CITeR
CENTER FOR
IDENTIFICATION
TECHNOLOGY
RESEARCH

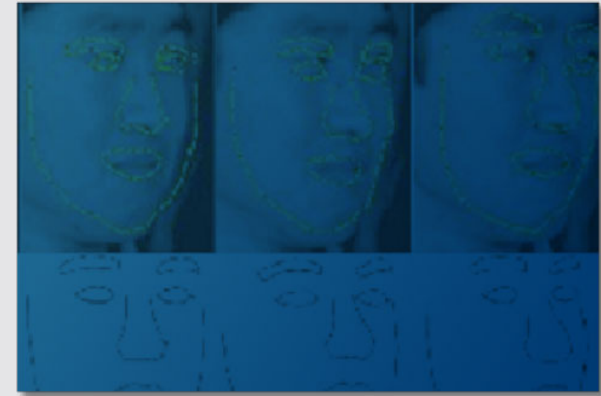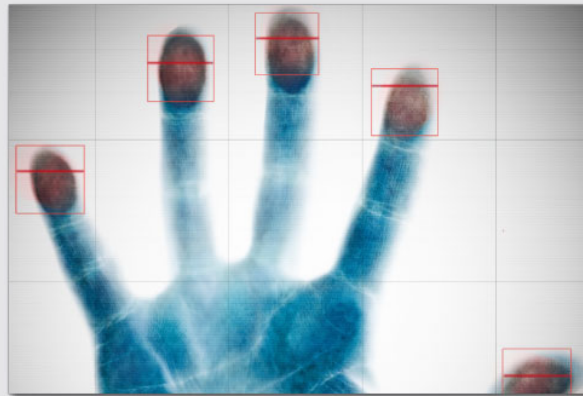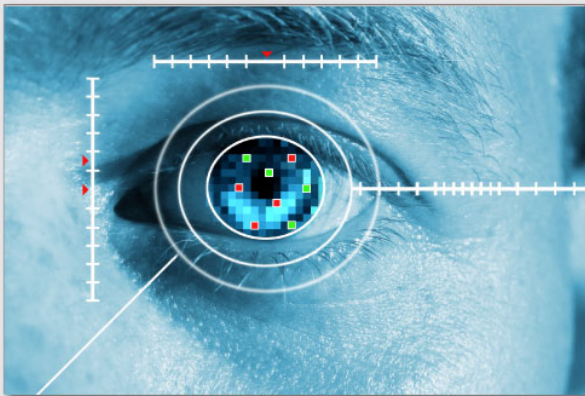A National Science Foundation
Industry/University Cooperative Research Center

Who You Are –
Research Challenges in Biometrics (Identity)

Dr. Stephanie Schuckers, Clarkson University

Director, Center for Identification Technology Research

Presented April 2014

University at Buffalo
The State University of New York

Clarkson
UNIVERSITY
defy convention

THE UNIVERSITY
OF ARIZONA.

West Virginia University

Authentication

- **What you have**

  e.g., ID cards, passports, keys

- **What you know**

  e.g., password, PIN, user ID

- **Who you are**

  e.g., biometrics: fingerprints, face, iris, voice, DNA

  Two step—enrollment (reference) and verification (matching)

MATT

'Grandma, do you mind if I do an iris recognition scan?'

