CS305 - Social, Ethical, and Legal Implications of Computing

- Spring 2012 -

Andrew P. Black

Slides based on material by Bart Massey and

Warren Harrison

Portland State
UNIVERSITY

What Is Privacy?

[From Wikipedia]

- The ability of an individual or group to seclude themselves or information about themselves
- *Privacy* is related to *anonymity*, but not the same thing
- “Private Information” is inherently special or personally sensitive.
- Privacy is broader than security:
  - includes appropriateness of use

Types of Privacy

- Physical
  - touching
  - seeing
- Informational
  - information about you – what information should be private? can we characterize it?
- Do we have a right to privacy?
- What is the connection to computing?

How has computing and digital technology affected society?

- Digital technology allows us to store, organize and retrieve massive amounts of data
- Digital technology allows anybody to communicate with thousands or millions of people at a time
- Data-mining can “de-anonymize” data

Video Surveillance

- Suppose I'm out on 4th Avenue and I see you doing something *incredibly stupid*.
- I take a video of you with my cell phone, and put it on YouTube.
- Have I violated your privacy?

Video Surveillance

- Suppose I'm out on 4th Avenue and I see you doing something *incredibly stupid and illegal*.
- I take a video of you with my cell phone, and put it on Youtube.
- Have I violated your privacy?

Video Surveillance

- What about this:
  - **Red light runner & crashes:**
    - http://www.youtube.com/watch?v=ZHOD6qIi2c4&feature=related

Video Surveillance

- Hidden Nanny-Cam – what do you think?

Video Surveillance

- Hidden Nanny-Cam – what do you think?
- How about these:
  - **Hidden camera captures Boynton Beach burglary:**
    - http://www.youtube.com/watch?v=KNtTX_VaEzk
  - **NPR Exec Slams Tea Party On Hidden Camera:**
    - http://www.youtube.com/watch?v=Z4qvjyz7o5g

What Does the Law Say About Sound and Video Recording?

- Oregon Revised Statutes
  - http://www.leg.state.or.us/ors/
- Videotaping:
  - 163.700 Invasion of personal privacy.
- In theatres:
  - 164.882 Unlawful operation of an audiovisual device.
- Telecommunications:
  - 165.540 Obtaining contents of communications.
- The Photographer's Right
  - http://www.krages.com/ThePhotographersRight.pdf

Data Privacy

- Public record
- Public information
- Personal information
- Disclosing Information [by you]
  - statutory disclosure
  - voluntary disclosure
  - involuntary disclosure

Major Personal Info Databases

- Credit Reporting Services [what is it used for?]
  - Equifax
  - Experian
  - TransUnion
- National Crime Information Center (NCIC)
- Department of Motor Vehicles (State)
- Internal Revenue Service (Federal/State)

What is Personal Information?

- Text says “information that is not public information or part of a public record”
- What about information about *you*, known by *others*?
- Who has the right to control information about a multi-party event?
  - You tell me your birthday
  - I see you on the corner of 82nd and Foster
  - I get a letter from you with your return address
  - You post your favorite movies on Facebook

Private vs. Governmental Data Access

Fourth Amendment

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Restrictions on Government Access to Personal Property

- In general, need a warrant [*probable cause*]
- Exceptions
  - voluntary disclosure [scope of consent]
  - plain view
  - behavior inconsistent with a reasonable expectation of privacy
  - third party possession/searches/permission
  - abandonment
  - implied consent
  - exigent circumstances
  - search incident to arrest/inventory searches
  - border searches
  - workplace searches [complicated]

Information Owned by Third Parties

- 4th Amendment protects only those items under your control — it doesn't cover records about *you* maintained by *someone else*.
  - banking information
  - telephone records
  - credit card purchases
  - e-mail on a server
- no reasonable expectation of privacy in US
- can subpoena third party materials …

Electronic Communications Privacy Act (ECPA)

