Carnegie Mellon University

Privacy Engineering

Examples of System Design Strategy

Prof. Travis Breaux

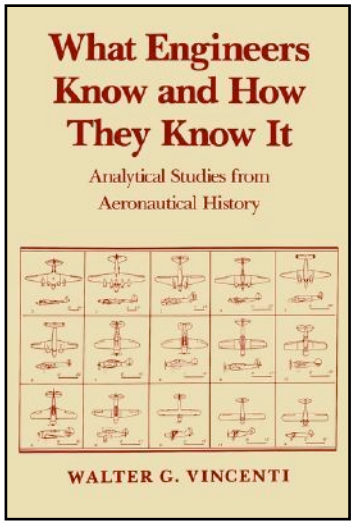
Privacy Engineering Workshop, NIST, Gaithersburg Campus

Wednesday, April 9, 2014

institute for SOFTWARE RESEARCH

Engineering and Design

- Fundamental Design Concepts
  - Define the Operating Principles
  - Define the Normal Configuration
- Criteria and Specifications
  - Translate qualitative goals into quantitative processes
- Theoretical Tools
  - Adapt scientific theory to create tooling for design, construction and evaluation of systems
- Quantitative Data



Walter Vincenti

Aesthetics and Design

Why engineer privacy?

Maximize Data Utility

- Collect everything, value is realized later
- Ensure open access; this drives innovation
- Disclose to leverage third-party value
- Retain as long as practically possible
- Avoid destruction

Balancing utility and risk

Maximize Data Utility

- Collect everything, value is realized later
- Ensure open access; this drives innovation
- Disclose to leverage third-party value
- Retain as long as practically possible
- Avoid destruction

Minimize Privacy Risk

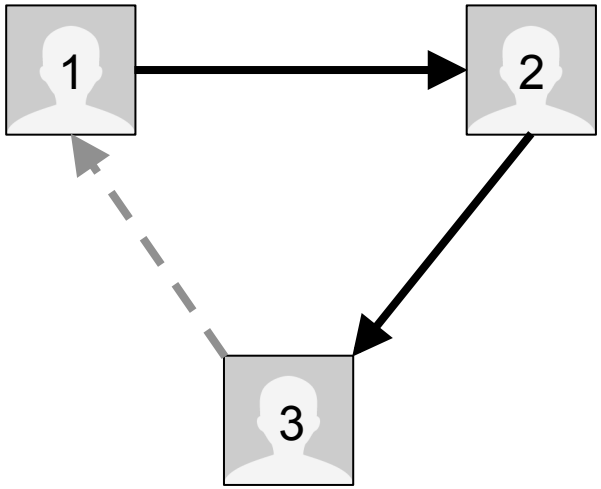
- Limit collection based on stated needs
- Limit access, obtain consent for new uses
- Limit disclosure and third-party uses
- Destroy when no longer needed
- Embrace destruction

Anatomy of Engineering

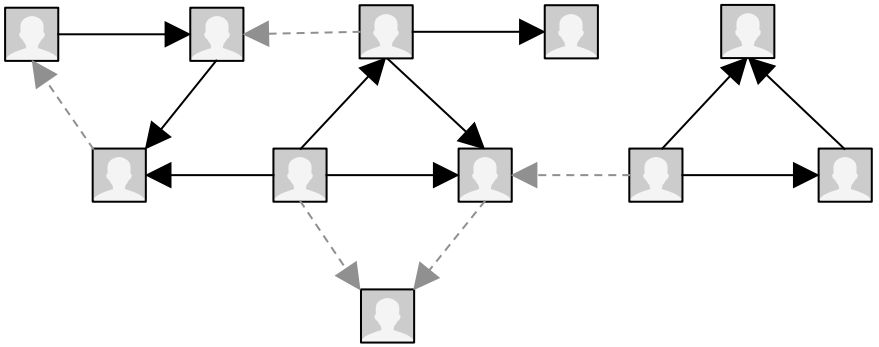
- **Internal logic of problems**: conceptual models of things being controlled and any environmental constraints
- **Internal needs of design**: what quality criteria should be used to satisfy stakeholder needs?
- **Need for decreased uncertainty**: multiple hierarchies of problems that introduce uncertainty
  - Problems in developing tools to discover and apply the scientific theory that drives design
  - Problems in the designs themselves
  - Problems in the environment

