# Technologies for Privacy

**Latanya Sweeney, Ph.D.**
**School of Computer Science, Carnegie Mellon University**
**http://privacy.cs.cmu.edu/center/index.html**
**August 2003**

## Problem Addressed

The emergence of many new technologies (several of which are DARPA funded) 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.

**Carnegie Mellon solution.**
The Privacy Technology Center will proactively construct privacy technology with provable guarantees of privacy protection while allowing society to collect and share person-specific information for many worthy purposes.

## Core Participants

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

## Leadership

The Privacy Technology Center assumes a leadership role in developing socially-responsible technology, providing policy and legal analyses that examine the effectiveness of these technologies, and to recommend policy accordingly. Our upcoming workshops seek to educate privacy advocates, watch groups, and Congress about solutions that merge technology and policy together.

**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

## Background on Privacy

*Privacy* reflects the ability of a person, organization, government, or entity to control its own space, where the concept of space (or "privacy space") takes on different contexts and is not limited to people.

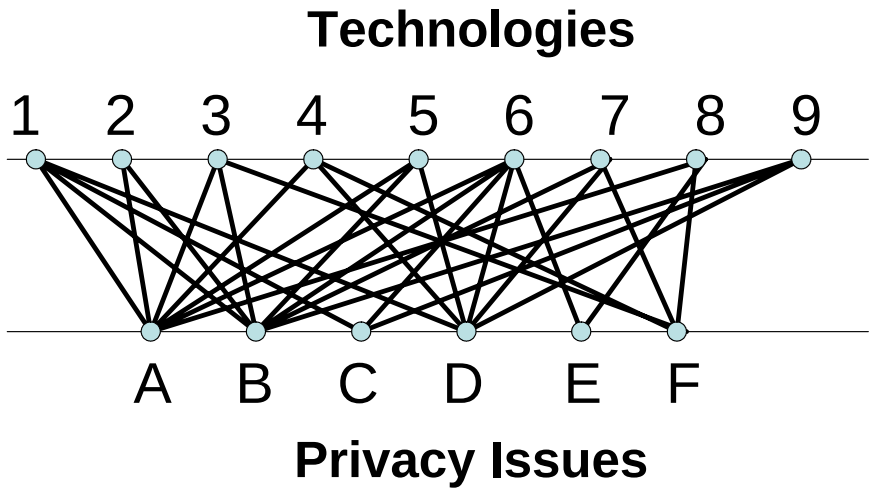
When privacy space refers to the fragments of data one leaves behind as a person (or more generally, an entity) moves through daily life, the notion of privacy is called *data privacy*. Traditional remedies rely on consent and stated policies, but today's technologically-empowered society overtax these solutions. What are needed are provable methods for sufficiently anonymizing data and for specifying and enforcing policies so that data can be shared consistent with societal standards.

## 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 Mobile 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-genetics

## Privacy Issues

- A. Video, wiretapping and surveillance
- B. Civil liberties, illegal search
- C. Medical privacy
- D. Employment, workplace privacy
- E. Educational records privacy
- F. Copyright law




**Emerging technologies (numbers) related to privacy issues (letters). See keys above.**

## Emerging Technologies and Some Proposed Solutions

Below is an overview of the some proposed solutions to privacy issues in emerging technologies.

## Group 1. Human Recognition and Identification

- **Face recognition**
- **Biometrics (DNA, fingerprints, iris, gait)**

### Solutions

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

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

## Group 2. Ubiquitous Video

- **Video Surveillance**
- **Ubiquitous Networks (Sensors)**

### Solutions

**Video abstraction:** Video Footprinter -- people replaced with the trails they leave behind; Video Blobber– faces cryptographically covered in video; Video Counting and Reporting Behaviors

## Group 3. Ubiquitous Data Sharing

- **Semantic Web**
- **Data Mining (person-specific patterns)**
- **Bio-Terrorism Surveillance**

### Solutions

**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.
**Privacy and Context Awareness("eWallet")**: Policy specification and enforcement for data.
**Data Valuation by Simulation:** Determine usefulness of a data source prior to investing arrangements to get actual data
**Roster Collocation Networks:** termining collocations of people while protecting privacy.

## Group 4. Information Capturing Tools

- **Professional Assistants ("RADAR")**
- **Personal Diary ("Lifelog," "Informedia")**
- **Speech recognition**

### Solutions

**Video (and Sound) Opt-Out: T**echnical 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.

## Group 5. Positioning Technology

- **E911 Mobile Phones**
- **IR Tags**
- **GPS**

### Solutions

**Blocking devices:** Physical devices to control unwanted reporting.
**Point location query restriction:** Answer aggregate queries from a point location database without sharing sensitive location information.

## Group 6. Personal Care

- **Personal Robots**
- **Intelligent Spaces**
- **CareMedia**

### Solutions

**Reuse previously described solutions:** Face de-identification, Video Footprinter, Video Blobber, Video Counting and Reporting Behaviors, Video and Sound Opt-Out, Privacy and Context Awareness (eWallet), Privacy Agent