until needed
  - The after-market in personal data is the problem; property rights in the personal data will only legitimize the problem

- Radin
  - If information privacy is more like a human right, inalienable, and then non-waivable and non-transferable; a tort against personal integrity
  - Similar to other consumer issues in offline world