Internal logic of problems

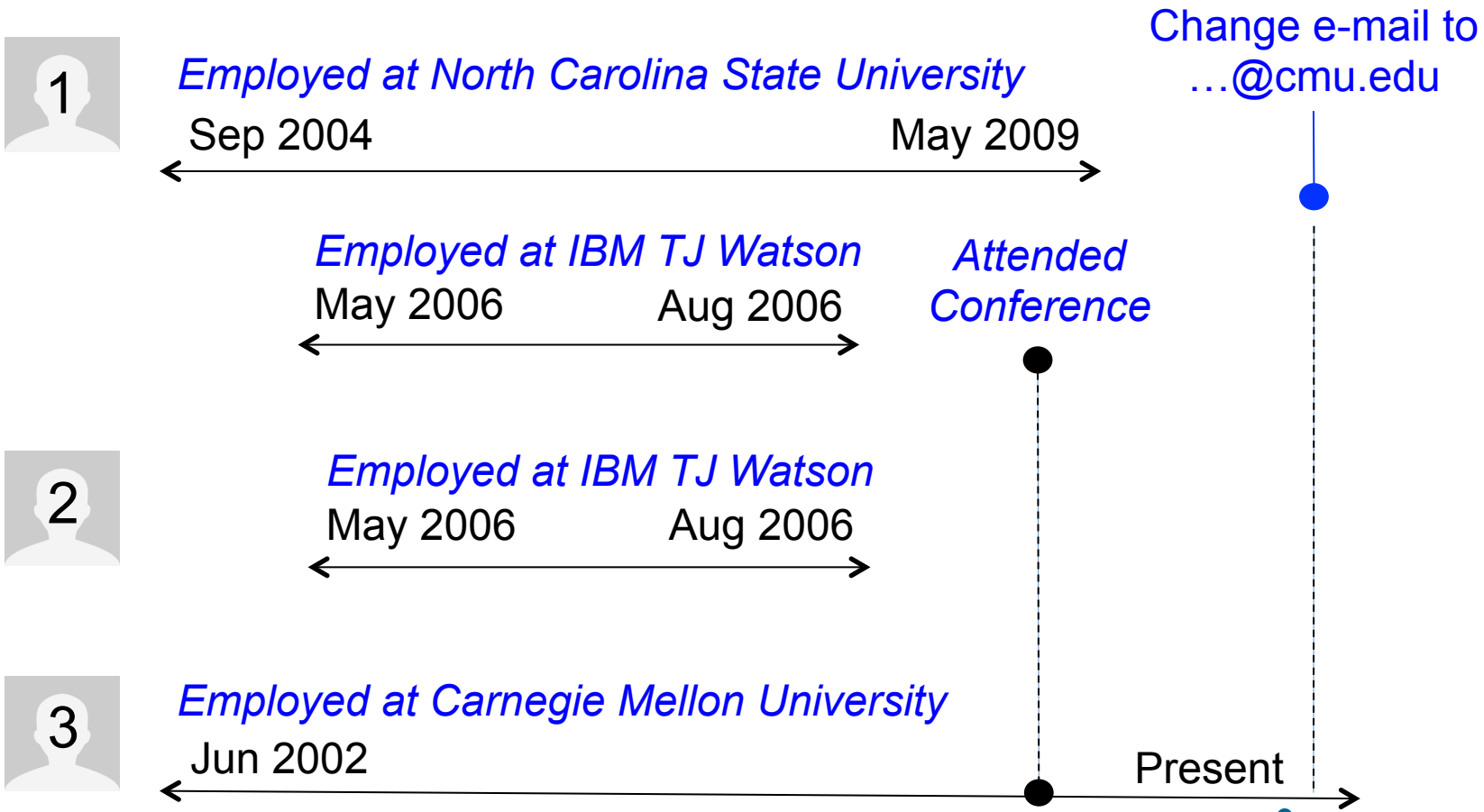
Social networks



- Person 1 knows person 2
- Person 2 knows person 3
- Does person 1 know person 3?
- What do we mean by “know”?



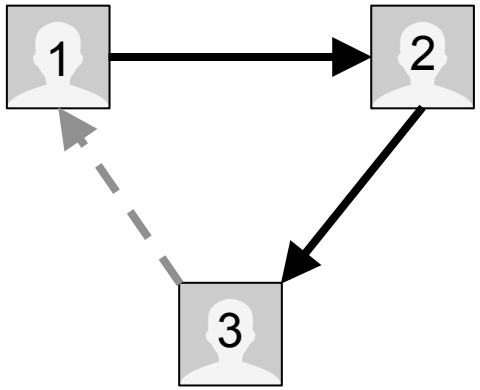
People you may know…



Internal needs of design

Social networks

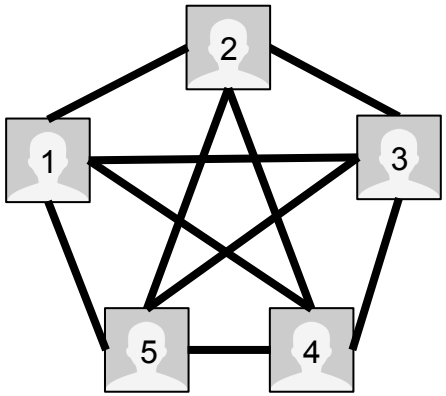
- Social networks "thrive" when users:
  - Engage – check up on each other
  - Interact – share information with each other
  - Connect – find new and old acquaintances



- How to maximize these qualities?
  - Close Triads
  - Homophily – love of same
  - Propinquity – closeness, kinship
  - Reciprocity – exchange for mutual benefit

Need for decreased uncertainty

Social Networks



Congratulations, you know everyone!

- How do users behave in a fully connected network, and why?
- Lack of intimacy reduces quality of interaction
- Fewer interactions lead to fewer engagements

Uncertainty–

- How to increase intimacy with opportunities to discover new connections?

Normal configuration

- Normal configuration is “the general shape and arrangement that is commonly agreed to best embody the operational principle” – *Vincenti*

- Examples of normal configurations:
  - Pop-up windows to confirm irreversible actions (Safety)
  - Progress bars (Awareness)
  - Default settings that restrict access (Security)
  - Virtual memory management (Performance)

Carnegie Mellon University

Children's Online Privacy Protection Rule

§312.5 Parental Consent.

