

Unless otherwise noted, the content of this course material is licensed under a Creative Commons BY-SA 3.0 License.

<http://creativecommons.org/licenses/by-sa/3.0/>

Copyright © 2009, Robert Frost.

You assume all responsibility for use and potential liability associated with any use of the material. Material contains copyrighted content, used in accordance with U.S. law. Copyright holders of content included in this material should contact [open.michigan@umich.edu](mailto:open.michigan@umich.edu) with any questions, corrections, or clarifications regarding the use of content. The Regents of the University of Michigan do not license the use of third party content posted to this site unless such a license is specifically granted in connection with particular content. Users of content are responsible for their compliance with applicable law. Mention of specific products in this material solely represents the opinion of the speaker and does not represent an endorsement by the University of Michigan. For more information about how to cite these materials visit <http://michigan.educommons.net/about/terms-of-use>.

Any medical information in this material is intended to inform and educate and is not a tool for self-diagnosis or a replacement for medical evaluation, advice, diagnosis or treatment by a healthcare professional. You should speak to your physician or make an appointment to be seen if you have questions or concerns about this information or your medical condition. Viewer discretion is advised: Material may contain medical images that may be disturbing to some viewers.

# Privacy in the Age of Digits

- Historical roots to notion of privacy
  - The state vs. “the people” (notice the modern terminology) in the British Empire, 1640-1780
  - Traditionally based in security of one’s goods and property—negative notion of freedom; need a more positive notion of constitutive public space built on private individuals, as in Europe
  - Fourth Amendment protects against “unreasonable search and seizure”: there is no prima facie “right to privacy”
  - Warrants and judicial review as early protections in the US

# Infections to the Notion of Privacy

- Should corporations as “legal persons” be protected by the same privacy rights as “real persons”? *Santa Clara County v. Southern Pacific RR*, 1886...
- Corporations have a right to privacy but, on the flip side, cannot be punished
- Again, issues of accountability
- Libertarian notion: “...the right to be left alone,” Judge Thomas M. Cooley, *MI Supreme Court* (1880), Lewis D. Brandeis, *US Supreme Court* (1929): a thin foundation...
- This leaves public space uninhabited
- Need a positive, constitutive notion of privacy, as constructive

# A Contemporary Interpretation of Privacy

- Fourth Amendment litigation since 1960
  - Griswold v. Connecticut, 1964: Sex information as “private,” restriction on its diffusion as invasion of privacy
  - Roe v. Wade, 1973: The privacy of reproductive choice decisions
  - Lawrence v. Texas, 2003; overturned Bowers v. Hardwick, 1986: privacy of choices about sexual orientation
  - 2003: MA Court on gay marriage: combo of privacy and equal protection
  - 2005: Alito SCOTUS nomination key issue: “is there a constitutional right to privacy?” Very controversial.
- 1960s rise of databanks, Alan Westin’s work and more— new notion of “constructive” dangers to privacy
  - *Privacy and Freedom* (1967) and *Databanks in a Free Society* (1972);  
Simson Garfinkel, *Database Nation* (2000)



# Westin and Privacy, 1970 and after

- Emerging recognition of power of database linking: privacy can be violated (by the state) constructively by record-matching, data mining, and “business intelligence” or semantic matching techniques
- Data-doubles as affordances for privacy invasions
  - What “data crumbs” do we leave behind in everyday life?
  - Can our data doubles be detached from us and used against us?
  - Identity thefts and identity “spoofing”
- Result: first wave of data-integrity and privacy legislation at Federal and State levels, esp. Privacy Act of 1974
  - Note delicate balancing of privacy against FOIA (1966): a public “right to know” vs. personal privacy

# Barriers to Privacy Incursions by Business

- [caveat: journalism and “public personalities” excluded]
- Financial Records
  - Fair Credit Reporting Act (1971) & later amendments: right to review; context of credit reporting services; revisions now in Congress, thanks in part to ChoicePoint leakages
- Medical records
  - Danger of diffusion of private information to third parties (Eagleton imbroglio, 1972)
  - Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)
  - A rare instance of “opt-in” approach in the US, as different from Europe, where “opt-in” is usually the rule, especially under the EU’s Privacy Directives
- Problem: few protections against data sales to 3rd parties— it’s a “free market”!

