Privacy in an Always-Online World

Ben Adida
ben@mit.edu

13 July 2006
No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence

[...]

Everyone has the right to the protection of the law against such interference.

Article 12,
Universal Declaration of Human Rights,
United Nations.
This Talk

8 Simple Points about Privacy
Point #1

identifying a person is easy.
Ben Adida
ben@mit.edu
MIT ID
572-23-0305
SSN
942-83-2467
02118
Male
11/05/1976

87% of the population is uniquely identified
[Sweeney, CMU, 2000-2001]
ACGCTTAATCTCTAGGAGGTATG

20 randomly selected SNPs in a genome record form a unique identifier
BR Boot Cut Blue Jeans
CK Grey Dress Shirt
KC Dark Brown Shoes
Skaden Blue/Silver Watch
Timbuk2 Laptop Bag

enough to identify me
enough to identify me
Point #2

online applications are radically altering the state of privacy.
Consequences

How to Clean Up Your Digital Dirt

By JARED FLESHER

Unflattering personal information drifting around the Internet, known by some as "digital dirt," can doom a job search before it even gets started. Job hunters should know that recruiters can, and often do, read much of what's posted about them on the Web.

Auto club fires 27 in message board crackdown

SAN DIEGO, Calif. (AP) — A California automobile club has fired 27 workers for posting messages on a popular social networking Web site.

Feds after Google data

RECORDS SOUGHT IN U.S. QUEST TO REVIVE PORN LAW

By Howard Mintz
Mercury News
The New Reality

• What you do when you’re 15 will haunt you forever.  
  maybe it will haunt everyone equally?

• “Your Data” on Google is not as private as “Your Data” on your hard drive.  
  maybe this will change?
Point #3

bridging the physical and digital significantly impacts on privacy.
Identification and tracking of persons using RFID-tagged items

Abstract

A method and system for identifying and tracking persons using RFID-tagged items carried on the persons. Previous purchase records for each person who shops at a retail store are collected by POS terminals and stored in a transaction database. When a person carrying or wearing items having RFID tags enters the store or other designated area, a RFID tag scanner located therein scans the RFID tags on that person and reads the RFID tag information. The RFID tag information collected from the person is correlated with transaction records stored in the transaction database according to known correlation algorithms. Based on the results of the correlation, the exact identity of the person or certain characteristics about the person can be determined. This information is used to monitor the movement of the person through the store or other areas.
What’s Troubling

• Surreptitious data collection
• Unintuitive power of correlation
• What is the benefit?
Point #4

personal data is provided in exchange for some benefit.
Passwords revealed by sweet deal

More than 70% of people would reveal their computer password in exchange for a bar of chocolate, a survey has found.
So what’s on the horizon?
Point #5

identity infrastructures will impact privacy.
Identity Infrastructures

• Microsoft CardSpace, Liberty Alliance OpenID, LID, etc...

• Give user control over their online identity

• Provide a standardized UI for authentication and the exchange of personal information

• Make the user aware of the private data transaction.
Point #6

technology can help but policy is also required.
Technology

• Secure delegation
certificate from a third party enables offline authentication.

• Minimized data reveal
  “I’m over 21” doesn’t reveal my age.

• Unlinkability
  two authentications aren’t necessarily linked.
Technology can’t....

- prevent RFID from being read
  *they’re made to be read cheaply*
- obscure your face or license plate
- anonymize every transaction
  *recall the numerous means of identification*
Policy!

- Significant differences throughout the world
  - *Europe*: individual control over data
  - *US*: mostly contract law
- Can mandate an auditing process
- Can mandate a transparency of the audit
Policy supported by Technology

- TAMI research group at MIT
  
  *Transparent Accountable Datamining Initiative*

- “trace” information access in protected databases

- enforced by Trusted Platform Module?
  
  *same technology as that deployed for DRM*

- works when there is an “enforcement” checkpoint
Point #7

privacy and security are different but connected.
Veterans' data swiped in theft

By Greg Sandoval
Staff Writer, CNET News.com
Published: May 22, 2006, 2:50 PM PDT

Credit Bureau Reports Data Loss

(June 20, 2006)–A possible identity theft scare is hitting close to home at one of the nation’s big credit bureaus.

A little more than half of the workers at Equifax could be affected by the theft of a company laptop containing employee names and Social Security numbers.

Citigroup’s Lost Tapes Cast Spotlight On Data Security

Banks are considering a variety of measures to tighten the security for customer information.

By Steven Marlin
InformationWeek
Jun 7, 2005 02:00 PM
Point #8

privacy will depend on incentives and transparency.
• **Economic Incentives**
  *Businesses will carry the burden of identity theft. Thus, businesses should value privacy.*

• **Transparency to the User**
  *Standardizing the authentication process provides an opportunity to educate and empower the user.*
In Summary

1. identifying a person is easy
2. online applications are radically altering the state of privacy.
3. bridging the physical and digital significantly impacts on privacy.
4. personal data is provided in exchange for some benefit.
5. identity infrastructures will impact privacy.
6. technology can help but policy is also required.
7. privacy and security are different but connected.
8. privacy will depend on incentives and transparency.
Questions?