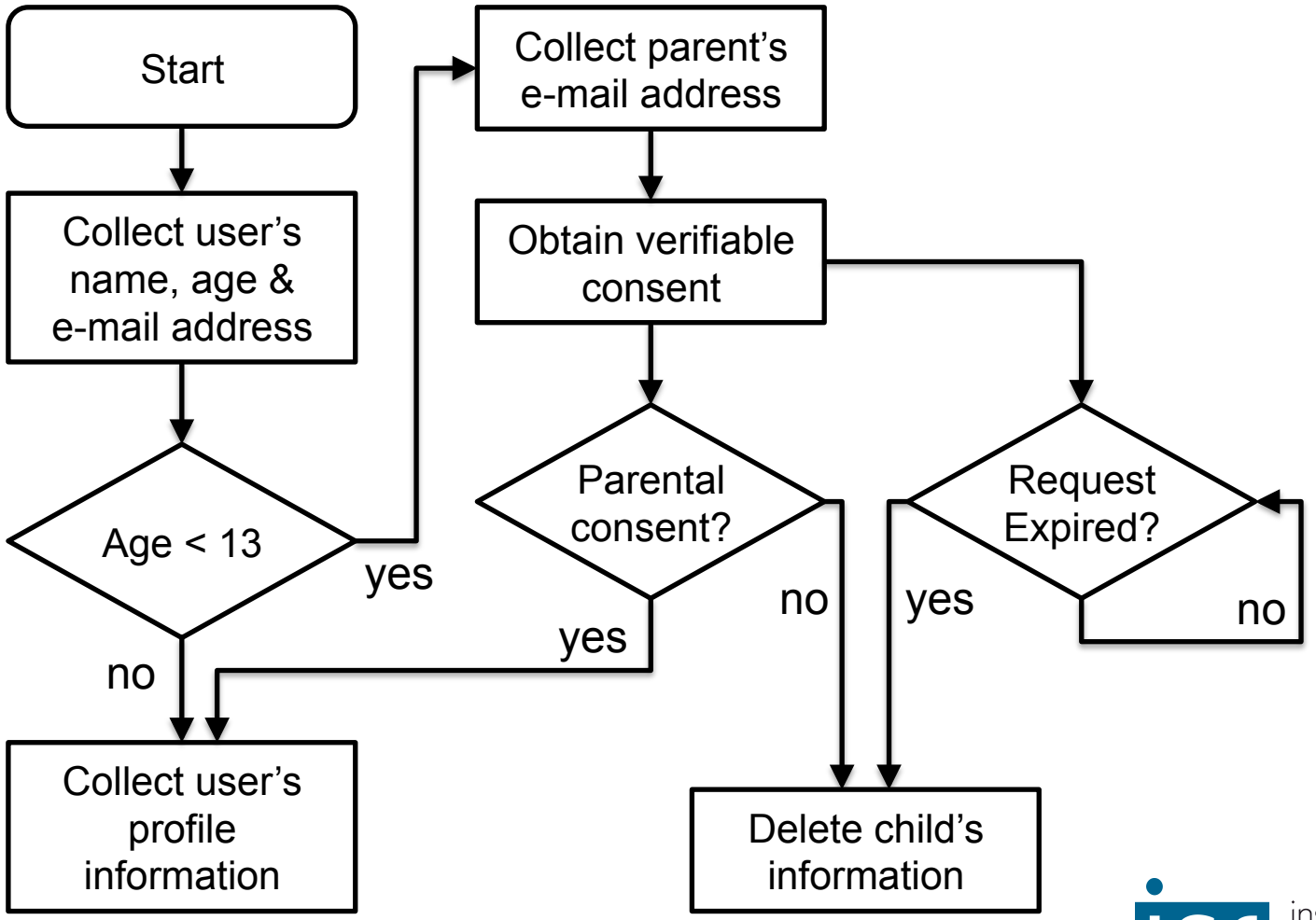
(a) General requirements. (1) An operator is required to obtain verifiable parental consent before any collection, use, and/or disclosure of personal information from children…

(b) Mechanisms for verifiable parental consent.

(1) An operator must make reasonable efforts to obtain verifiable parental consent…

(2) Methods to obtain verifiable parental consent that satisfy the requirements of this paragraph include: providing a consent form to be signed by the parent and returned to the operator by postal mail or facsimile; requiring a parent to use a credit card in connection with a transaction; having a parent call a toll-free telephone number staffed by trained personnel; using a digital certificate that uses public key technology; and using e-mail accompanied by a PIN or password obtained through one of the verification methods listed in this paragraph.

Implementing Verifiable Consent



HIPAA De-Identification Safe Harbor

- Names
- All geographic subdivisions smaller than a state, except for first 3 digits of ZIP code*
- Dates directly related to an individual
- Telephone number
- Fax number
- Electronic mail address
- Social security number
- Medical record number
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers
- Device identifiers and serial numbers
- Universal Resource Locators
- Internet Protocol addresses
- Biometric identifiers
- Full face photographs
- Any other uniquely identifying number, characteristic or code**

"Normal" based on theory

- De-identification standards should be based on strong theoretical foundations*
  - k-anonymity – individual records cannot be distinguished from at least k-1 other individuals whose information also appears in the dataset [Sweeney, 2002]
  - ℓ-diversity – requires that each sensitive class has at least ℓ well-represented values for the class [Machanavajjhala et al. 2006]
  - t-closeness – the distance between the distribution of a sensitive attribute in a sensitive class and in the entire dataset is no more than t [Li et al., 2007]

**that explain when datasets are subject to re-identification attacks*

"Normal" based on experience

- Payment Card Industry (PCI) Data Security Standard
  - **PCI-DSS 3.2**: Do not store sensitive authentication data after authorization (even if encrypted)
- NIST Special Pub. 800-53, Rev. 4, Appendix J
  - **AR-8:** Keeps an accurate accounting of disclosures held in each system under its control, including: date, nature and purpose of disclosure; name and address of receiving agency

Innovative solutions?