CENTER FOR
IDENTIFICATION
TECHNOLOGY
RESEARCH

© CITeR
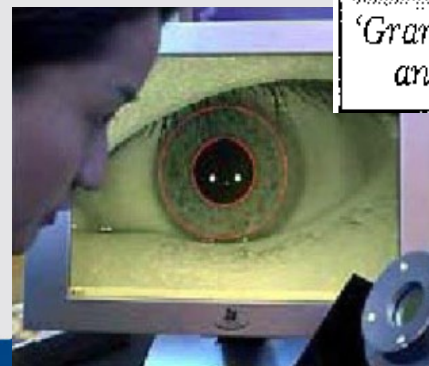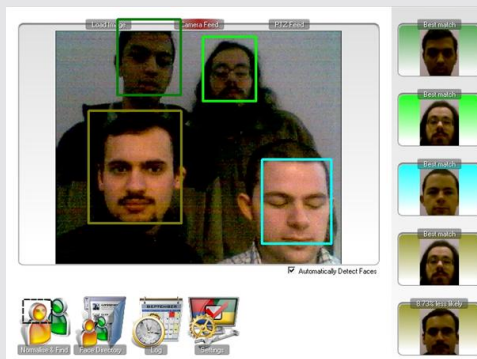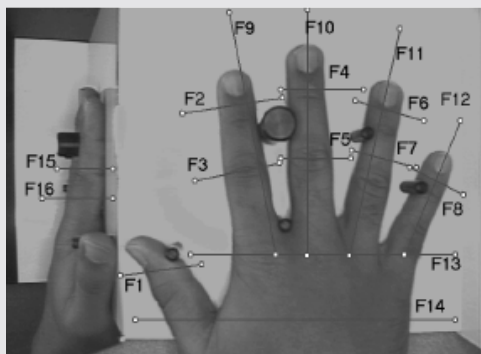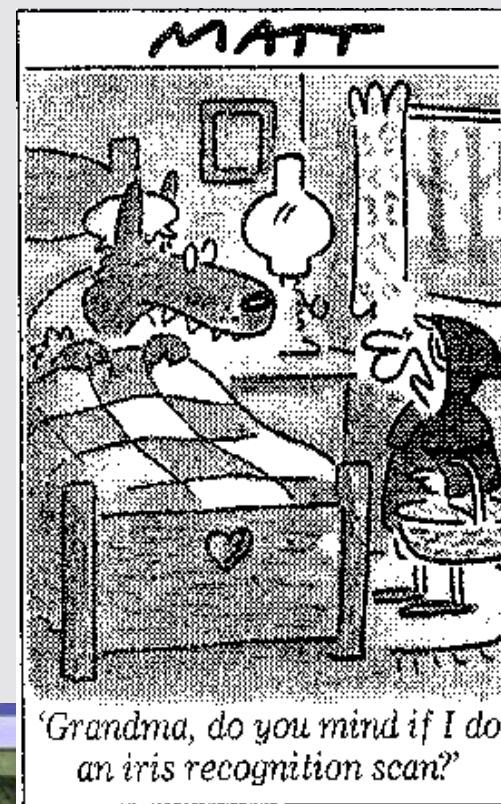
Identity

- Medentity is tied to a subject in a one-to-one manner.

- Ourdentity is an identity that exists by mutual agreements between a subject and a third party.

- Theirdentity is an identity that a third party guesses and internally creates without explicit consent from the subject.
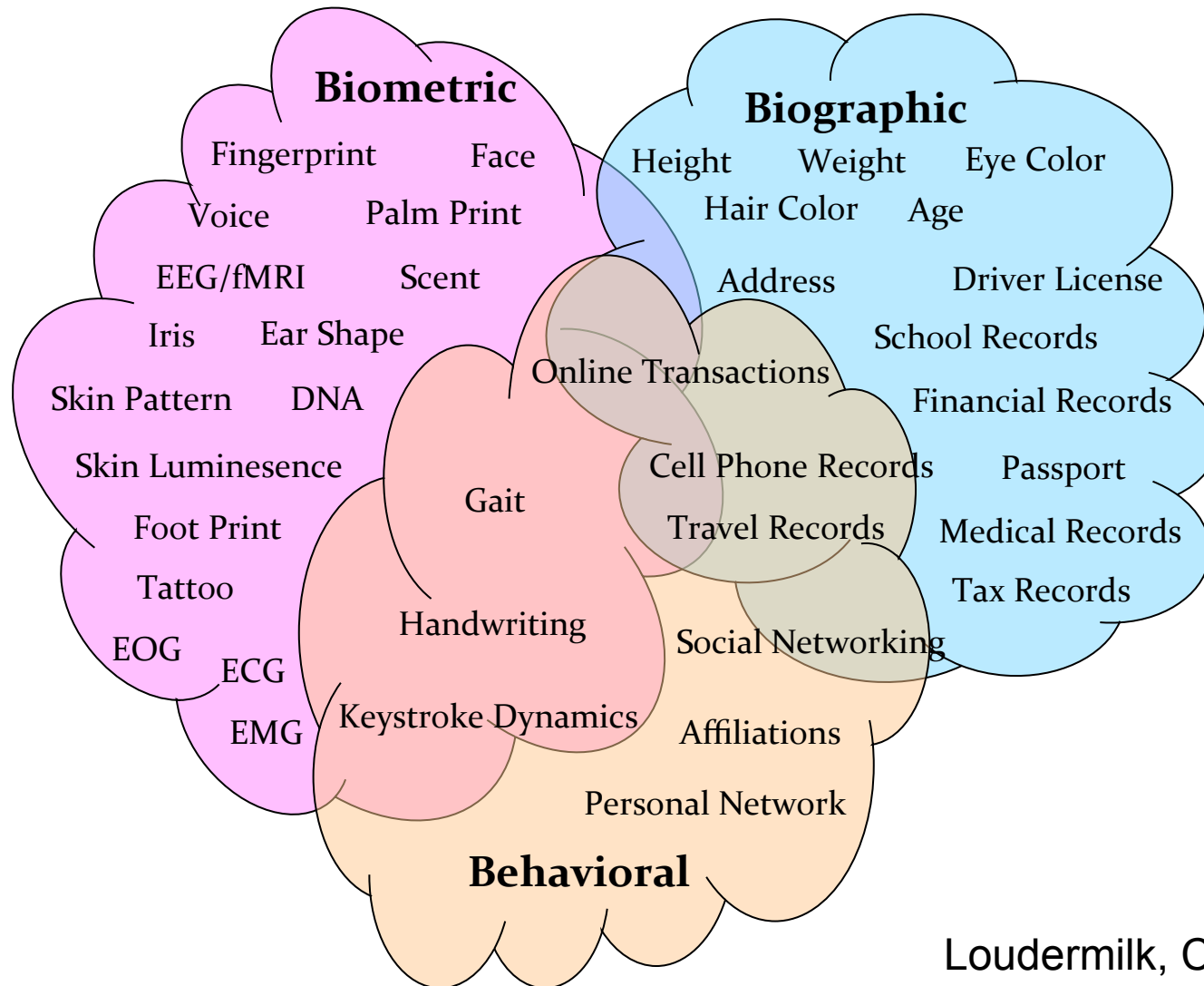

