

# Biometrics

MO826 / MC936

**Prof. Dr. Anderson Rocha**

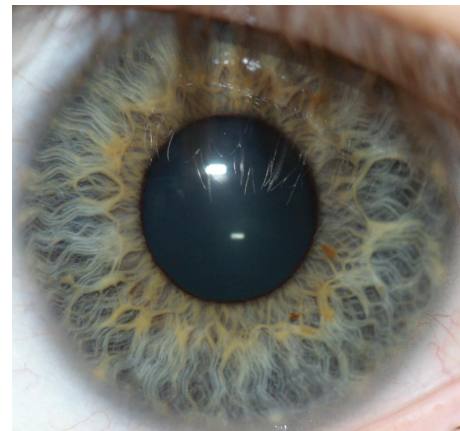
*Microsoft Research Faculty Fellow  
Affiliate Member, Brazilian Academy of Sciences  
Reasoning for Complex Data (Recod) Lab.*

[anderson.rocha@ic.unicamp.br](mailto:anderson.rocha@ic.unicamp.br)  
<http://www.ic.unicamp.br/~rocha>

**Reasoning for Complex Data (RECOD) Lab.**  
Institute of Computing,  
University of Campinas (Unicamp)

Av. Albert Einstein, 1251 – Cidade Universitária  
CEP 13083-970 • Campinas/SP – Brasil

I thank Prof. Walter J. Scheirer (Univ. of Notre Dame)  
for kindly sharing his class materials



Course Introduction / Biometrics Basics

# What about you?

- Undergrad / MS / Ph.D.?
- Any experience with Vision, Machine Learning, or Artificial Intelligence?
- What interests you about Biometrics?

# What is this course all about?

Biometrics: “the measurement of the properties of living beings”

(in Greek: *βίος* = “life”, *μέτρον* = “measurement”)



~~“What is the average size of a rat’s cranium?”~~



# Or maybe it's...

Biometrics: “the use of physical or behavioral properties of human beings for automatic identity recognition”



“But she warned him not to be deceived by appearances, for ~~beauty~~ is found within.”  
identity

*Beauty and the Beast*, 1991

# The last decade in biometrics

# Biometrics in 2005



Image credit: Lance Cpl. Jeremy Harris, U.S Marine Corps

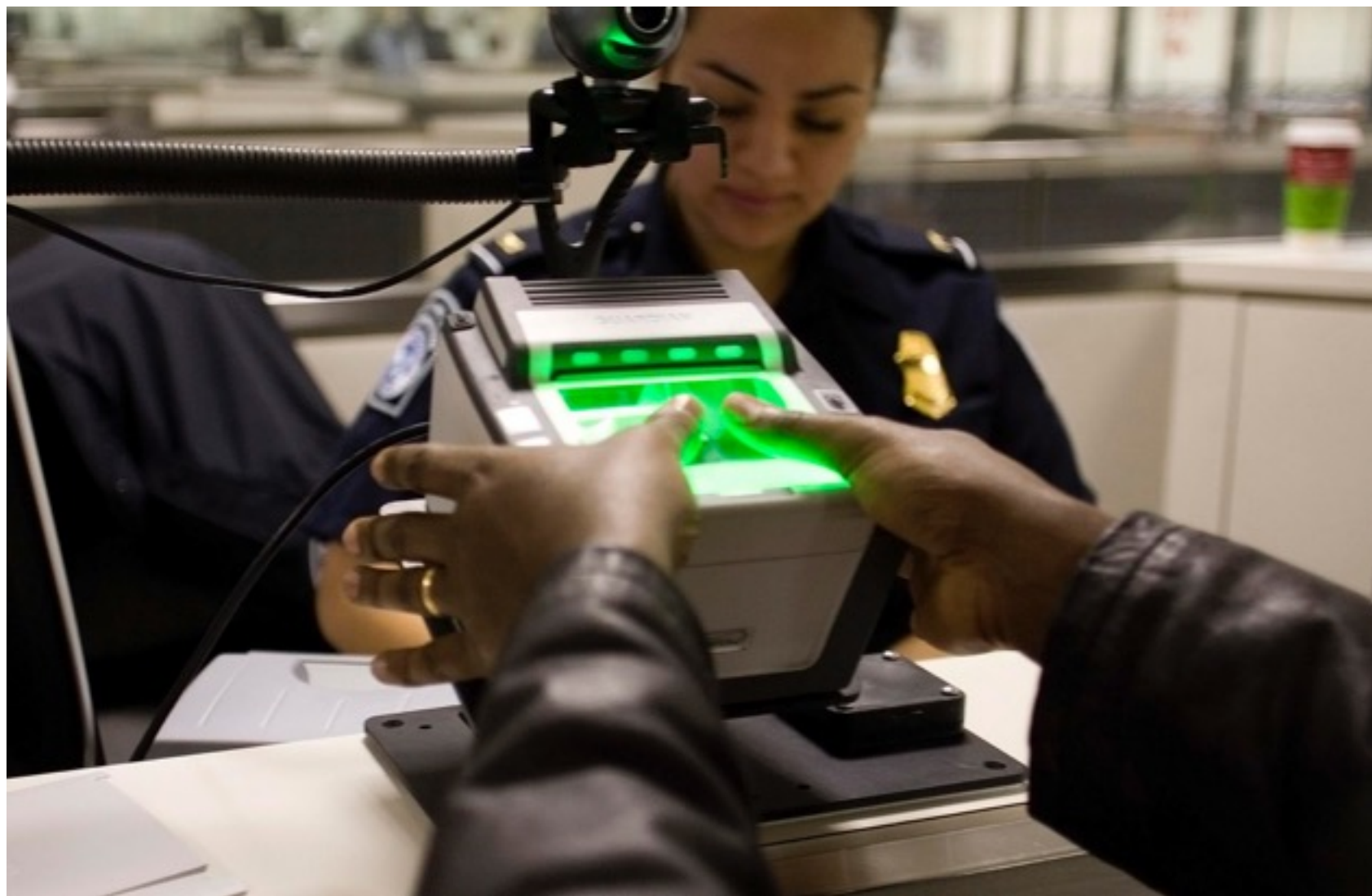


# Friend or Foe?



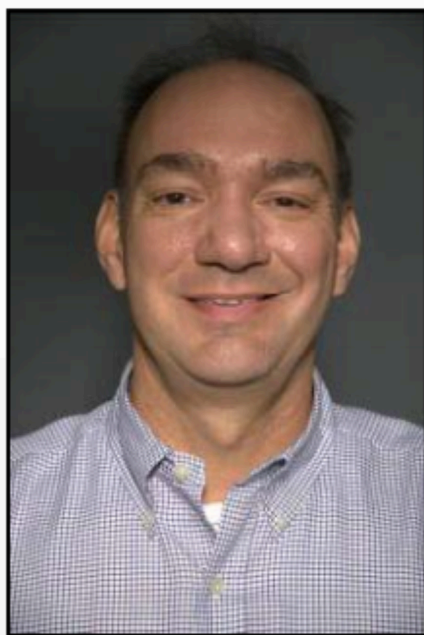


# US-VISIT



# Notre Dame Biometrics Evaluation Research

## Unconstrained Face Acquisition



Mugshot



Iris Verification

# A pivot from security



- US withdrawal from Iraq and wind down of the war in Afghanistan
- 14 years without a major terrorist action against the United States
- **Large collections, no unified infrastructure to search them.**



# The problem has not gone away

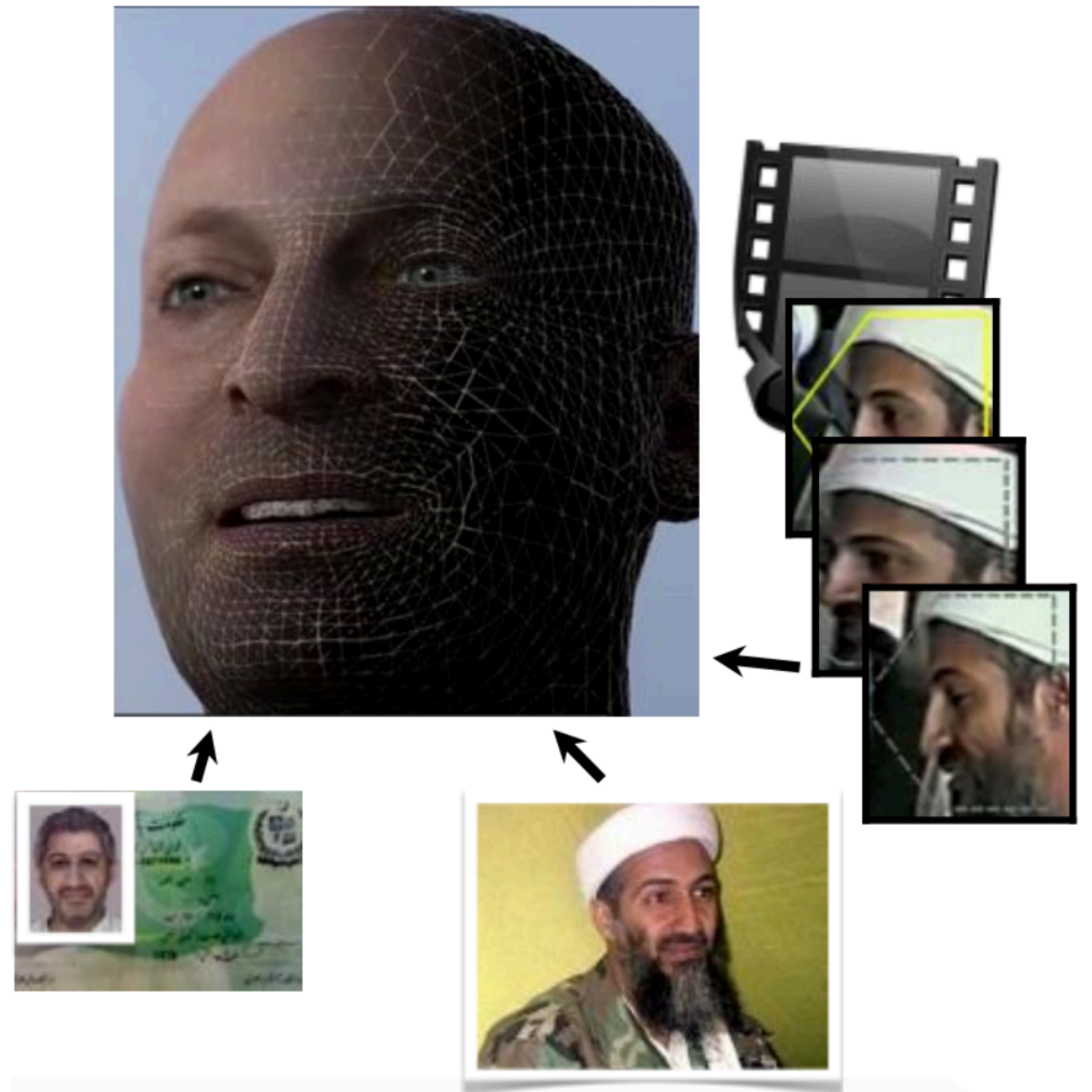


Image credit: David Green



# IARPA Janus

- Move from mugshots to operationally relevant sources
- Representations to leverage arbitrarily large data sources
- Scale to an arbitrarily large number of sources
- Tolerance for partial and incomplete data



# Biometrics in 2009



Image Credit: Reuters

# Biometrics as “Liberation”

- Developing countries have weak and unreliable identification documents
- Almost 100 countries do not reliably issue birth certificates



How does this impact food distribution, education, and disaster relief?