# Current Business Practices that Impinge on Right to Privacy

- Data mining/harvesting and records linkage
  - “Constructive” invasions by assembling disparate data
  - EFTs, automatic payments; information on consumer purchases
  - Insurance records, job applications, [some] health records
  - Marketing surveys
  - Data resales
- “Spam” and junk mail
  - Are these privacy invasions or mere annoyances?
  - Can we put a cost incurred by consumers on these practices, then charge-back to the culprits?
  - Larger issue: if attention is a major personal asset in the information society, when businesses grab our attention, are they stealing from us?

# Marketers' Invasions

- Sociologists meet marketers: using census data for Zip Codes and census tracts
- The market for customer lists; data resales
  - Direct Marketing Association and friends
  - Where does “marketing info” end and privacy invasions begin?
  - Should we consider privacy a right that can be licensed out or, if it is violated, should we be able to collect fees?
- Emergence of real-time tracking and data harvesting
  - loyalty cards: trade privacy for discounts?
  - “smart” devices tracking shoppers
  - RFIDs replacing UPCs & bar codes: powerful data integration
- “Do Not Call” legislation (2003) and the rise of “opt-out” as the current mode for privacy protections



# The Bad Guys... Solutions?

- Phishing
- Identity theft
- [Industrial espionage]
- Spam, rootkits, zombie machines/hijacking; failure of CAN-SPAM Act
- Will government-mandated “back-doors” (under the PATRIOT Act) be used by the bad guys?
- Overt discrimination when private info is *not* required
- Solution[?]: Pamela Samuelson’s proposal to treat personal data as intellectual property

# Public Perceptions of Privacy Issues

- UCLA Internet use study (11/2001): fears of privacy incursions by business as barrier to Net adoption
  - Data sales: genies out of the bottle?
  - Data integrity: the danger of “false positives”
    - ChoicePoint and other disasters
    - Anti-“terrorist” mistakes--or not(?)
- As noted earlier, vast amounts of data “out there” that can be reassembled
  - Invasive “prof ling”
  - Identity theft
- Note well, however: most identity theft arises from dumpster diving, not IT incursions

# Dilemmas in Locating Responsibility to Preserve Privacy

- Medical and financial records as the key
- Who really invades more, business or the state?
- post-911 sea change: government can invade privacy almost at will in search of “terrorists”
- Should business be allowed to have a similar right to snoop based on notion of preëmptive presumptions about piracy?

# Opt-In vs. Opt-Out

- Recent legislation as “opt-out”
  - Note your recurring Privacy Statements from banks
  - A consequence of failure of earlier self-regulation via “privacy policies”: “opt-out” links are often used to validate email addresses
  - Spotty record of business’ self-regulation
    - failures historically in workplace safety, environment, etc.
    - currently, a widespread ignoring of NAB’s “Code of Conduct” in broadcasting: end of “fairness doctrine” in 1980s
    - late-1990s: widespread recognition that companies violated their own privacy policies, posted on the Web
- Would “opt-in” be more effective?
  - A new market for volunteered information?
  - This would reflect issues of cost-bearing



# Post 9/11 Issues

- USA PATRIOT Act, 2001
  - Not only “preventative detention,” but law allows officials to demand that news of incursions be suppressed
  - Library circulation info; re: PATRIOT Act vs ALA traditions. USAG’s office claims no use of this provision, while ALA has counted dozens.
  - Expanded powers to subpoena almost any records in the interest of “national security”
  - “Back doors” [again], DoJ “letters,” etc.
- We know that racial profiling is unacceptable; what of ethnic profiling after 9/11?
- Recent Supreme Court caveats on expanded snooping and detention powers...

# A “Deep Meaning” to Post-911?

- Intercepting Net communications at ISPs—vast change from old telecommunications practices
  - Old system held telecomm providers harmless for acts of telephone & fax users; now they are subject to contempt of court if they refuse to divulge user info (Verizon issue, 2003):  
<[http://www.eff.org/Cases/RIAA\\_v\\_Verizon/](http://www.eff.org/Cases/RIAA_v_Verizon/)>
  - Ministry of Homeland Security & other agencies can examine ISP logs without warrants
  - Following that practice, RIAA, using DMCA, now subpoenas ISPs
- The new surveillance régime
  - Liberty vs. security (Franklin: those who seek the latter to assure the former deserve neither!)
  - Accountability: requests for info & FOIA requests can put one under surveillance
- TIPs TIA, and other snooping initiatives