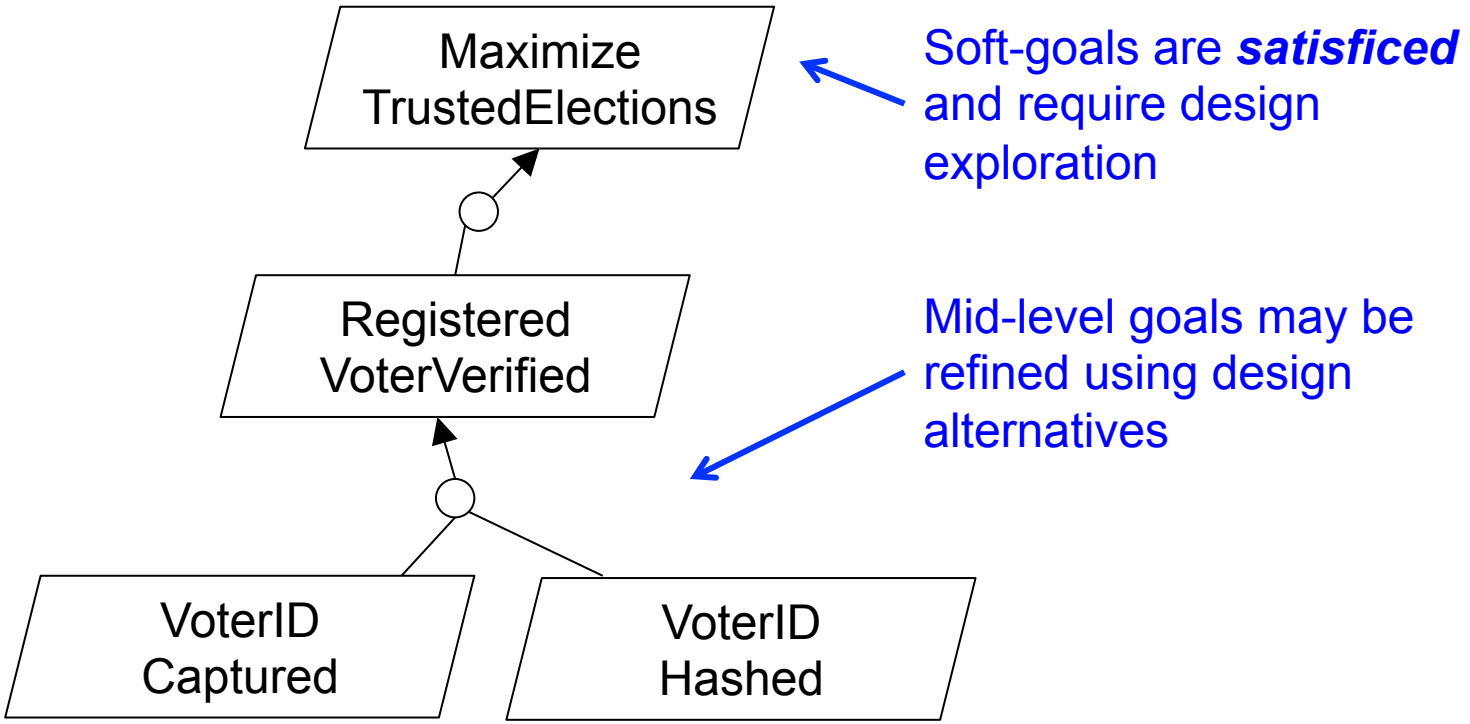
- Normal configurations exist for problems that have been encountered before

Use cases, flows and exceptions

Use Case Name	**Commenting on Tagged Photo**
Actors	Tagged Friend, Poster
Pre-conditions	Friend was tagged in the Poster's photo
Flow of events	1. Friend views the photo 2. Friend reads the description, including their tag 3. Friend accepts the tagged photo and writes a comment on the photo
Post-conditions	Comment is viewable with the photo
Alternate flows and exceptions	• Friend was incorrectly tagged in the photo • Friend rejects photo and removes the tag

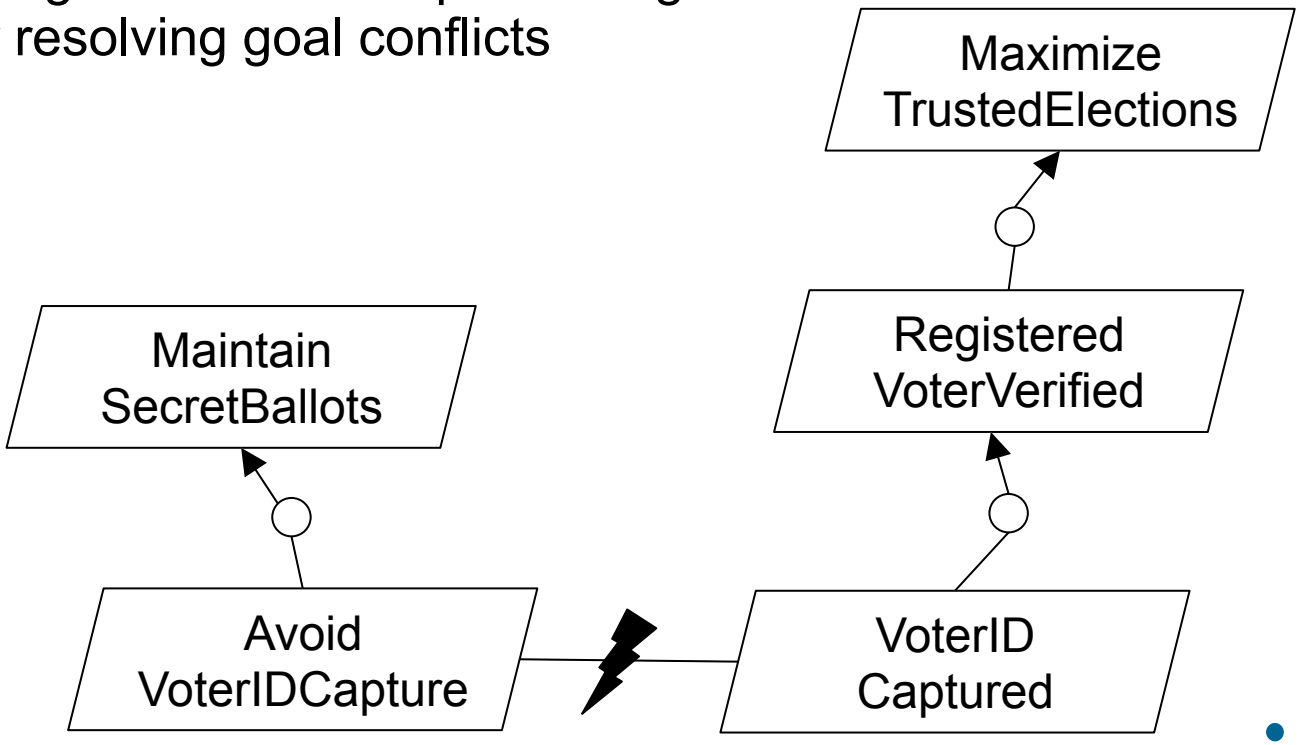
Goal modeling

- Goals are elicited from key stakeholders to obtain and refine high-level objectives into low-level requirements