[http://www.unicef.org/protection/files/Birth\\_Registration.pdf](http://www.unicef.org/protection/files/Birth_Registration.pdf)

<http://www.independent.co.uk/news/world/politics/220-million-children-who-dont-exist-a-birth-certificate-is-a-passport-to-a-better-life--so-why-cant-we-all-have-one-8735046.html>



# Case Study: India

- World's 4<sup>th</sup> Largest Economy
- World's Largest Social Service Programs
  - Touches 150M Families at \$30B per year
  - 20 – 40% “leakage”
- World's largest democracy
  - 714M Voters, 364 Political Parties
- And yet in 2009... Over 600 million people had no definitive identity



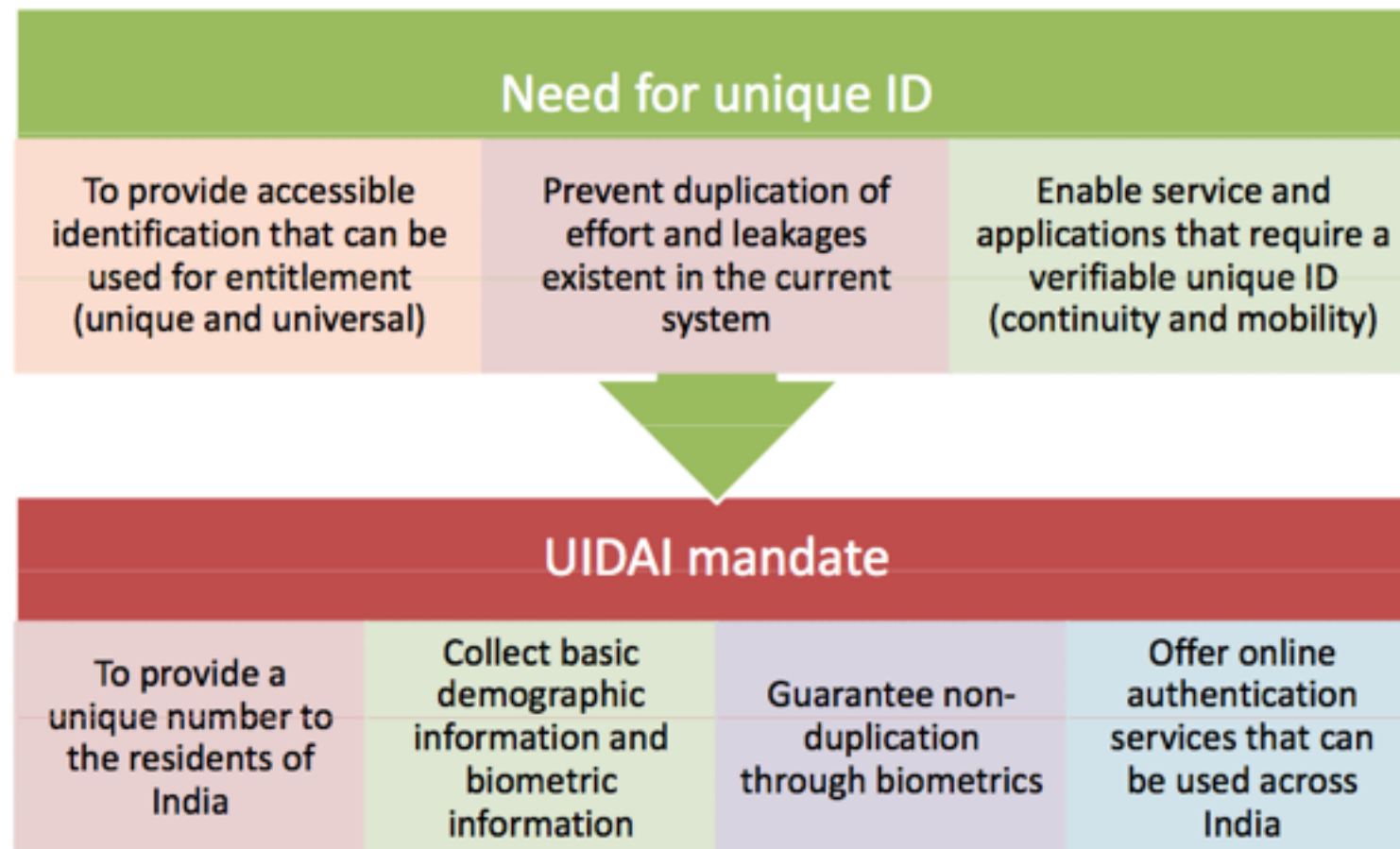


# The Need in India

- Poor do not have access to benefits and services due to inability to prove identity
- No universality of identity means re-proving again and again
- No continuity or mobility of identity
- Financial Exclusion
  - Only 18% of people have bank accounts and only 35% have savings
  - No Access to Credit
  - Savings “under the mattress”



