Technologies for Privacy

Latanya Sweeney
with contributions from
Raj Reddy, Norman Sadeh, Michael Shamos
School of Computer Science
Carnegie Mellon University

July 31, 2003

Problem Addressed in this Talk

The emergence of many new technologies becomes increasingly hampered by privacy concerns because these technologies leave society vulnerable to privacy abuses.

Current situation.
Let society choose between benefiting from the technology and maintaining privacy protections.

Our solution.
Privacy Technology Center will proactively construct privacy technology that address growing privacy concerns in emerging technologies, thereby enabling both research on and adoption of emerging technologies by assuring compliance to social and legal norms.

Privacy Technology Center
Core People

Anastassia Ailamaki
Chris Atkeson
Guy Blelloch
Manuel Blum
Jamie Callan
Jamie Carbonell
Kathleen Carley
Robert Collins
Lorrie Cranor
Samuel Edoho-Eket
Maxine Eskenazi
Scott Fahlman

David Farber
David Garlan
Ralph Gross
Alex Hauptmann
Takeo Kanade
Bradley Malin
Bruce Maggs
Tom Mitchell
Norman Sadeh
William Scherlis
Jeff Schneider
Henry Schneiderman

Michael Shamos
Mel Siegel
Daniel Siewiorek
Asim Smailagic
Peter Steenkiste
Scott Stevens
Latanya Sweeney
Katia Sycara
Robert Thibedeau
Howard Wactlar
Alex Waibel

Upcoming Workshops

Researchers and Privacy Advocates
Examine Emerging Technologies
Tentative: October 7-8, 2003, at Carnegie Mellon

Congressional Briefing
on Privacy and Emerging Technologies
Tentative: November 19, 2003, Senate Office Building, DC

Emerging Technologies with Privacy Concerns

1. Face recognition, Biometrics (DNA, fingerprints, iris, gait)
2. Video Surveillance, Ubiquitous Networks (Sensors)
3. Semantic Web, Data Mining, Bio-Terrorism Surveillance
4. Professional Assistants (email and scheduling), Lifelog recording
5. E911 Cell Phones, IR Tags, GPS
6. Personal Robots, Intelligent Spaces, CareMedia
7. Peer to peer Sharing, Spam Blockers, Instant Messaging
8. Tutoring Systems, Classroom Recording, Cheating Detectors
9. DNA sequences, Genomic data, Pharmaco-genomics

Some Privacy Technology Solutions

- Face de-identification
- Self-controlling data
- Video abstraction
- CertBox (“privacy appliance”)
- Reasonable cause (“selective revelation”)
- Distributed surveillance
- Privacy and context awareness (“eWallet”)
- Data valuation by simulation
- Roster collocation networks
- Video and sound opt-out
- Text anonymizer
- Privacy agent
- Blocking devices
- Point location query restriction

Human Recognition and Identification Benefits and Concerns

1. Face recognition, Biometrics (DNA, fingerprints, iris, gait)

Benefits:

- Face recognition: Criminal identification in public spaces
- Biometric authentication: Improved safety at work, school and home

Privacy concerns:

- Tracking identified, innocent people through daily life.
- Face recognition software is not accurate.
- Consequences of recognizing the wrong person

Human Recognition and Identification Some Technology Solutions

1. Face recognition, Biometrics (DNA, fingerprints, iris, gait)

- Face de-identification

Face de-identification provides a mechanism for controlling the ability to track individuals without due process.

- Self-controlling data

Self-controlling data provides a mechanism for limiting the secondary use of biometric data.

Ubiquitous Video
Benefits and Concerns

2. Video Surveillance, Ubiquitous Networks (Sensors)

Benefits:

- Crime detection
- Monitoring traffic flow and pedestrian congestion; compiling consumer demographics in shopping malls; logging routine maintenance tasks at nuclear facilities.
- Mobile communication using laptops.