Goal conflicts

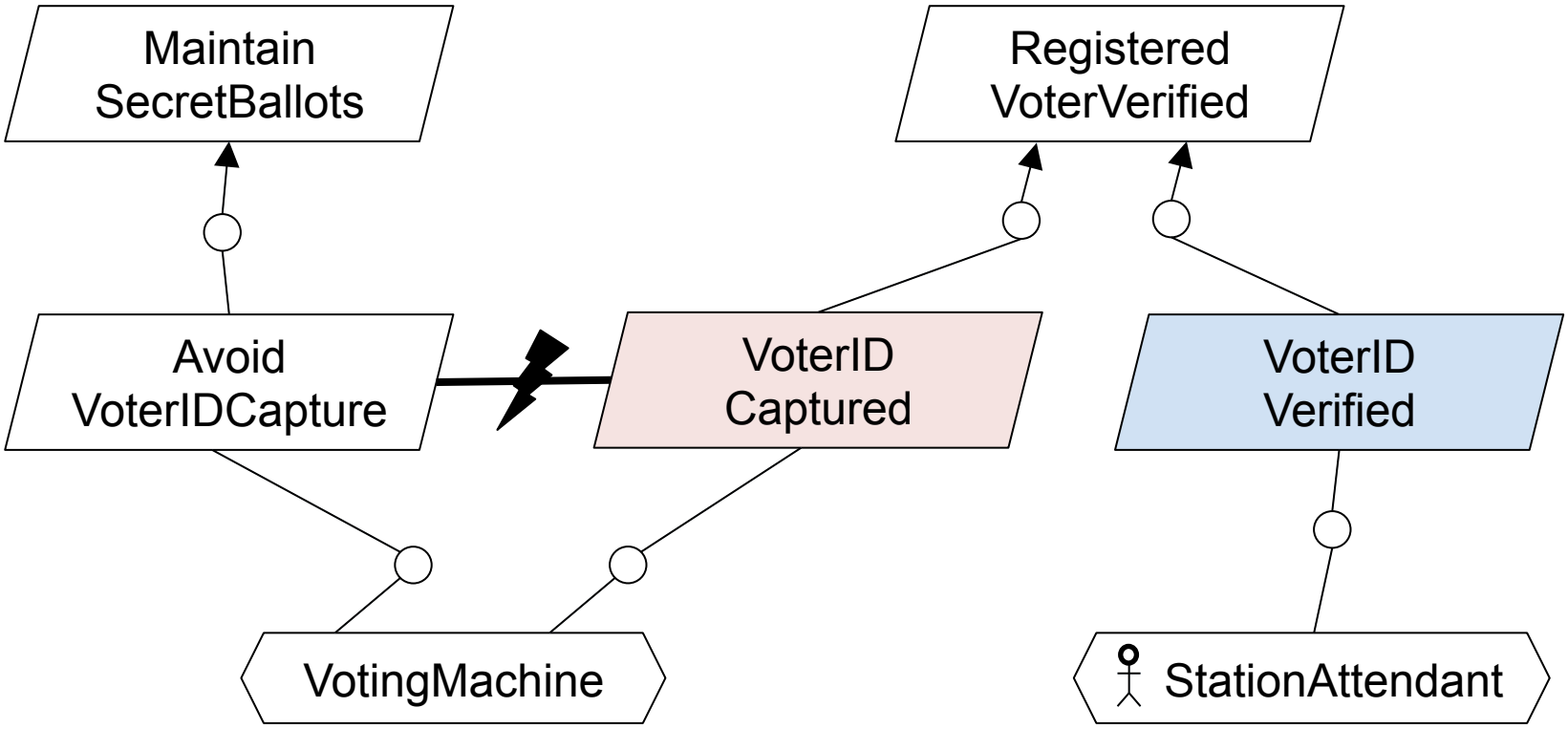
- Conflicts arise between goals at different levels in the goal hierarchy
- Designers have multiple strategies for resolving goal conflicts