# The Unique ID Initiative



# Information Collected for UID

KYR Fields – Name, Address, Gender, DOB 

Photo & Address Verification 

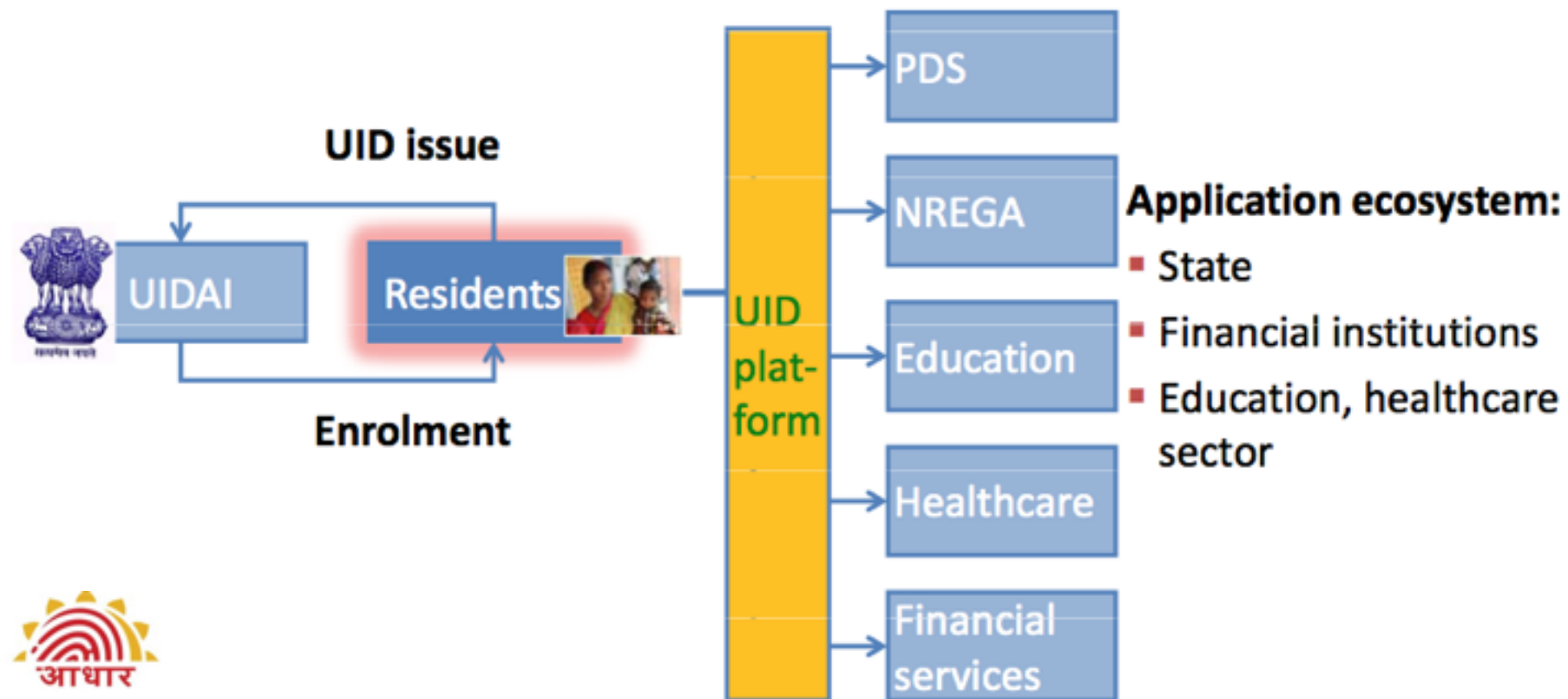
Photo 

10-fingerprints on Slap scanner 

Iris Scan 



# UID From the User's Perspective

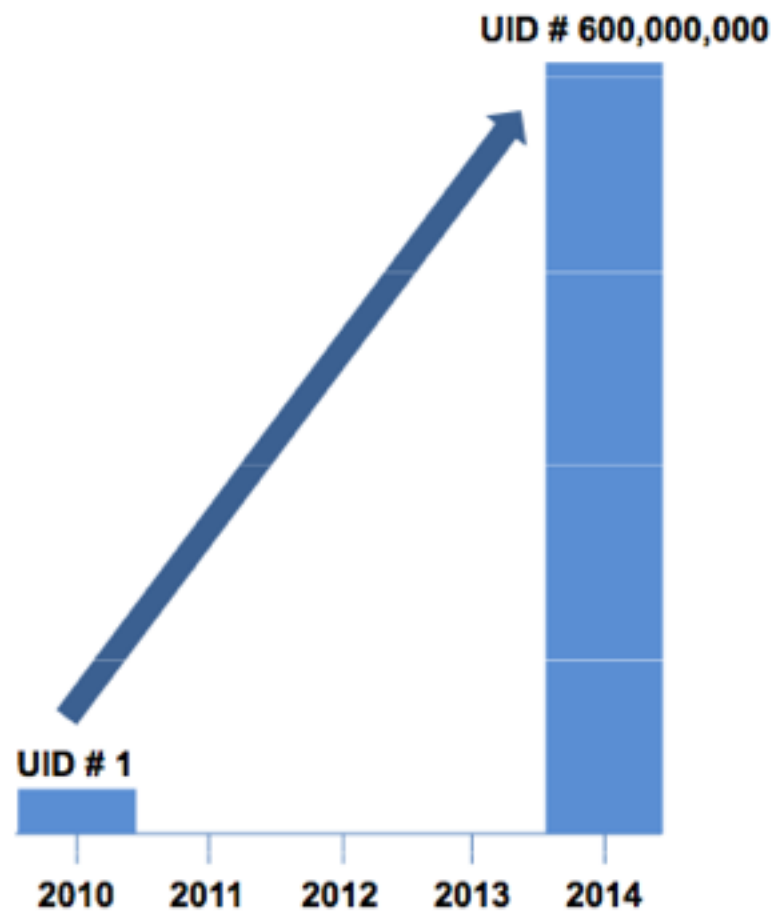




# UID Enrollment Goals



## Ambitious Targets



July 2015: 879M enrollments  
**By December: 1 Billion**



# Recent Blowback....



OPINION

## Alarm Bells On Aadhar

Our worst privacy nightmares will come true if Aadhar is mounted without a stringent and water-tight law backing it.

ARINDAM MUKHERJEE



Creating Digital Locker services only for Aadhaar holders is a threat to the right of equality for Indian citizens, alleges Sudhir Yadav, the petitioner

## Linking voter card to Aadhaar can lead to abuse of data: Sitaram Yechury to CEC Nasim Zaidi

Yechury termed the exercise by electoral officers as “strange” and expressed concern about the possible misuse of such a database.

# Biometrics in 2015

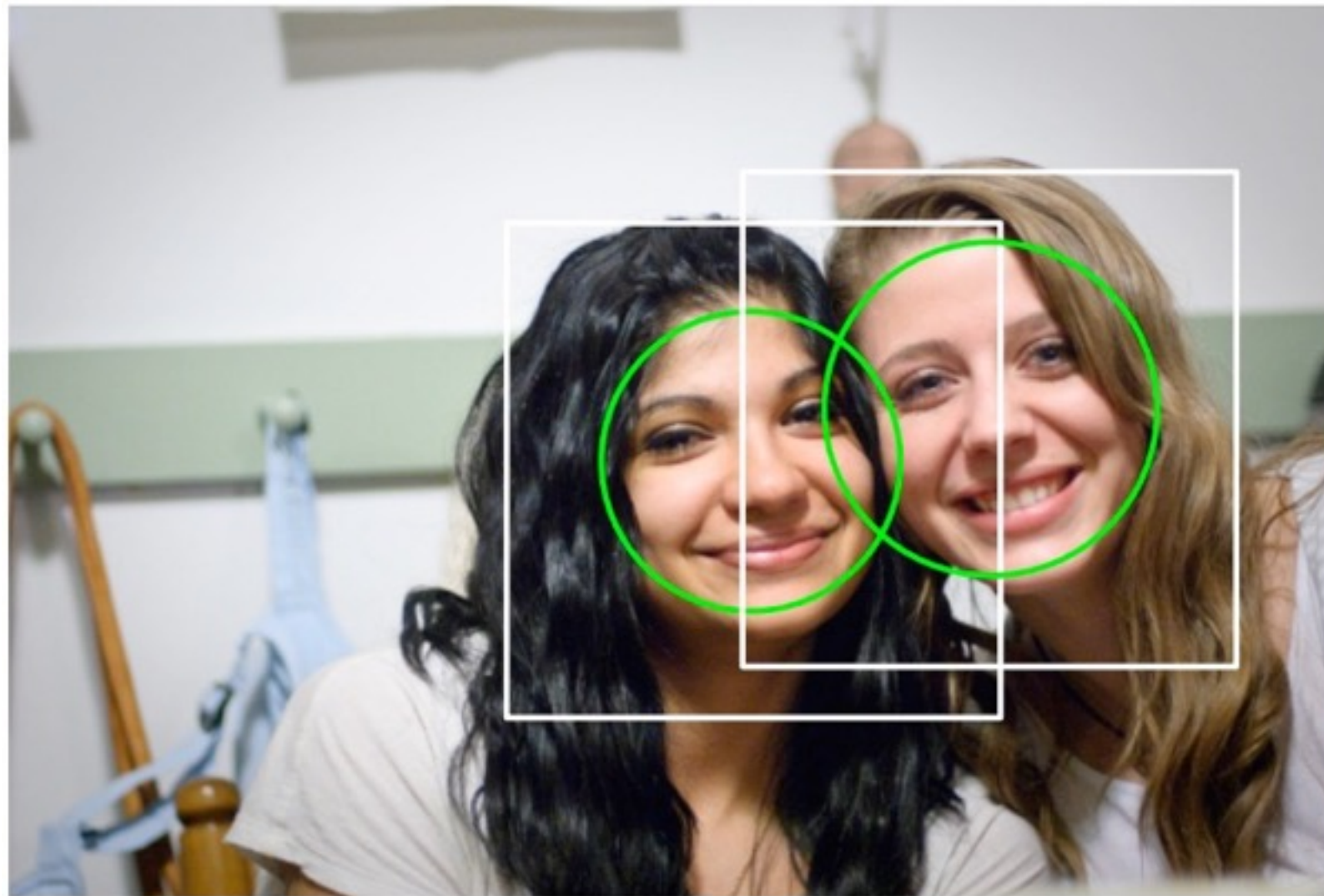


Image Credit: Flickr member wickenden / <http://vision.seas.harvard.edu/pubfig83/>