"On the Internet, nobody knows you're a dog."

Peter Steiner, The New Yorker, July 5, 1993

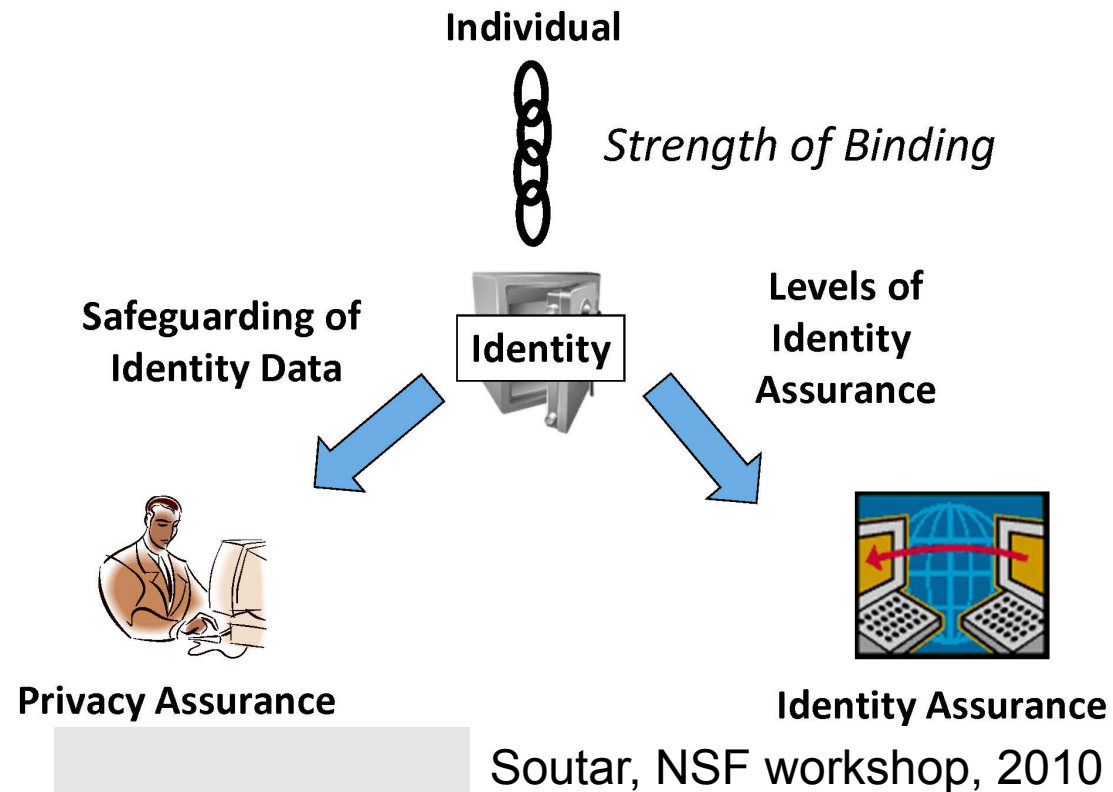Elisa Bertino, NSF Workshop Biometrics, 2010.
Searls, D., "Mydentity & Ourdentity vs. Theirdentity," 2006.