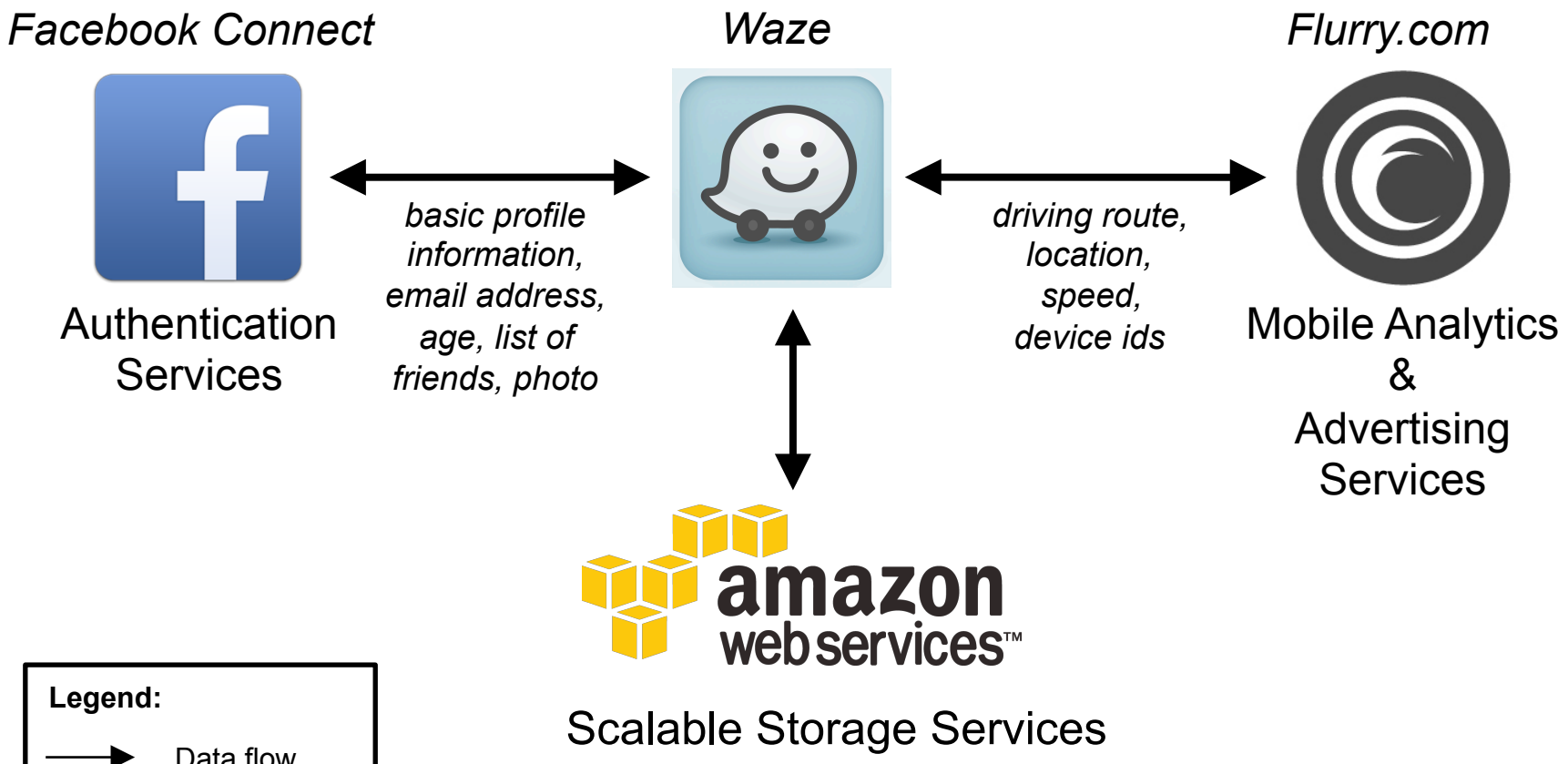
Strengthening goals for risks

- Unacceptable exposure to risk may require strengthening goals
- Ensuring that ballots are secret involves different risk levels
  - Avoid[VoterIDCapture] – minimal risk, because only the vote is recorded, and not the voter ID
  - Avoid[VoterIDLinking] – higher risk, because timestamps may be used to correlate votes and voter IDs
  - Avoid[VoterIDTransfer] – highest risk, because the votes and voter IDs are linked internally

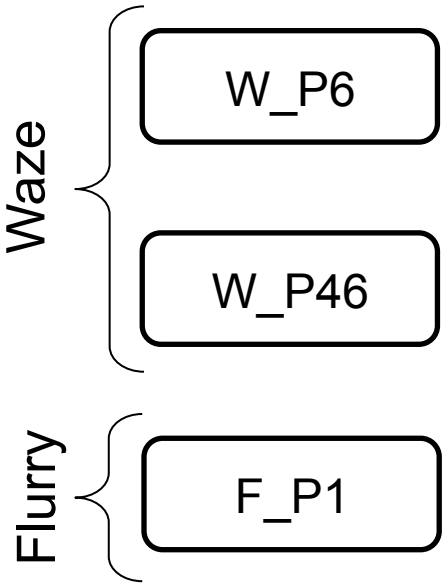
Transfer conflicts outside system



Example Service Integration



Tracing multi-party data flows



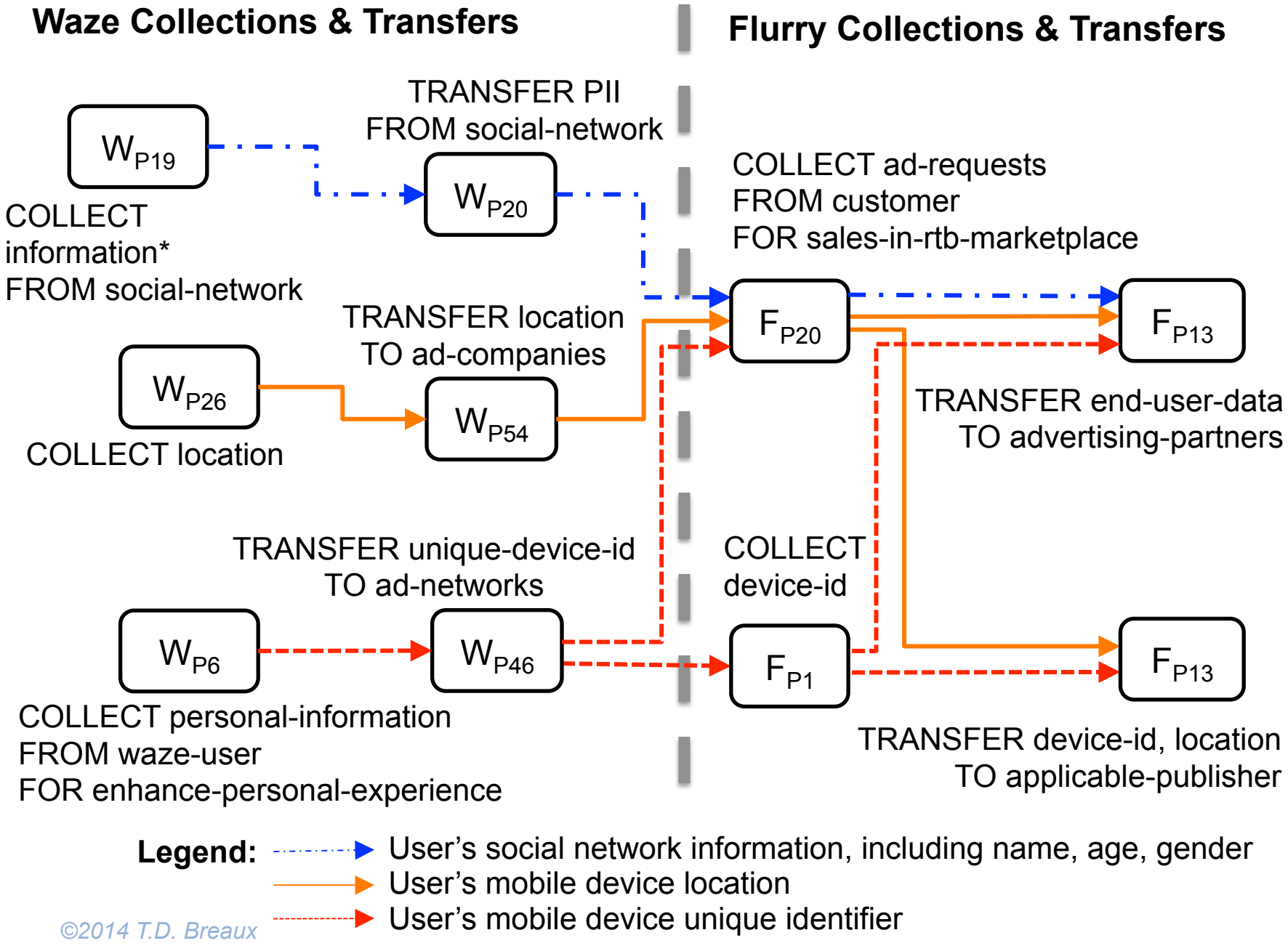
COLLECT personal-information FROM waze-user
FOR enhancing-service-experience

