CS 380S

0x1A Great Papers in Computer Security

Vitaly Shmatikov

http://www.cs.utexas.edu/~shmat/courses/cs380s/

H. Nissenbaum

Privacy as Contextual Integrity

(Washington Law Review 2004)

Common-Law Right to Privacy

- Characterized by Samuel Warren and Louis Brandeis (1890)
- "An individual's right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others"

Definitions of Privacy (1)

- "Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves" --Charles Fried
- "Privacy is a limitation of others' access to an individual through information, attention, or physical proximity" --Ruth Gavison
- "Privacy is the right to control information about and access to oneself" -- Priscilla Regan

Definitions of Privacy (2)

- "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extend information about them is communicated to others”
- “...privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve”
  - A. Westin. “Privacy and Freedom” (1967)

Three Guiding Legal Principles

- Protecting privacy of individuals against intrusive government agents
  - 1st, 3rd, 4th, 5th, 9th, 14th amendments, Privacy Act (1974)
- Restricting access to sensitive, personal, or private information
  - FERPA, Right to Financial Privacy Act, Video Privacy Protection Act, HIPAA
- Curtailing intrusions into spaces or spheres deemed private or personal
  - 3rd, 4th amendments

Gray Areas

- Private vs. public space
- USA PATRIOT Act
- "Credit headers"
  - Basic information in a credit report about the person to whom the credit report applies - name, variations of names, current and prior addresses, phone number, date of birth, SSN
- Online privacy in the workplace

Downsides of Three Principles

- Not conditioned on additional dimensions
  - Time, location, etc.
- Privacy based on dichotomies
  - Private – public
  - Sensitive – non-sensitive
  - Government – private

  …

Modern Privacy Threats

- Automated capture of enhanced/large amounts of information
  - RFID tags, EZ Pass, online tracking, video surveillance, DRM, etc.
- Consumer profiling, data mining, aggregation
  - ChoicePoint, Census, credit bureaus, etc.
- Public records online
  - Courts, county clerks, etc.
  - Local vs. global access of data

Contextual Integrity

- Philosophical account of privacy
  - Aims to describe what people care about
- Main idea: every transfer of personal information happens in a certain social context
- Context-dependent norms govern the type of information and the principles of transmission
  - Information is categorized by type
    - Example: personal health information, psychiatric records, ...
    - Rejects public/private dichotomy
  - Principles of transmission depend on context
    - Confidentiality, reciprocity, etc

Cornerstone Norms

- Norms of appropriateness determine what types of information are or are not appropriate for a given context
- Norms of distribution determine the principles governing flow or transfer of information from one party to another
  - Volunteered, inferred, mandated, expected, demanded, etc.
  - Discretion, entitlement, third-party confidentiality, commercial exchange, reciprocal vs. one-way, etc.

Privacy as Contextual Integrity

- Contextual integrity is respected when norms of appropriateness and distribution are respected
- It is violated when any of the norms are infringed

Example: Gramm-Leach-Bliley