# Google

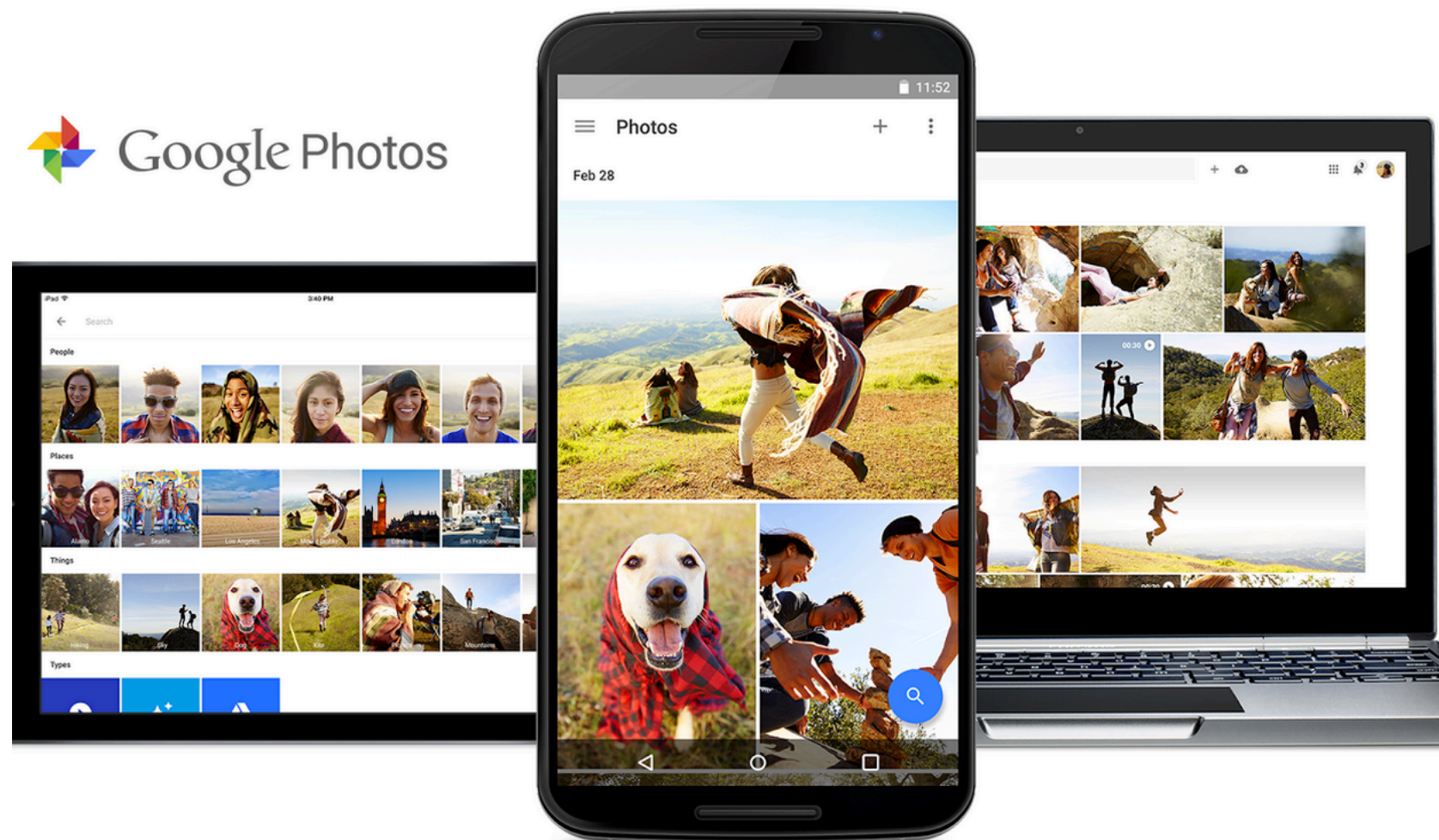


Image Credit: Google

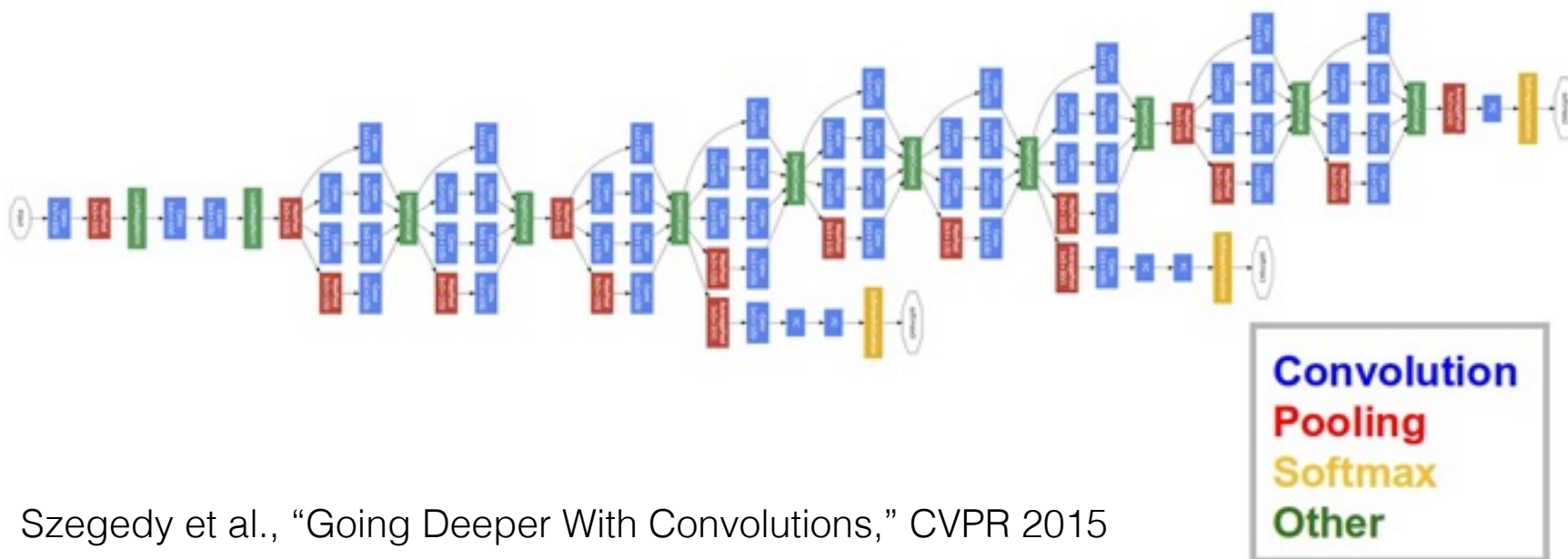


# Deep Learning



CVPR 2015: Google FaceNet. Tens of millions of training examples



Schroff et al., "FaceNet: A Unified Embedding for Face Recognition and Clustering," CVPR 2015



ILSVRC 2014: GoogLeNet. 22 Layers, 1.5M training examples

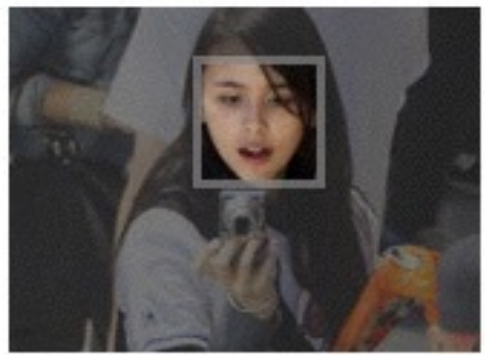





Szegedy et al., "Going Deeper With Convolutions," CVPR 2015

# Facebook

facebook  Search  Home

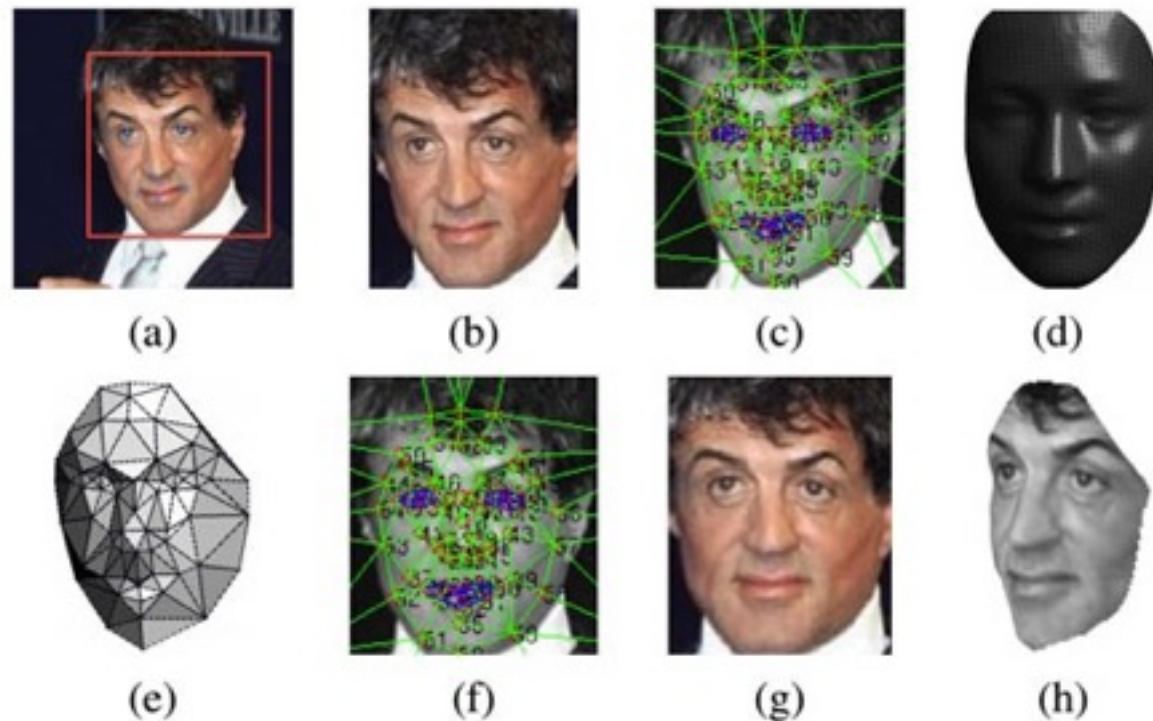
## Who's in These Photos?

The photos you uploaded were grouped automatically so you can quickly label and notify friends in these pictures. (Friends can always untag themselves.)

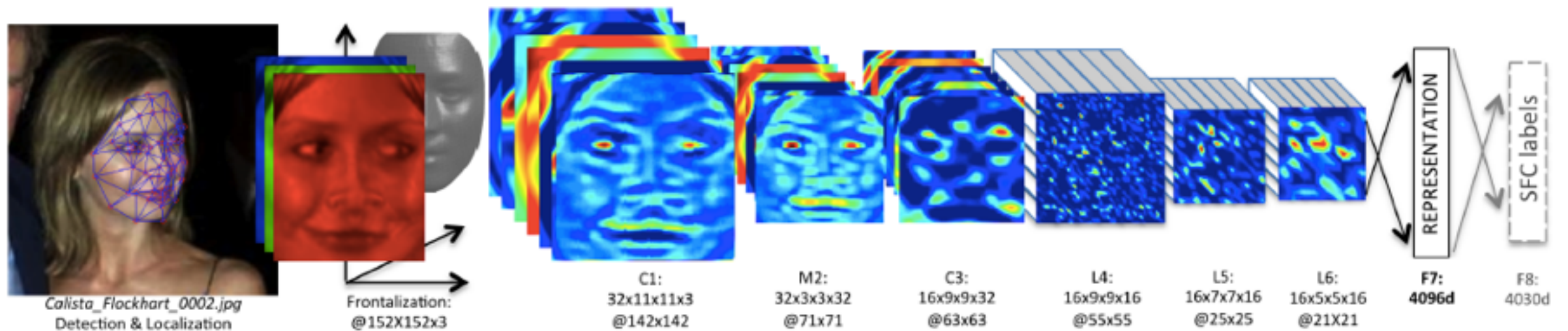
		
Who is this?	Who is this?	Who is this?
		
Who is this?	Who is this?	Who is this?



