CPSC156: The Internet Co-Evolution of Technology and Society

Lecture 14: March 6, 2007

Further Reflections on Sensitive Information

Retail Shopping on the Internet

- Consumer can complete the purchase
  - Without leaving his home
  - Without having to face or talk to another person
- Each purchase leaves a trail of electronic evidence
  - Retailer logs the transaction both for order fulfillment and for customer profiling.
  - Retailer sends the transaction data to other organizations in order to complete the transaction (credit card, shipper, warehouse, factory, *etc.*).
  - Retailer gives or sells these transaction data to business partners and others.
  - Retailer and advertisers put cookies on consumers' machines.
  - Internet traffic is carried by many routers owned by many ISPs.

Retail Shopping in a B&M Store

- Consumer can make the purchase
  - In a store that he has never been to before, where he is unlikely to know anyone.
  - With cash (and not have to identify himself).
- But he may leave a trail of evidence anyway.
  - There may be a surveillance camera in the store.
  - Someone in the store may recognize him, even if he's never been there before and doesn't recognize the observer.
  - A check-out clerk or inventory system may record the purchase, particularly if he buys an unusual item.

Discussion Point:
Which Scenario is More Private?

- Bottom line: Neither is private!

  “You have no privacy. Get over it.”
  - Scott McNeely, SUN Microsystems CEO

- However, the B&M-store purchase with cash is, at this time, more likely not to create a searchable, linkable, profilable record.

“Public Records” in the Internet Age

Depending on State and Federal law, “public records” can include:

- Birth, death, marriage, and divorce records
- Court documents and arrest warrants (including those of people who were acquitted)
- Property ownership and tax-compliance records
- Driver’s license information
- Occupational certification

They are, by definition, “open to inspection by any person.”

How “Public” are They?

Traditionally: Many public records were “practically obscure.”

- Stored at the local level on hard-to-search media, *e.g.*, paper, microfiche, or offline computer disks.
- Not often accurately and usefully indexed.

Now: More and more public records, especially Federal records, are being put on public web pages in standard, searchable formats.

What are “Public Records” Used For?

In addition to straightforward, known uses (such as credential checks by employers and title searches by home buyers), they’re used for:

- Commercial profiling and marketing
- Dossier compilation
- Identity theft and “pretexting”
- Private investigation

Discussion point: Will “reinventing oneself” and “social forgiveness” be things of the past?

Do We Need a More Nuanced Approach?

Can we distinguish among

- Private information
  - Only the "data subject" has a right to it.
  - ? Example: Legal activity in a private home.
- Public information
  - Everyone has a right to it.
  - ? Example: Government contracts with businesses
- Nonpublic personal information
  - Only parties with a legitimate reason to use it have a right to it.
  - Example: Certain financial information (see, *e.g.*, the Graham-Leach-Bliley Act)

<u>Discussion point</u>: Should some Internet-accessible "public records" be only conditionally accessible? Should data subjects have more control?

Further Reading on These and Related Topics

EPIC's material on

- Public records:
  www.epic.org/privacy/publicrecords/
- Spam:
  www.epic.org/privacy/junk_mail/spam/
- Profiling:
  www.epic.org/privacy/profiling/

FTC information on Graham-Leach-Bliley:
www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.htm

Identification Infrastructure Today I

- We are often asked to “present gov’t-issued photo ID.”
  - Airports
  - Buildings
  - Some high-value financial transactions
- Many gov’t-issued photo IDs are easily forgeable.
  - Drivers’ licenses
  - Passports
- We are often asked to provide personally identifying information (PII).
  - Social security number
  - Mother’s maiden name
  - Date of birth
- Many people and organizations have access to this PII.

Identification Infrastructure Today II

- Security of “foundation documents” (*e.g.*, birth certificates) is terrible.
- According to the US Department of Justice, the rate of identity theft is growing faster than that of any other crime in the United States.
- Existing technology could improve, if not perfect, ID security, *e.g.*:
  - Biometrics
  - Cryptographic authentication
- There is extensive research interest in improving this technology (and the *systems* that support it).

Are Standard, Secure ID Systems Desirable?

+ Ordinary people could benefit from accurate, efficient identification, and identity thieves would have a harder time.
- Multi-purpose, electronic IDs facilitate tracking, linking, dossier compilation, and all of the other problems currently facilitated by Internet-accessible "public records."
- Multi-purpose, standard "secure" IDs magnify the importance of errors in ID systems.

Possible Approaches

- Build secure ID systems that *don't* facilitate linking and tracking.
  - Tracking a "targeted" person should require a court-ordered key.
  - Tracking someone for whom one doesn't have such a key should be provably infeasible.
  - There's already a plausible start on this in the security-theory literature.
- Organizations could "seize the high ground" by not retaining usage data for identification and authorization tokens (*a fortiori* not mining, selling, or linking it).
  - At least one ID start-up company is making this claim.
  - How can such a claim be proven?
  - Security theory does not address this question (yet!).

What May We Use To Prevent Unwanted Phone Calls?

+ Technology
  - Answering machines
  - Caller ID
+ Money (together with technology)
  - “Privacy-guard service” from SNET

? Government

  - “Do-Not-Call” lists seem to be controversial.

What May We Use To Prevent Unwanted Email?

+ Technology
  - Filters
  - CAPTCHAs
  - “Computational postage”

? Government
  + Yes, if the unwanted email is “trespass to chattel,” which requires that it “harm” the recipient’s computer system. (CyberPromotions)
  – No, if the email is merely “unwanted.” (Hamidi)

Is a Network like a Country?

- Size, diversity, and universal connectivity imply risk. Get over it!
- Subnetworks ≈ neighborhoods (J Yeh, CS457)
  - Some segregation happens naturally.
  - Gov't-sanctioned segregation is wrong.
- Alternative: Network nodes ≈ homes (JF)
  - A man's computer is his castle.
  - Do I have to be rich or tech-savvy to deserve control over my own computer?