TRANSFER unique-device-id TO ad-networks

COLLECT device-id, device-os, mac-address

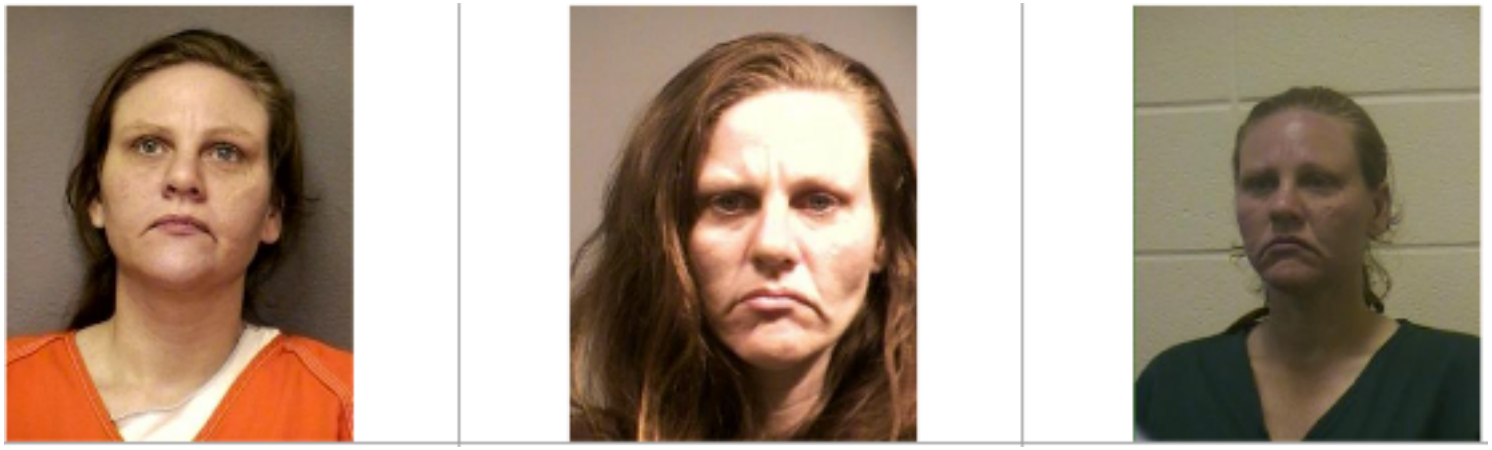
Assume: unique device id is part of personal information
Assume: unique device id is a synonym for device id and mac address

Example from Waze and Flurry.com privacy policy



2D Still-Images in MBE Study

- Three law enforcement mugshots taken from the same person at different times



Grother et al. “Report on the Evaluation of 2D Still-Image Face Recognition Algorithms”, Multiple Biometric Evaluation, NIST Interagency Report 7709, 2010.

Good, Bad, Ugly Challenge (GBU)

Phillips et al., “An Introduction to the Good, the Bad, & the Ugly Face Recognition Challenge Problem,” NIST 2010

Labeled Faces in the Wild (LFW)

- Face photos curated by photo journalists prior to being posted on the web



Three photos of Janica Kostelic, a former World Cup alpine ski racer and for-time Olympic gold medalist

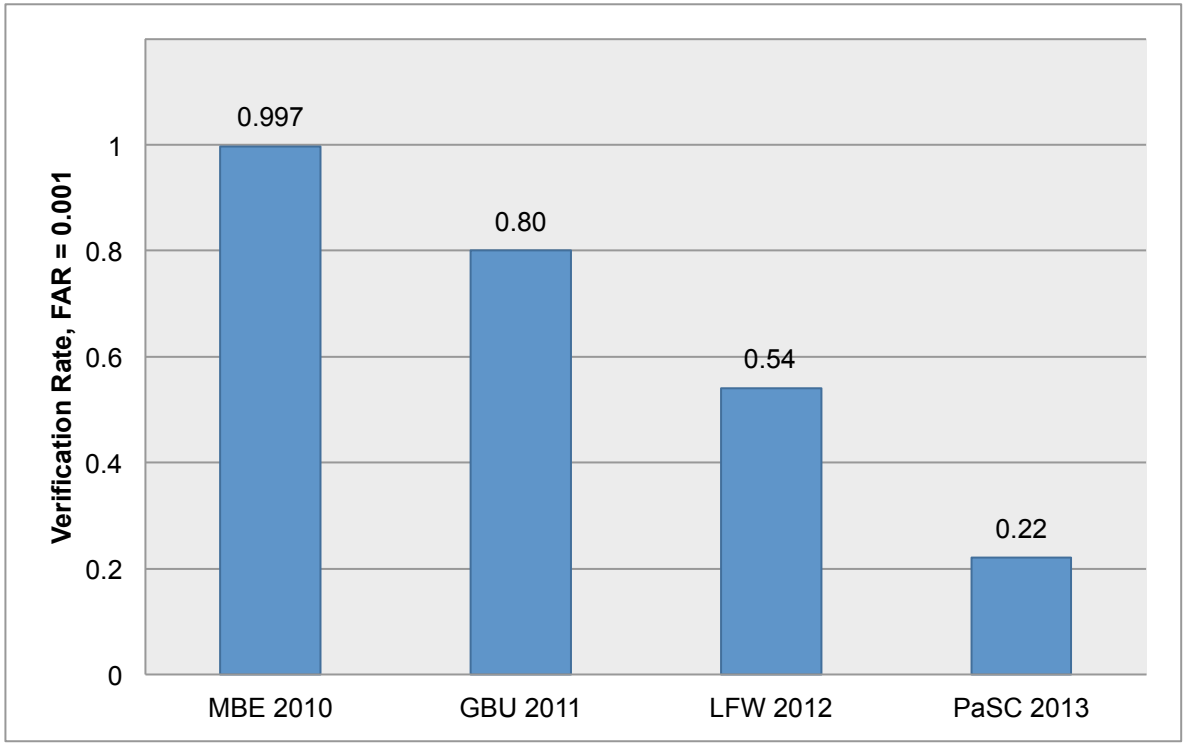
Point-and-Shoot Challenge (PaSC)