# Facebook AI Research



DeepFace:  
Good Alignment +  
Four Million Faces



# How-Old.net



Image Credit: Microsoft



# What must we be aware of?

- + Pros: efficiency, convenience, improved access, improved security
- Cons: unique identifiers, support unwarranted surveillance, difficulty with storage, questionable security



# Function Creep

“The expansion of a process or system, where data collected for one specific purpose are subsequently used for another unintended or unauthorized purpose”

Most familiar example in the US: SSN



# Function Creep and Biometrics

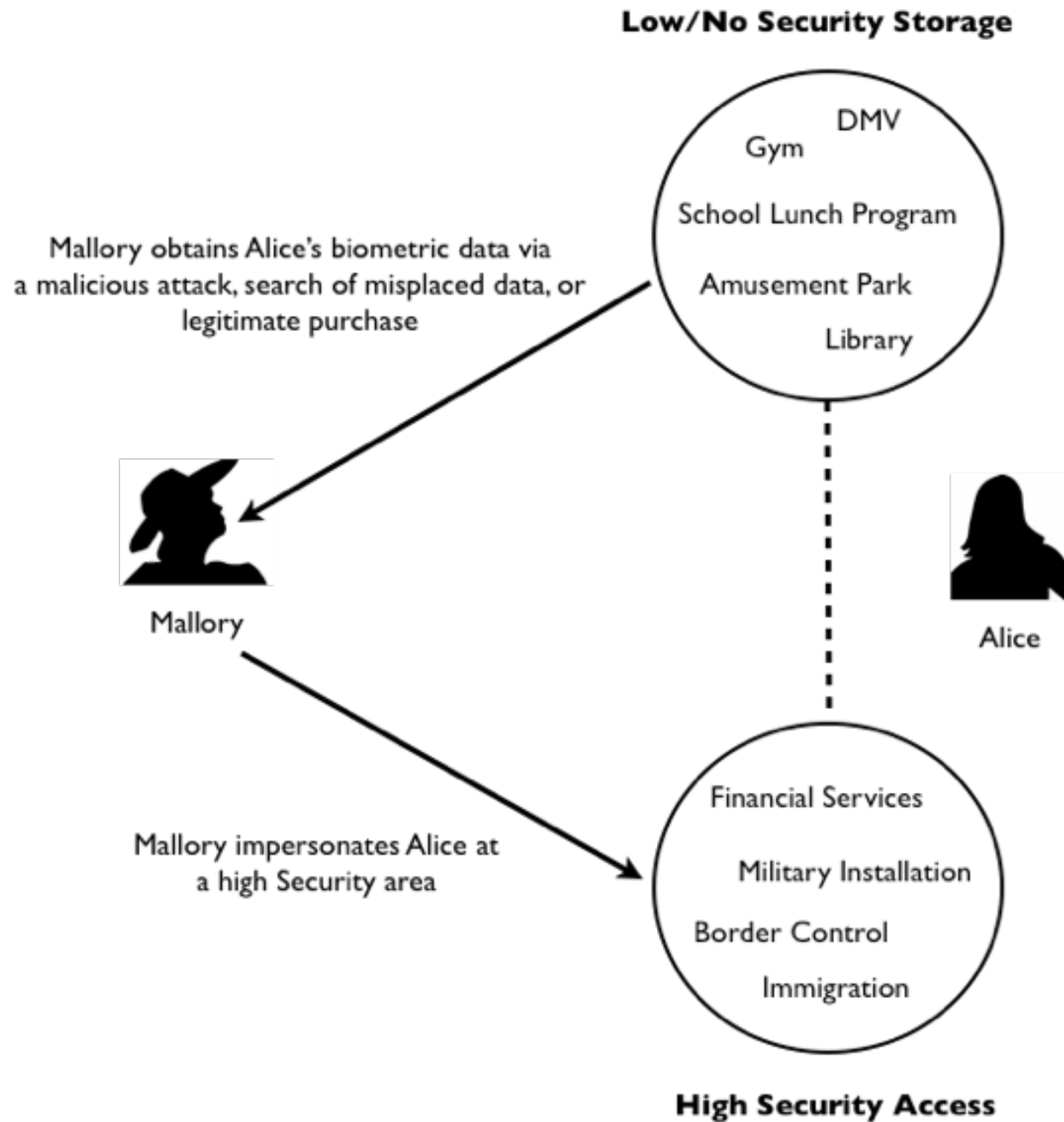
In 2001, Colorado tried to sell face fingerprint data collected by its DMV



Driver's License Section © BY-SA 2.0 Jeffrey Beall



# The Biometric Dilemma



# Who is watching out for your data?



# Biometrics, Body, and Identity

- The same biometrics can be used in different ways
  - Identification, genetics research, medical monitoring, ethnic categorization
- Serious risk for discrimination based on what is measured from the human body





# Informatization of the Body

- Baudrillard\* describes a process of *dematerialization*:
  - Thing → Commodity → Sign → Information



What does this say about the potential for biometrics to dehumanize the body and offend human dignity?

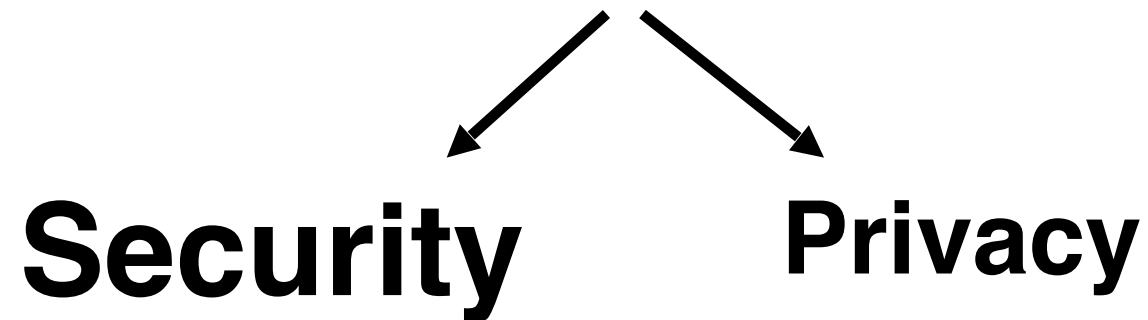
# Security is a Two-way Street



- Biometrics can be incorporated into large security frameworks
  - Identity Assurance
- Biometrics suffer from the same flaws as traditional software security systems (and more!)
  - Limitations of Pattern Recognition

# Security and Privacy

An Inherent Trade-Off ?



Deterrence,  
Accuracy,  
Efficiency,  
Usefulness



Identity protection,  
Attribute protection,  
Limit inference,  
Limit abuse



# Definitions

# Deconstructing “Biometrics”

“the use of physical or behavioral properties of human beings for automatic identity recognition”

- Something characteristic **only** to me
  - (e.g., my face, my handwriting, my voice)
- **Not** something I know
  - (e.g., a password or PIN)
- **Not** something I have
  - (e.g., a key or authentication token)

# Deconstructing “Biometrics”

“the use of physical or behavioral properties of human beings for automatic identity recognition”

- We need a **living subject**

# Pop Quiz

Which fingerprint is the real one?



Latex



Wood Glue



Gelatine



# Deconstructing “Biometrics”

“the use of physical or behavioral properties of human beings for automatic identity recognition”



Image Credit: Frank Couch/Birmingham News

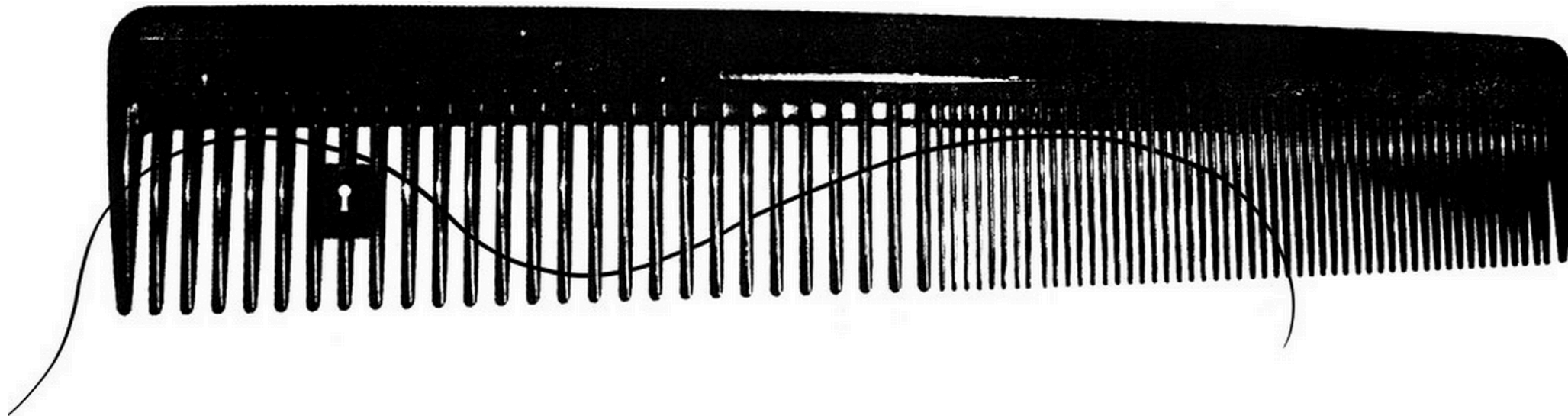
Why do we want computers to do this?

- High throughput
- Repeatability
- Predictability

# How reliable are humans?

## Fix the Flaws in Forensic Science

By ERIC S. LANDER APRIL 21, 2015

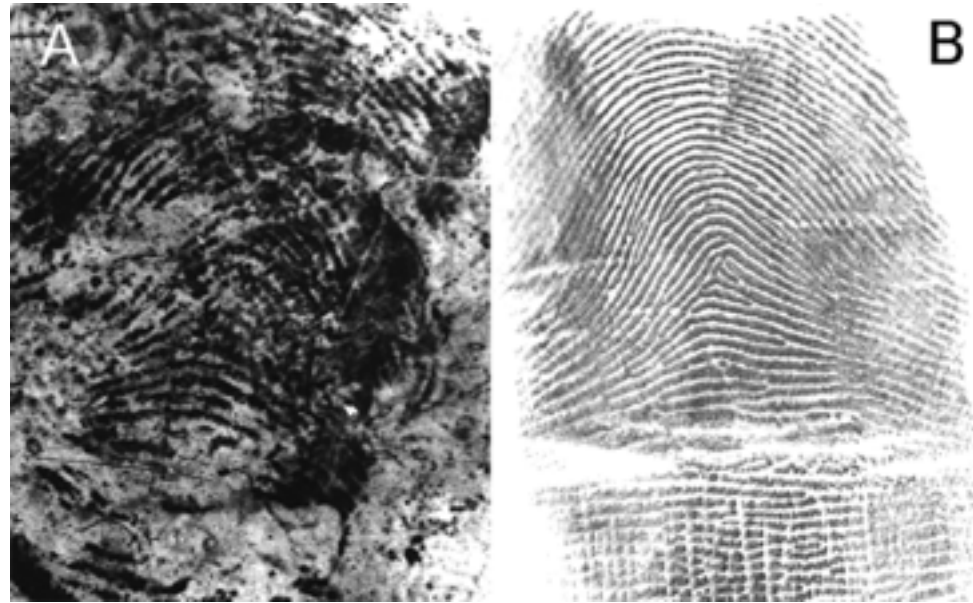


Mike McQuade

THE [F.B.I.](#) stunned the legal community on Monday with its acknowledgment that testimony by its forensic scientists about hair identification was scientifically indefensible in nearly every one of more than 250 cases reviewed. But the conclusion should come as no surprise to scientists. It is the culmination of a collision between law and science . . .