CITeR
CENTER FOR
IDENTIFICATION
TECHNOLOGY   3
RESEARCH
© CITeR

Elements of Human Identification

Biometric
Fingerprint
Face
Voice
Palm Print
EEG/fMRI
Scent
Iris
Ear Shape
Skin Pattern
DNA
Skin Luminesence
Foot Print
Tattoo
EOG
ECG
EMG

Biographic
Height
Weight
Eye Color
Hair Color
Age
Address
Driver License
School Records
Financial Records
Passport
Medical Records
Tax Records

Online Transactions
Cell Phone Records
Travel Records

Gait
Handwriting
Keystroke Dynamics

Social Networking
Affiliations
Personal Network

Behavioral

Loudermilk, ConnectID, 2014

4

Privacy

- Personal information

    Biographic information (name, age, DOB, address, gender)

    Issued identifiers (e.g., social security number)

    Physiologic (e.g. biometrics, medical)

    Geographic, behavioral, social, purchasing, etc.

- PII--"Personally Identifiable Information"

- Obligation to protect personal information

- Revealing data in return for benefits

- Disclosure of how data used and giving individuals control
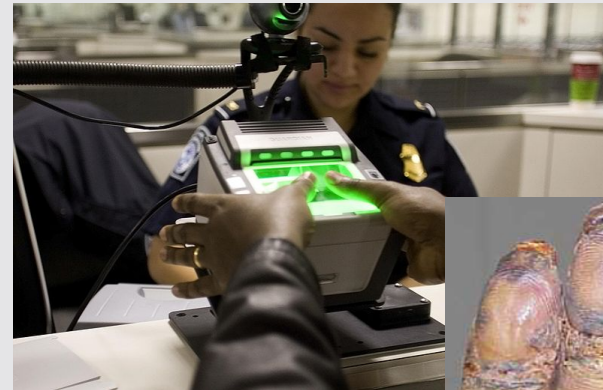
- Need technologies to support

Individual

Strength of Binding

Safeguarding of Identity Data

Identity

Levels of Identity Assurance

Privacy Assurance

Identity Assurance

Soutar, NSF workshop, 2010

CITeR
CENTER FOR IDENTIFICATION TECHNOLOGY RESEARCH

© CITeR

Large Scale Biometric Systems

Grillo, Biometric Consortium Presentation, 2010

- Department of Homeland Security
  - Over 100 million person biometric database
  - Line of defense at the border
  - Altered fingers to "hide" identity
- Unique Identification Authority of India (UIDAI)
  - Enrolling over 1.2 billion people
  - Providing "credentials" for access to social benefits and banking sector; for many first "identity"
  - "Leap frog" of the developed world

Feng, et al, IEEE TIFS article, 2009.

http://uidai.gov.in

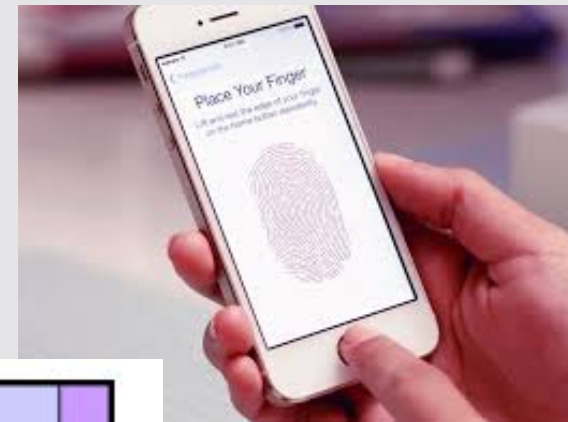AADHAR

IDENTIFICATION TECHNOLOGY RESEARCH

6

© CITeR

BYOD

- Rise in mobile payments

  -Near field communication using mobile devices for "credit card" payments at the point of service

- Increased need for security AT the device

  -"Bring your own device" (BYOD)