Variables…

- Locations
- Sensor
- Camera distance
- Pose

Beveridge et al. “The Challenge of Face Recognition from Digital Point-and-Shoot Cameras,” Rev. 1.0, 2012

Facial recognition evaluation



- Verification rates reported for each evaluation; assumes 1/1000 False Accept Rate (FAR)

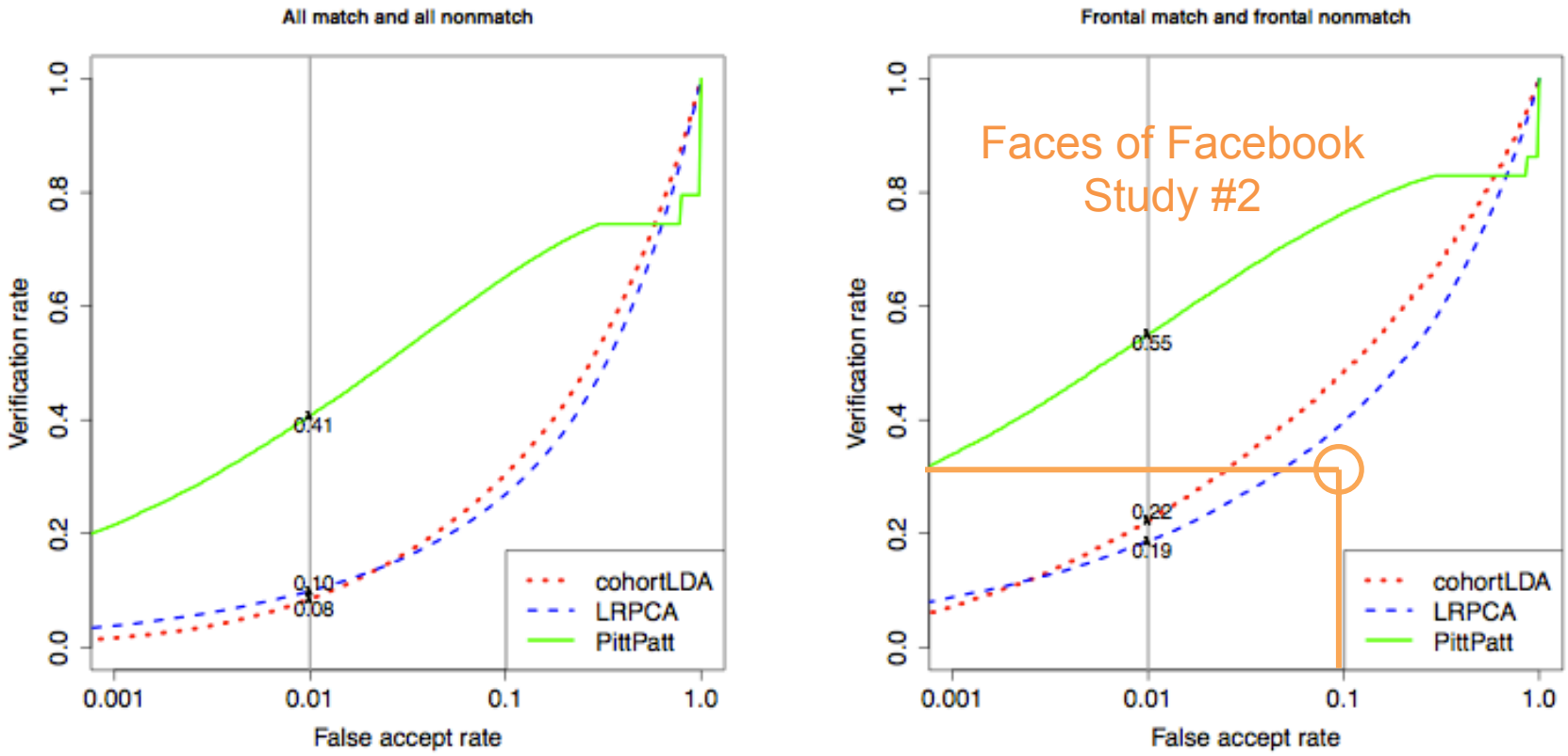
Beveridge et al. "The Challenge of Face Recognition from Digital Point-and-Shoot Cameras," Rev. 1.0, 2012

Faces of Facebook Study

- Researchers collected 261,262 images from 25,051 Facebook (FB) profiles
- Compared these to 3 webcam photos of participants
- Study Results:
  - Detected 114,745 “unique faces” in FB data
  - Verification rate: 31.18% with FAR 0.1

Acquisti, Gross, Stutzman. “Faces of Facebook: Privacy in the Age of Augmented Reality”, Black Hat 2012

Face Recognition Performance



Faces of Facebook Study #2 performing frontal matches had a verification rate of 31.18% with FAR 0.1

Presentation Summary

- Design is driven by operating principles
- Design aims to reduce uncertainty through:
  - Strong theoretical foundations
  - Experience drawn from failure
- Designers can use informal and formal specification to explore and capture design strategy
- Designers can use quantitative data to evaluate design alternatives