# Mayfield Case

Latent print  
suspected to  
belong to  
Madrid bomber



Print belonging  
to Brandon  
Mayfield

Image Credit: Saks and Koehler, *Science*, 309 (5736), 2005

## Statement on Brandon Mayfield Case

---

**Washington, D.C.**

May 24, 2004

**FBI National Press Office**

(202) 324-3691

Upon review it was determined that the FBI identification was based on an image of substandard quality, which was particularly problematic because of the remarkable number of points of similarity between Mr. Mayfield's prints and the print details in the images submitted to the FBI.

The FBI apologizes to Mr. Mayfield and his family for the hardships that this matter has caused.



# Biometric Recognition Types



## Positive Recognition

A sample represents a subject known to the system (i.e., already registered)



## Negative Recognition

A sample represents a subject unknown to the system (i.e., not yet registered)

# Biometric Modality

- A **single** physical or behavioral property we use for biometric recognition

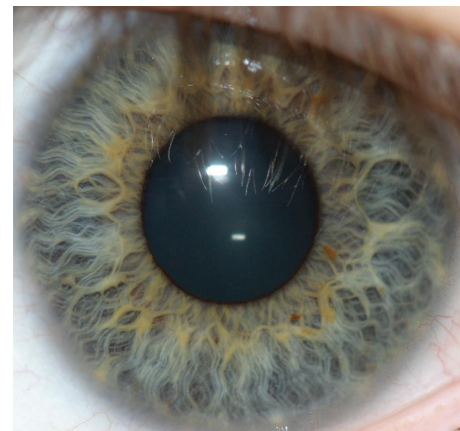


Table I. Comparison of different biometric systems according to [Jain et al. 2004]

●: high, ⊙: medium, ○: low

	<b>Universality</b>	<b>Distinctiveness</b>	<b>Permanence</b>	<b>Collectability</b>	<b>Performance</b>	<b>Acceptability</b>	<b>Circumvention</b>
<b>DNA</b>	●	●	●	○	●	○	○
<b>Ear</b>	⊙	⊙	●	⊙	⊙	●	⊙
<b>Face</b>	●	○	⊙	●	○	●	●
<b>Facial thermogram</b>	●	●	○	●	⊙	●	○
<b>Fingerprint</b>	⊙	●	●	⊙	●	⊙	⊙
<b>Gait</b>	⊙	○	○	●	○	●	⊙
<b>Hand geometry</b>	⊙	⊙	⊙	●	⊙	⊙	⊙
<b>Hand vein</b>	⊙	⊙	⊙	⊙	⊙	⊙	○
<b>Iris</b>	●	●	●	⊙	●	○	○
<b>Keystroke</b>	○	○	○	⊙	○	⊙	⊙
<b>Odor</b>	●	●	●	○	○	⊙	○
<b>Palmprint</b>	⊙	●	●	⊙	●	⊙	⊙
<b>Retina</b>	●	●	⊙	○	●	○	○
<b>Signature</b>	○	○	○	●	○	●	●
<b>Voice</b>	⊙	○	○	⊙	○	●	●



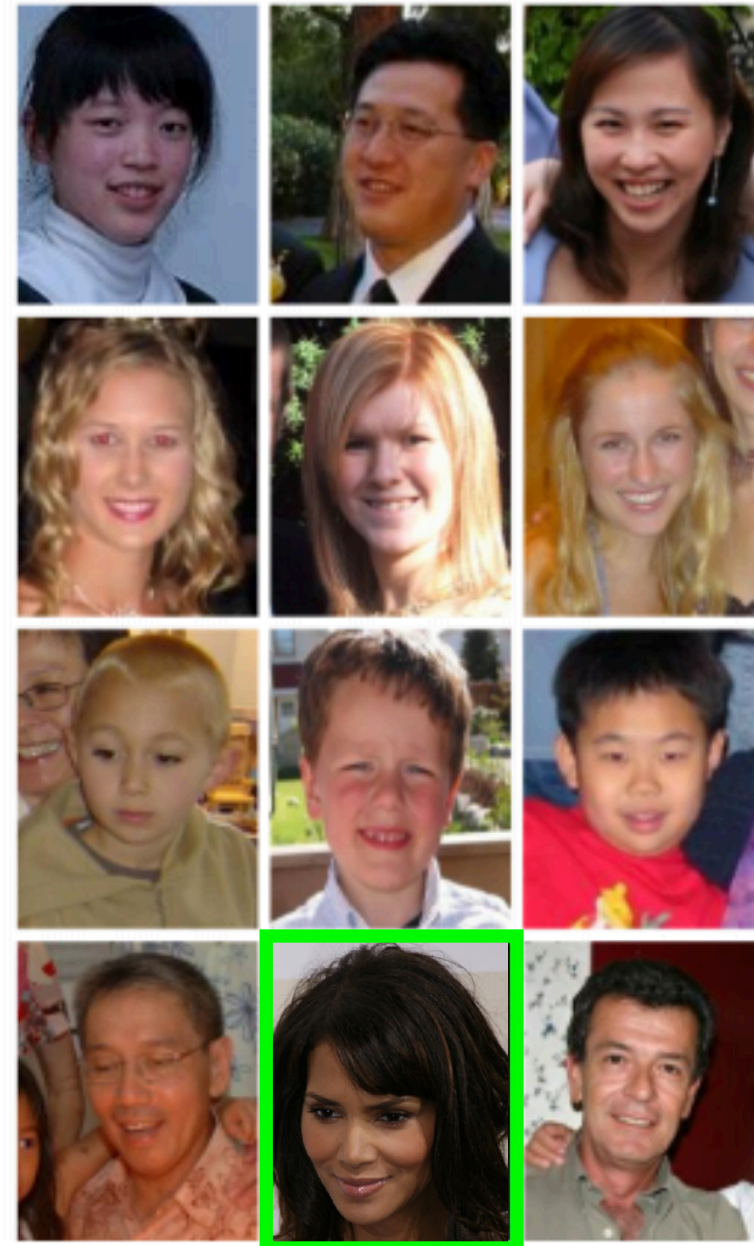
# Probe and Gallery

Gallery: A collection of enrolled templates

Probe: A sample presented to a biometric system



“Who is this?”



“Halle Barry”

# Authentication Types: Pair Matching

Do these two images match?

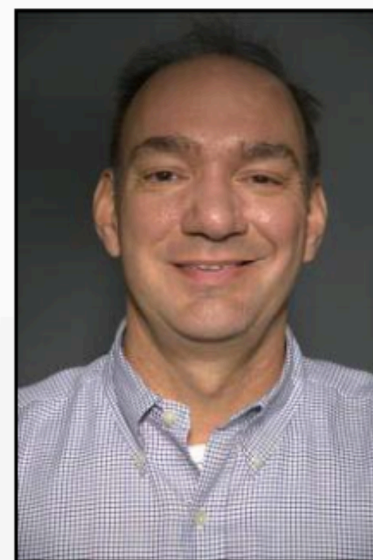


Answer: Yes or No

# Authentication Types: Verification

Does this sample of Kevin Bowyer match the one in our system?

New  
Sample



Stored  
Image

Answer: Verified or Not Verified



# Authentication Types: Identification

Does this person exist in our system?



Answer: Identified or Not Identified



# Authentication Types: Negative Authentication

- Negative Verification: I'm not the subject  $X$
- Negative Identification: I'm not a member of group  $X$

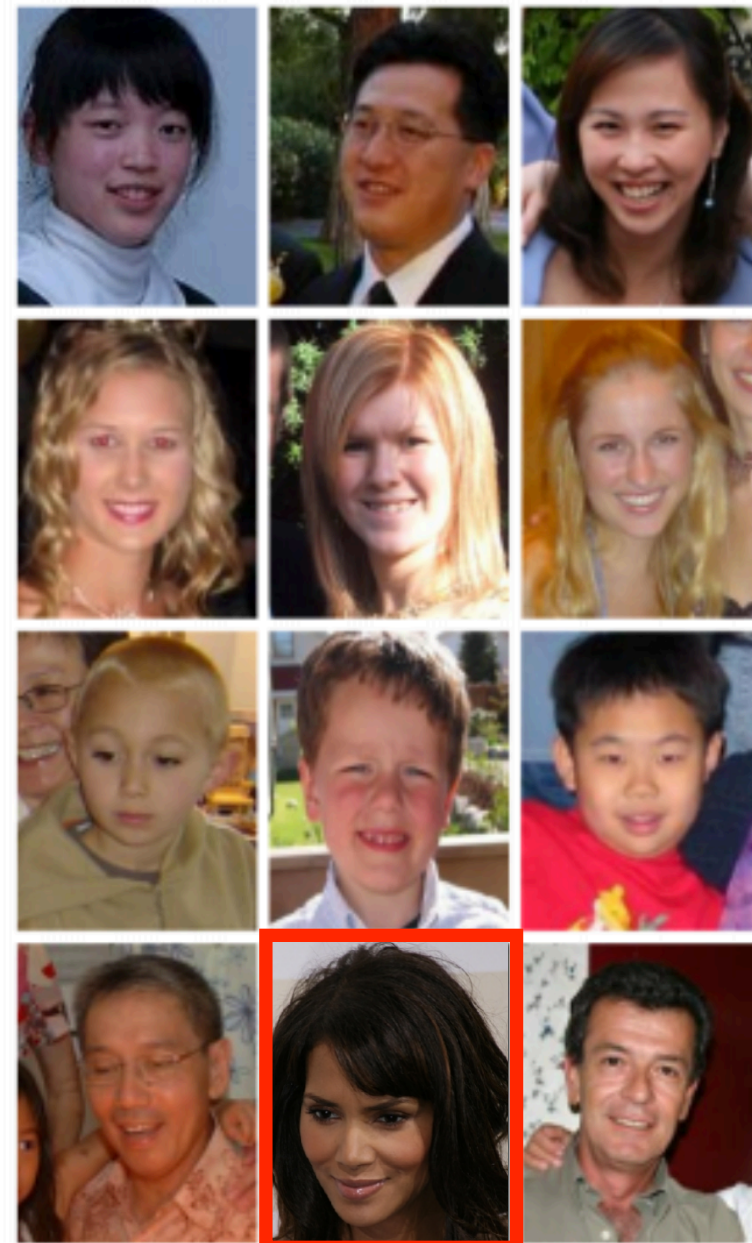
# Authentication Types: Deduplication

Known Records



~~New User~~

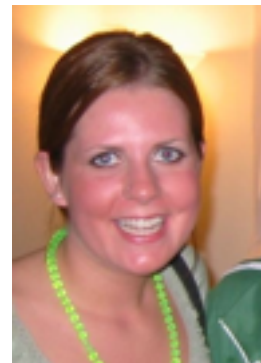
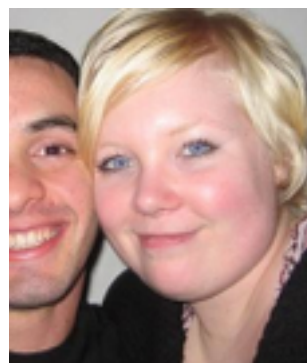
We know you!