  -Multifactor authentication

  -Convenience of security

Techradar, 1/16/2013

iPhone with a fingerprint reader embedded in the button

Challenges (and Research Directions) in Biometrics

- **Privacy**

  Data protection

  Data sharing

- **Security**

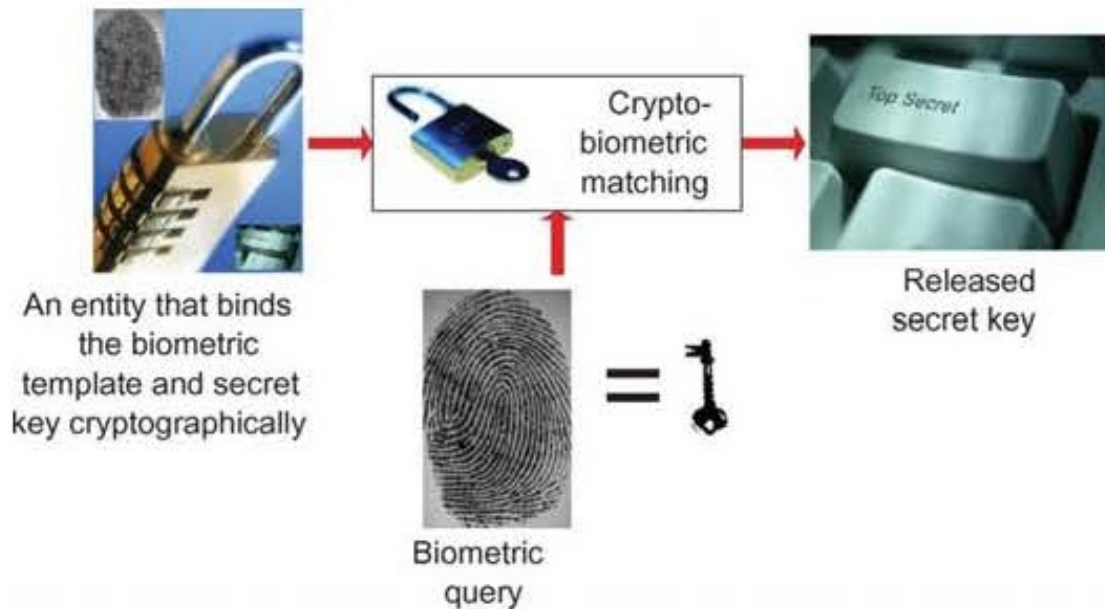 Biometrics are not secret

  Biometrics cannot be changed
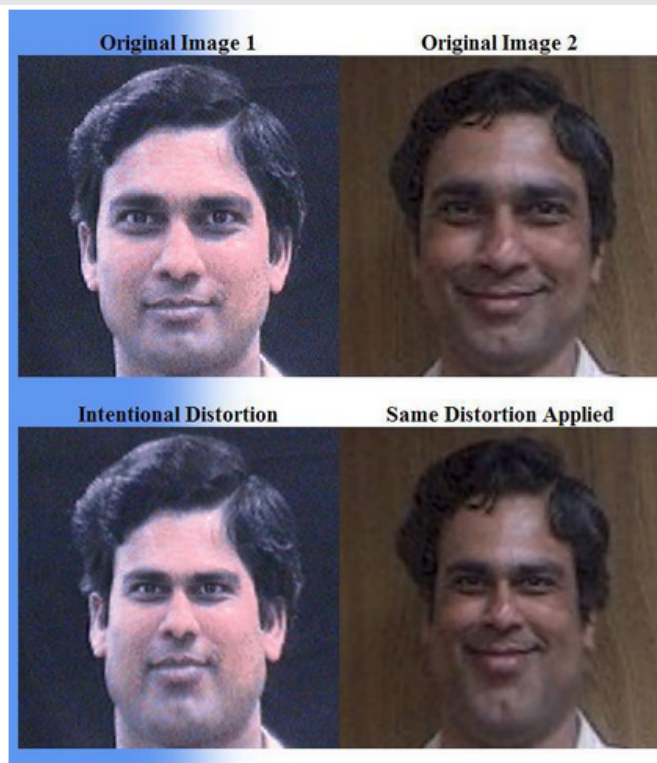
CITeR

CENTER FOR
IDENTIFICATION
TECHNOLOGY
RESEARCH

© CITeR

Template Security:
Addressing "Biometrics cannot be changed"