- Law since 1986
- When the government seeks stored e-mail, account records or subscriber information, they must comply with the ECPA.
- Statutory privacy rights for customers of computer network service providers.
- Distinguishes among communications held by providers of electronic communication services [ECS] when the communications are being held in electronic storage, and communications held by providers of remote computing services [RCS]

Provider of Electronic Communication Services

- provide ability to send or receive the electronic communications in question – *public or private*
- *electronic storage* – narrow definition: "any temporary/intermediate storage of an electronic communication incidental to transmission" – *i.e.*, copy of communication that is intended to be sent on to a final destination
  - e-mail received by service provider but not yet accessed by recipient – in electronic storage
  - e-mail accessed by recipient and saved in inbox – not in electronic storage

Provider of Remote Computing Services

- provided by an off-site computer that stores or processes data for a customer
- does not hold customer files on their way to a final intended destination – they are stored or processed by the provider for the convenience of the subscriber
- must be "available to the public" – *i.e.*, must be available to anyone willing to pay

Types of Information
Basic Subscriber Information

- identity of subscriber
  - name/address
- relationship with the service provider
  - length of service, type of service, subscriber number
- basic session connection records
  - local/long distance telephone connection records
- *Patriot Act* added:
  - records of session times/durations
  - dynamic IP addresses
  - originating phone number for dial-up or IP address
  - means and source of payment

Types of Information
Contents

- any information concerning the substance, purport or meaning of a communication
  - e-mail message, voice mail message, word processing files
- contents held by …
  - providers of electronic communication services
  - providers of remote computing services
  - neither

Types of Information
Records pertaining to customers

- record or other information pertaining to a subscriber that is not *Basic Subscriber Information* and not *Content*
  - logs
  - cell-site data
  - e-mail addresses with whom subscriber has corresponded

ECPA Restrictions

- Providers of services available to the public are restricted in terms of *voluntary disclosure*
  - forbid disclosure of contents to 3rd party
  - forbid disclosure of other records to government
- Subpoena for
  - basic subscriber information
  - any information outside the scope of the ECPA (e.g., provider is neither an ECS or an RCS)
- Subpoena with prior notice
  - content in electronic storage > 180 days
  - contents maintained by an RCS (i.e., opened e-mail, word processing files)
  - notice may be delayed up to 90 days with cause
- Threshold for obtaining a subpoena is low

Compelled Disclosure

- Subpoena for
  - basic subscriber information
  - any information outside the scope of the ECPA (e.g., provider is neither an ECS or an RCS)
- Subpoena with prior notice
  - content in electronic storage > 180 days
  - contents maintained by an RCS (i.e., opened e-mail, word processing files)
  - notice may be delayed up to 90 days with cause
- 2703(d) order – requires specific, articulable facts that information is relevant to an ongoing criminal investigation
  - account logs and transaction records
- 2703(d) order with prior notice
  - everything except unopened e-mail less than 180 days old
- Warrant served on provider for everything else

Oregon Computer Crime 164.377

(2) Any person commits computer crime who knowingly accesses, attempts to access or uses, or attempts to use, any computer, computer system, computer network or any part thereof for the purpose of:

(a) Devising or executing any scheme or artifice to defraud;

(b) Obtaining money, property or services by means of false or fraudulent pretenses, representations or promises; or

(c) Committing theft, including, but not limited to, theft of proprietary information.

(3) Any person who knowingly and without authorization alters, damages or destroys any computer, computer system, computer network, or any computer software, program, documentation or data contained in such computer, computer system or computer network, commits computer crime.

(4) Any person who knowingly and without authorization uses, accesses or attempts to access any computer, computer system, computer network, or any computer software, program, documentation or data contained in such computer, computer system or computer network, commits computer crime.

Other Crimes Involving Computing

- Stalking: ORS 163.730
- Forgery: ORS 165.002
- Fraudulent Communications Device: ORS 165.070
- Identity Theft: ORS 165.800
- Harassment: ORS 166.065
- Online Sexual Corruption of a Child: ORS 163.431
- Theft of Services: ORS 164.125 [see 164.035]