# Search



“Find all instances of this person”



Top 10 Hits

# Recognition Pipeline

Enrollment: New user comes in

Acquisition  $\Rightarrow$  Feature Extraction  $\Rightarrow$  Template Generation

Recognition: We need to make a decision

Acquisition  $\Rightarrow$  Feature Extraction  $\Rightarrow$  Matching  $\Rightarrow$  Labeling



# Recognition Pipeline: Acquisition

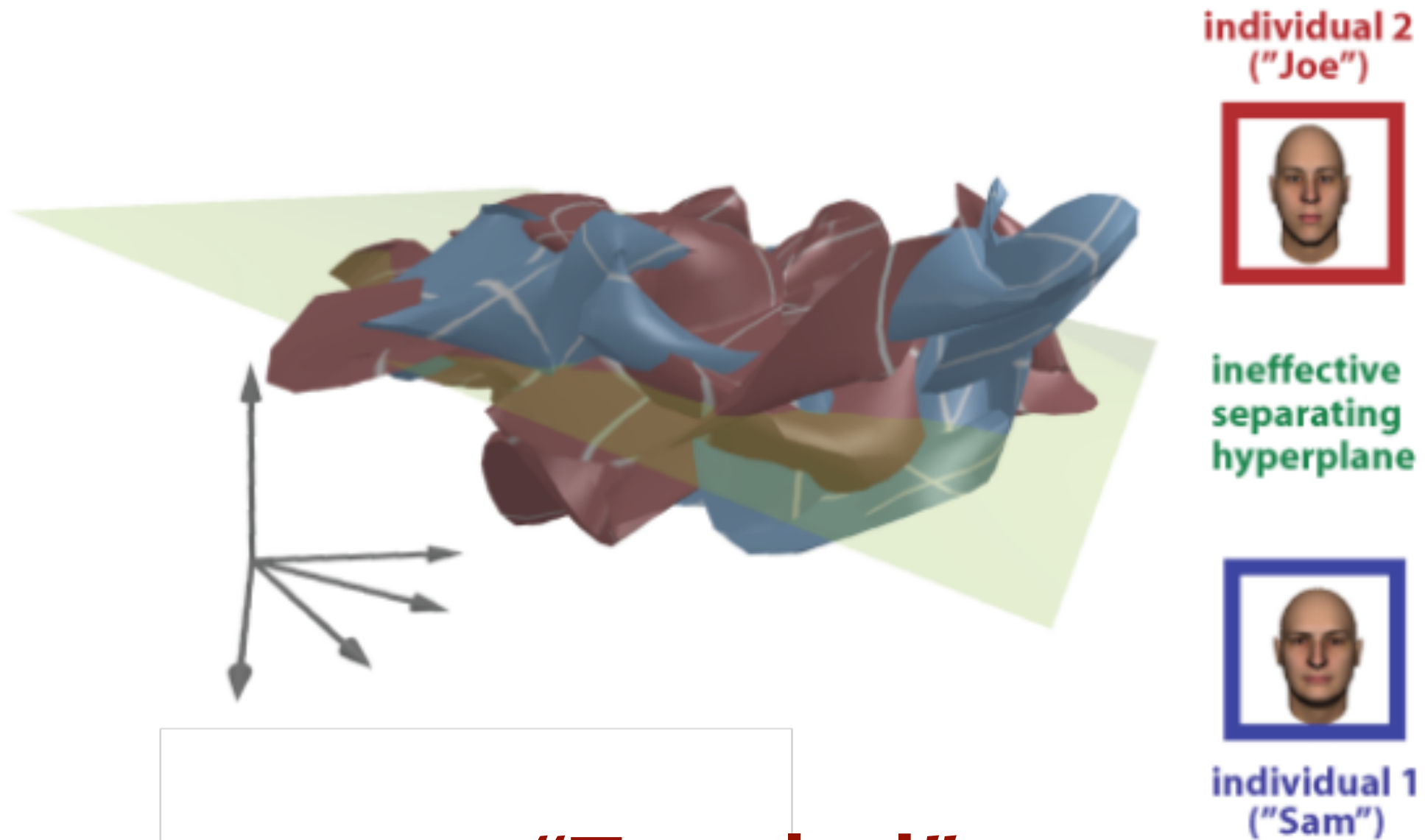
A biometric sample is the raw or pre-processed data collected from a subject by a sensor



Image Credit: NIST, First MBGC Kick-off Meeting

Let  $I \in \mathbb{R}^v$  be an image  
 $v$  = number of pixels

# pixel space



**"Tangled"**

Example courtesy of D. D. Cox

Individual 2  
(red)