Cancelable Biometrics


Biometric Cryptosystems

Nandakumar, et al, Fingerprint-Based Fuzzy Vault, 2007

**Security Metrics: Irreversibility, Unlinkability, Robustness, etc.**

N. Ratha, J. Connell, R. Bolle, Enhancing security and privacy in biometrics-based authentication systems 2001.

Presentation Attacks

- Spoofing is a common term also used

  Posing as another individual
  - Positive ID applications

  Hiding your identity
  - Negative ID applications
  - May form 'new' identity for positive ID
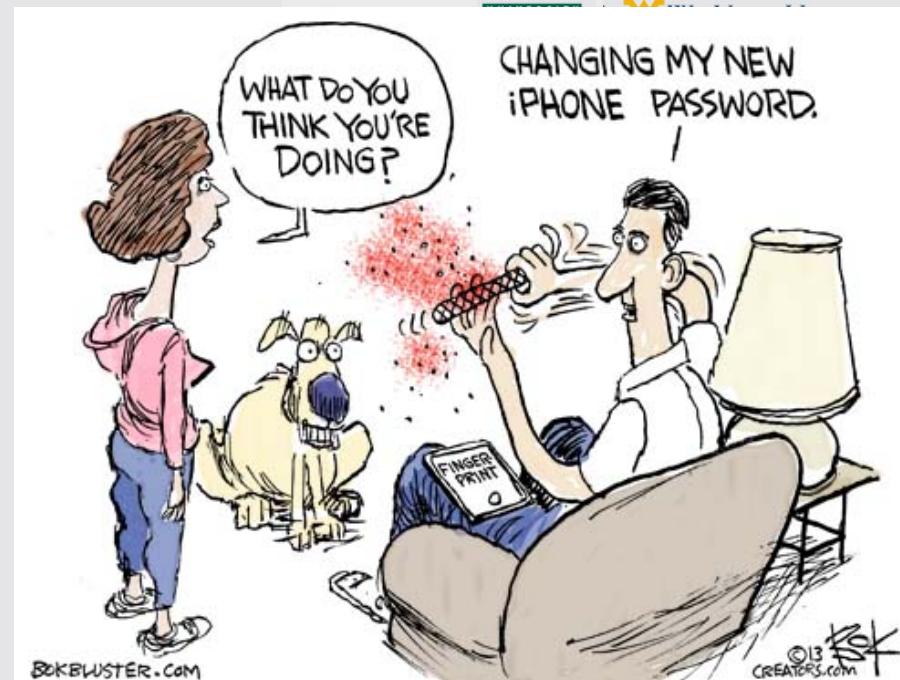
Fake FIngerprints
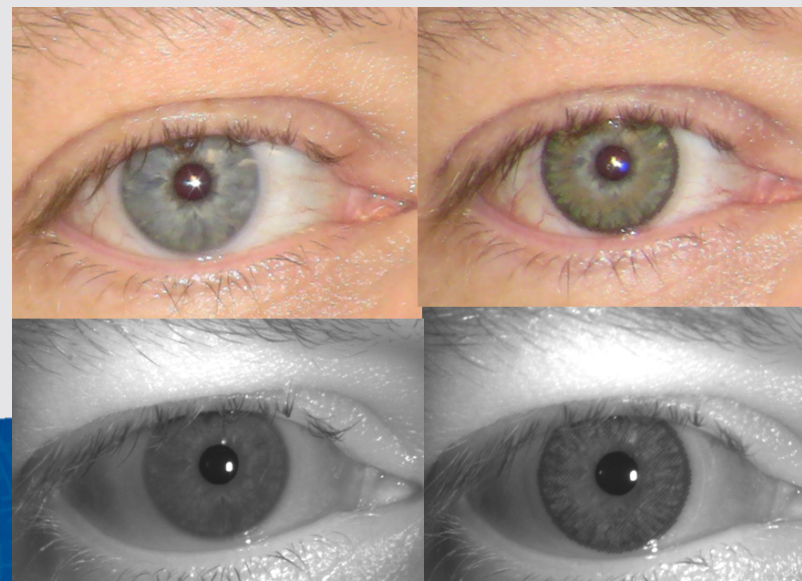
Patterned Contact Lens

Liveness Detection in Biometrics
Addressing "Biometrics is not Secret"

- Liveness Detection: Determining if a biometric is being "spoofed" through hardware and/or software
- "It Is '**Liveness**', **Not Secrecy**, That Counts." Denning, Information Security Magazine, 2001
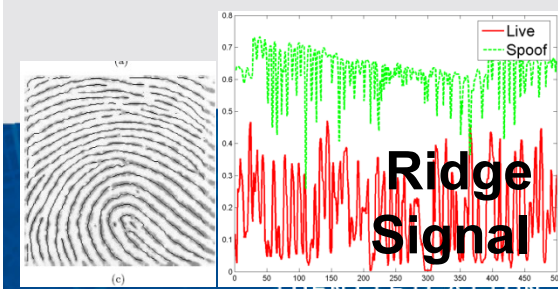
Hardware