Privacy concerns:

- Capturing intimacy and personal communications
- Tracking unidentified people, automobiles without consent
- Capturing unidentified people, who are exhibiting no suspicious behavior, but who may be subsequently identified

Ubiquitous Video
Some Technology Solutions

2. Video Surveillance, Ubiquitous Networks (Sensors)

- Video abstraction

(a) Video Footprinter -- people replaced with trails

(b) Video Blobber – faces covered

(c) Video Counting and Reporting Behaviors

Ubiquitous Data Sharing Benefits and Concerns

3. Semantic Web, Data Mining, Bio-Terrorism Surveillance

Benefits:

- Counter terrorism surveillance may improve safety.
- Bio-Terrorism surveillance can save lives by early detection of a biological agent and naturally occurring outbreaks.
- Semantic web enables more powerful computer uses

Privacy concerns:

- Erosion of civil liberties
- Illegal search from law-enforcement “mining” cases
- Patient privacy may render healthcare less effective.
- Access to uncontrolled and unprecedented amounts of data
- Collected data can be used for other government

Ubiquitous Data Sharing
Some Technology Solutions

3. Semantic Web, Data Mining, Bio-Terrorism Surveillance

- CertBox ("Privacy Appliance")

  De-identify data sufficient for HIPAA remaining useful for bio-terrorism surveillance

- Reasonable Cause ("Selective Revelation")

  Provide level of de-identification to match need.

- Distributed Surveillance

  Network of data holders compute answers to surveillance questions.

Ubiquitous Data Sharing
Some Technology Solutions

3. Semantic Web, Data Mining, Bio-Terrorism Surveillance

- Semantic Web Technologies to Reconcile Privacy and Context Awareness(“eWallet”)

  Policy specification and enforcement for personal data.

- Data Valuation by Simulation

  Determine usefulness of a data source prior to investing arrangements to get actual data

- Roster Collocation Networks

  Determining collocations of people while protecting privacy.

Information Capturing Tools Benefits and Concerns

4. Professional Assistants (email and scheduling),
Lifelog recording

Benefits:

- Automated clerical assistance
- Intelligent recall of one’s past
- Speech recognition: educating deaf students, reservations
  Medical transcription of clinical notes (and other dictation)

Privacy concerns:

- Reveal sensitive information while communicating
- Not allowing user-defined privacy controls
- Sharing information beyond the control of the user
- Recording others without consent
- Speech recognition: Increased number of wiretaps
  due to reduced effort for transcription.

Information Capturing Tools
Some Technology Solutions

4. Professional Assistants (email and scheduling),
Lifelog recording

- Video (and Sound) Opt-Out

Technical options for others to opt-out of recordings.

- Text Anonymizer

Sufficiently de-identify textual documents to meet legal standards for sharing.

- Privacy Agent

Intelligent privacy guard in automated communications.

Positioning Technology Benefits and Concerns

5. E911 Cell Phones, IR Tags, GPS

Benefits:

- Improved Navigation; Improved Rescue;
- Forgery prevention; Keyless Entry/Security systems
- Improves supply-chain management yielding more affordable goods and services
- Improved consumer safety by more accurate product recall

Privacy concerns:

- Privacy loss due to associations between tag and holder
- Tags on medical products, compromise medical privacy
- GPS data shared without customer control or awareness
- GPS data to enforce virtual speed control when driving

Positioning Technology
Some Technology Solutions

5. E911 Cell Phones, IR Tags, GPS

- Blocking devices

Physical devices to control unwanted reporting.

- Point location query restriction

Answer aggregated queries from a point location database without sharing sensitive location information.

Personal Care
Benefits and Concerns

6. Personal Robots, Intelligent Spaces, CareMedia

Benefits:

- Improved Geriatric Care
- Improved Standard of Living
- Improved Health Care Industry

Privacy concerns:

- Doctor/Patient Confidentiality
- Workplace privacy issues arise for staff
- Bodily privacy issues arise for patients
- Patient’s consent and opt-out of room-wide monitoring
- Information captured on visitors and others
- Captured information shared without consent.

Personal Care
Some Technology Solutions

6. Personal Robots, Intelligent Spaces, CareMedia

Face de-identification

Video Footprinter
Video Blobber
Video Counting and Reporting Behaviors

Video Opt-Out

Semantic Web Technologies to Reconcile Privacy and Context Awareness (eWallet)

Privacy Agent

Problem Addressed in this Talk

The emergence of many new technologies becomes increasingly hampered by privacy concerns because these technologies leave society vulnerable to privacy abuses.

Current situation.
Let society choose between benefiting from the technology and maintaining privacy protections.

Our solution.
Privacy Technology Center will proactively construct privacy technology that address growing privacy concerns in emerging technologies, thereby enabling both research on and adoption of emerging technologies by assuring compliance to social and legal norms.