

CPSC156a: The Internet Co-Evolution of Technology and Society

Lecture 18: November 11, 2003

**Further Reflections on
Privacy and Control**

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)

Discussion point: 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/online/pubs/buspubs/glbshort.htm