e.g., "Morpho, World's First Company to Receive Common Criteria Certification for Fake Finger Detection", July 2013
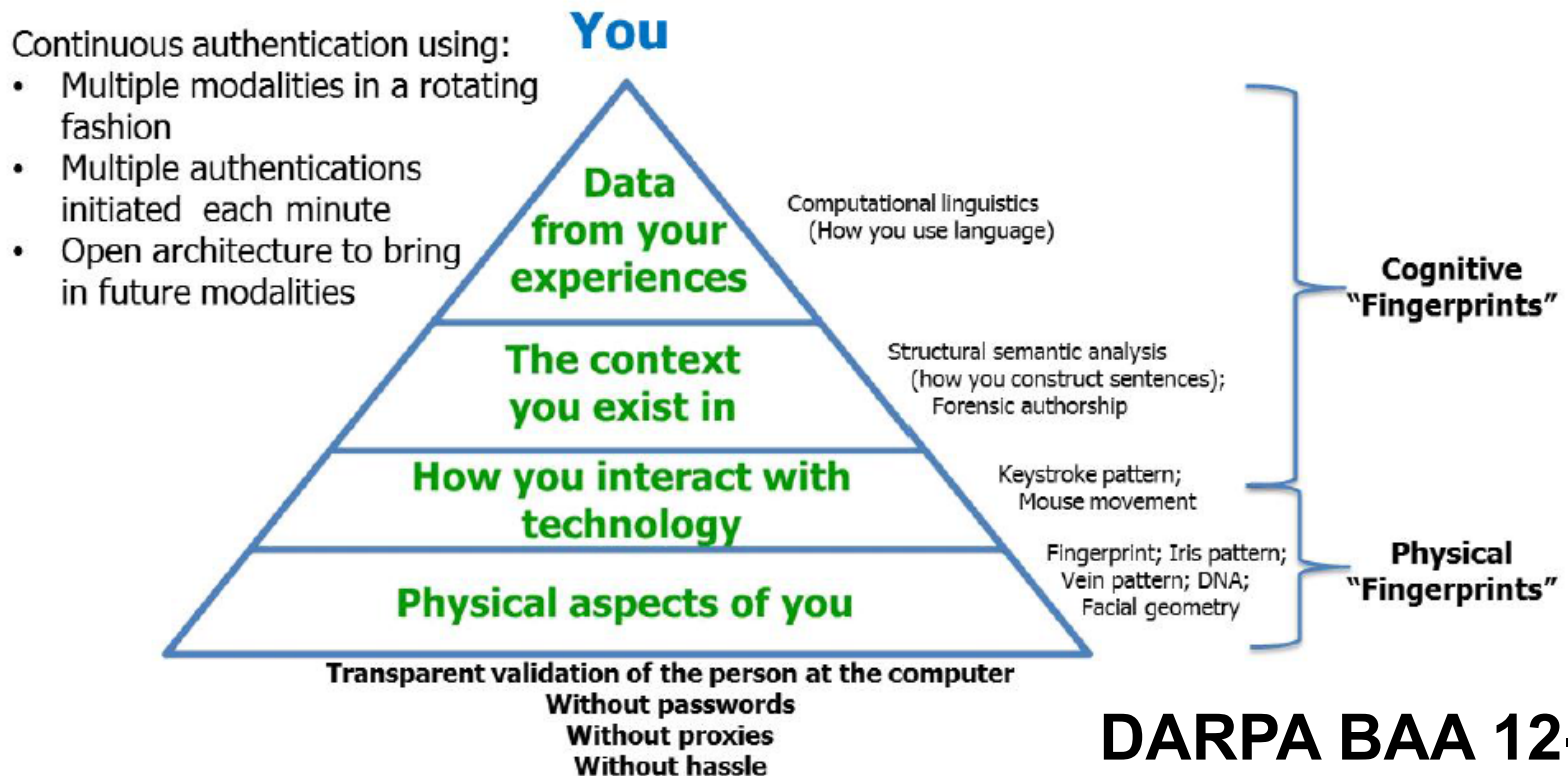
Software

Ridge Signal

Derakhshani R, Schuckers SAC
Pattern Recognition, 2003

Continuous or "active" authentication

Continuous authentication using:
- Multiple modalities in a rotating fashion
- Multiple authentications initiated each minute
- Open architecture to bring in future modalities

You

Data from your experiences — Computational linguistics (How you use language)

The context you exist in — Structural semantic analysis (how you construct sentences); Forensic authorship

How you interact with technology — Keystroke pattern; Mouse movement

Physical aspects of you — Fingerprint; Iris pattern; Vein pattern; DNA; Facial geometry

Cognitive "Fingerprints"

Physical "Fingerprints"

Transparent validation of the person at the computer
Without passwords
Without proxies
Without hassle

DARPA BAA 12-06

CITeR
CENTER FOR
IDENTIFICATION
TECHNOLOGY
RESEARCH

12

© CITeR

Biometrics?

Smart Watch

Vyteris

Smart patch
(for controlled delivery of drugs)

Google glasses

Sazonov et al, Obesity, 2009

Wearable monitor of energy intake (measuring "what you eat")

Research Challenges
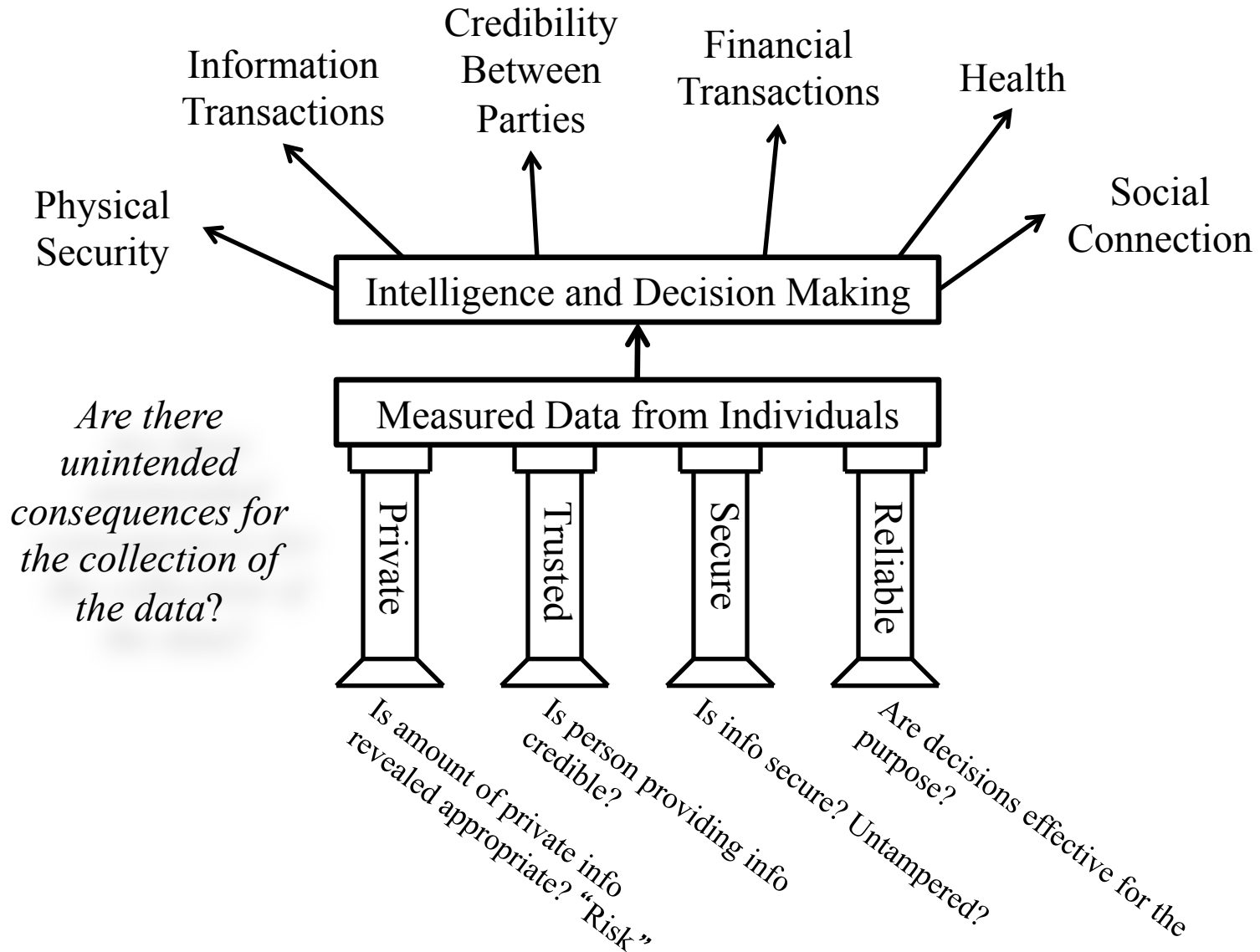
Research Challenge

Usable, Searchable without revealing identity

↑

Measured Data from Individuals

(Some of the time)

Measured Data from Individuals

↓

Confirm Identity without revealing the data