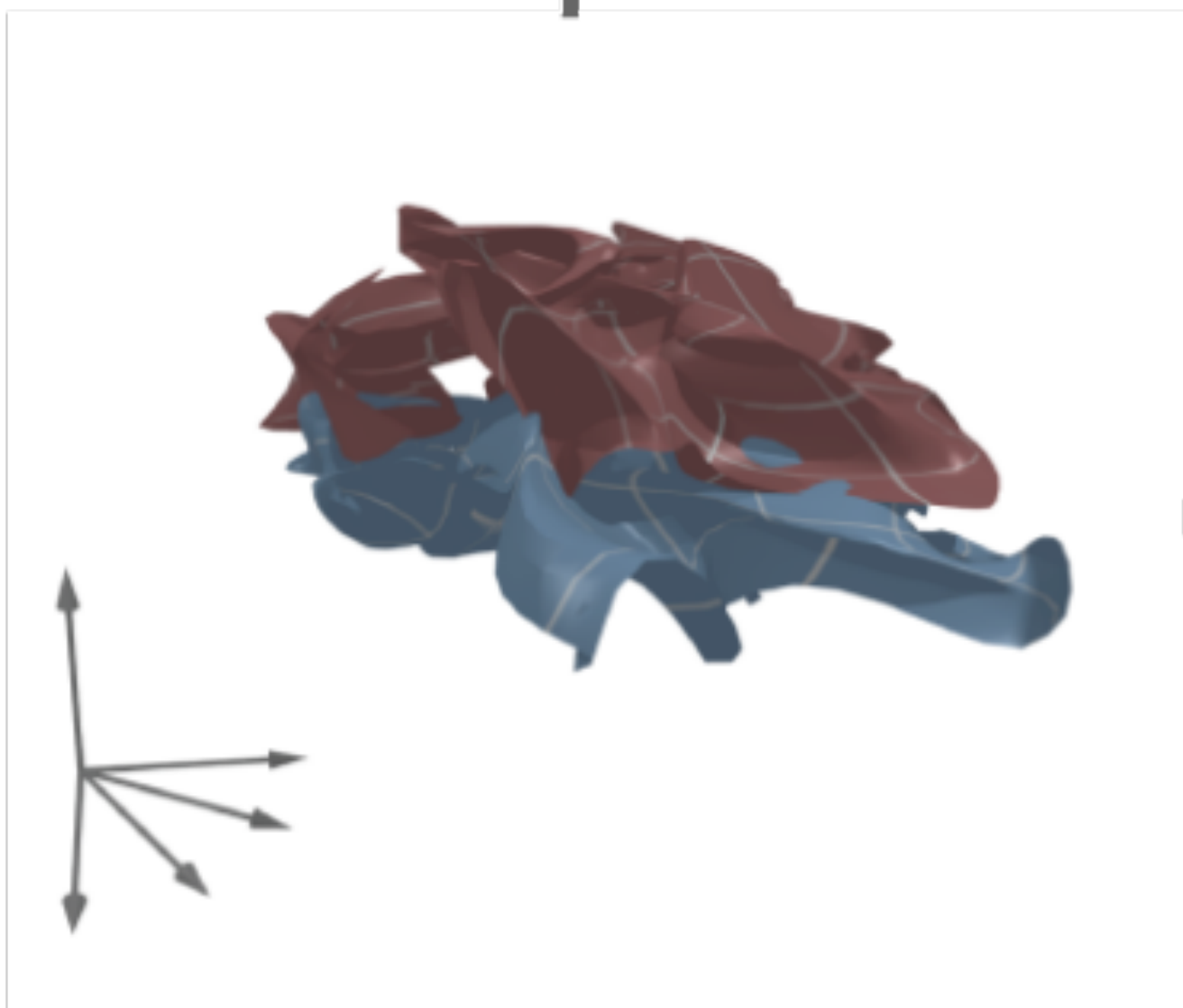


Active  
plane

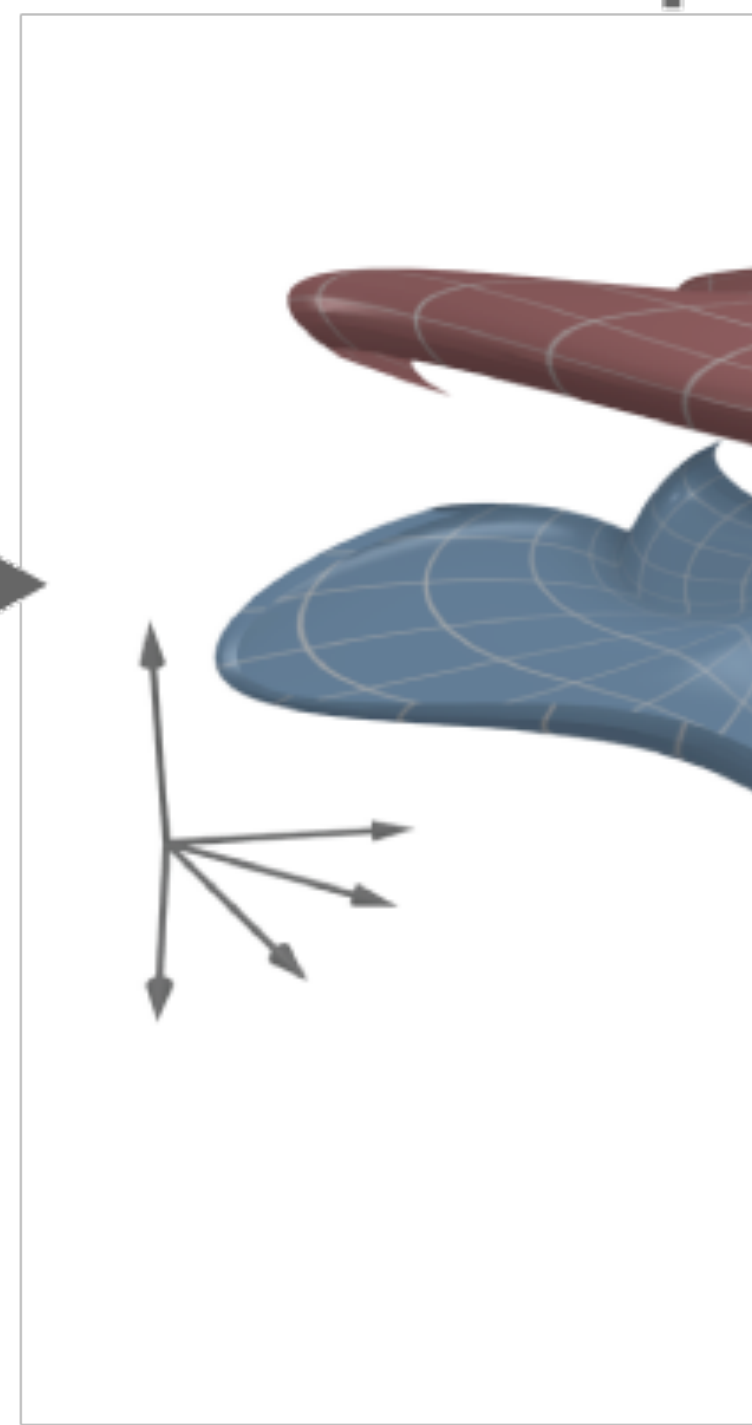


Individual 1  
(blue)

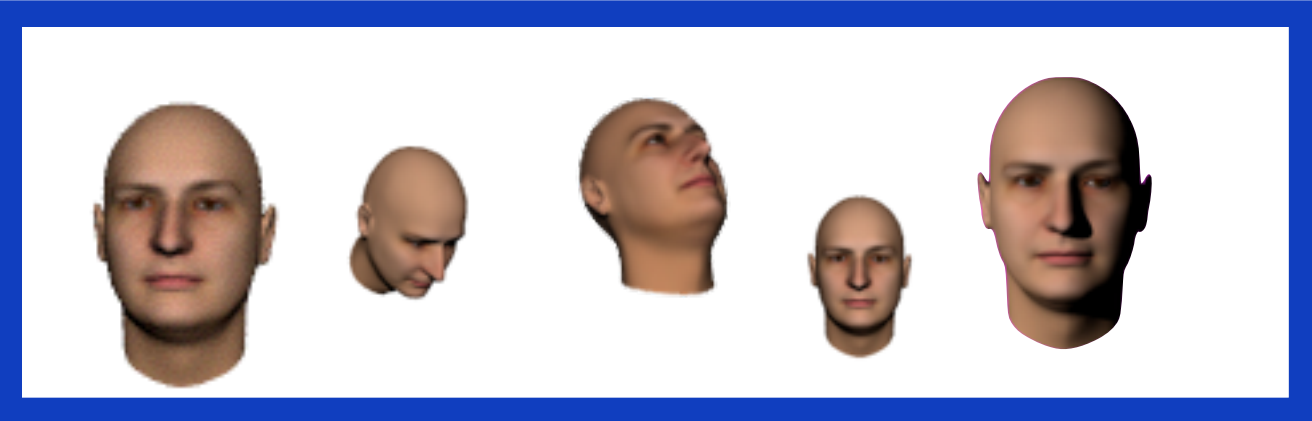
# V1 space



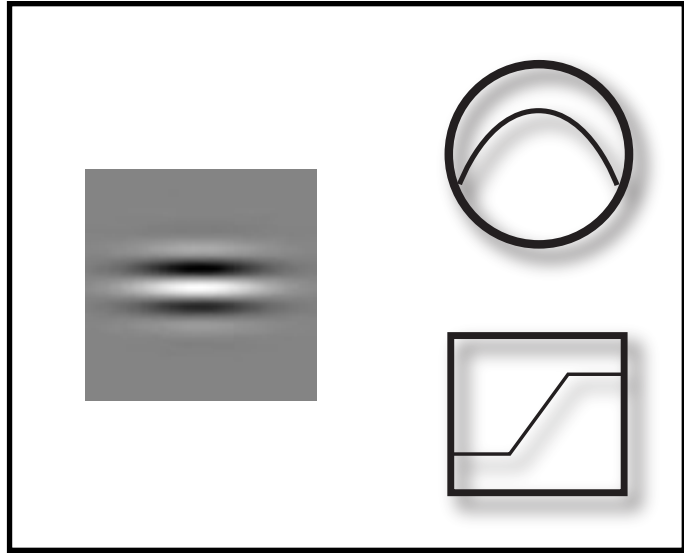
# IT space



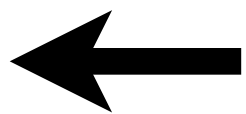
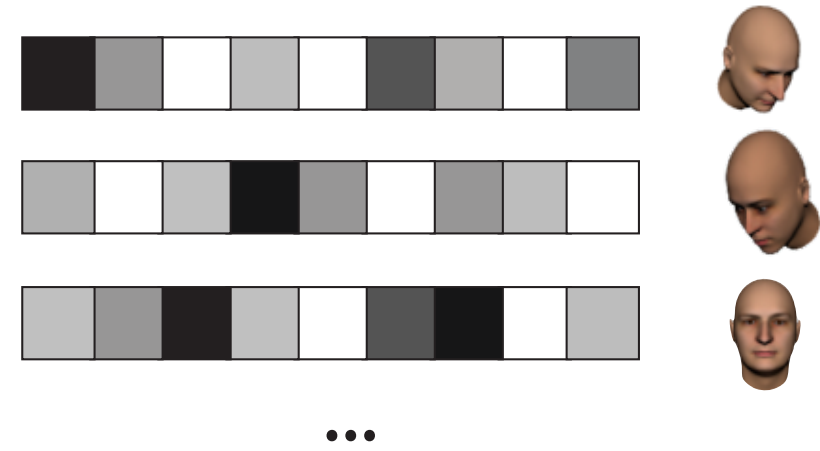
“Untangled”



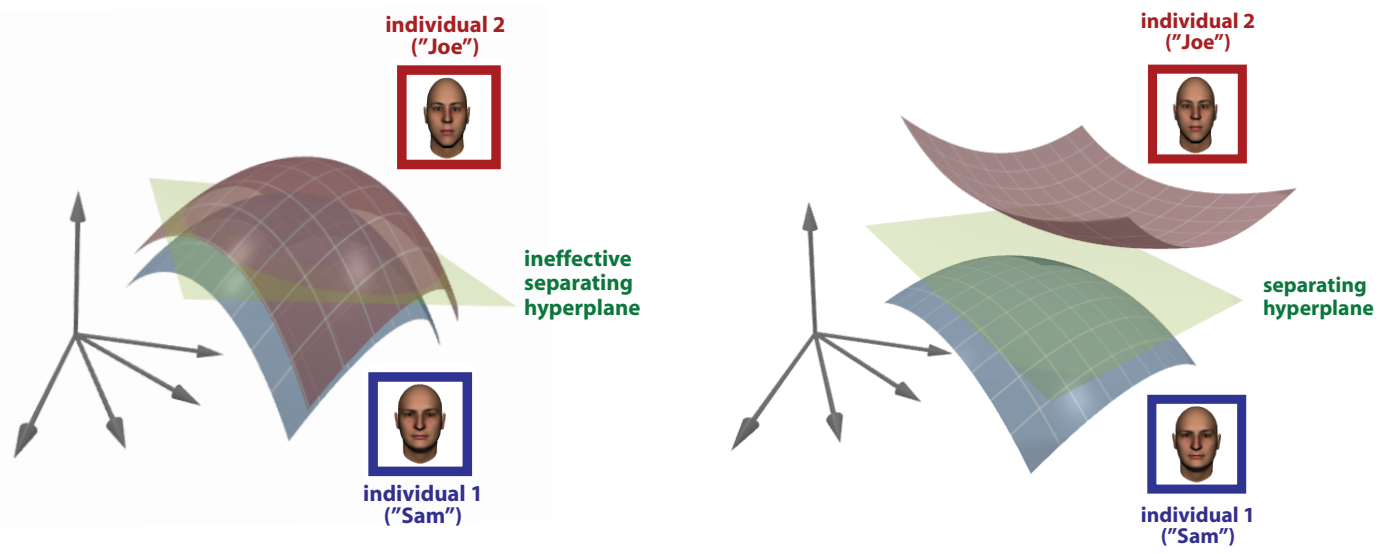
# Model



# Representation



# Visualize Best Projections

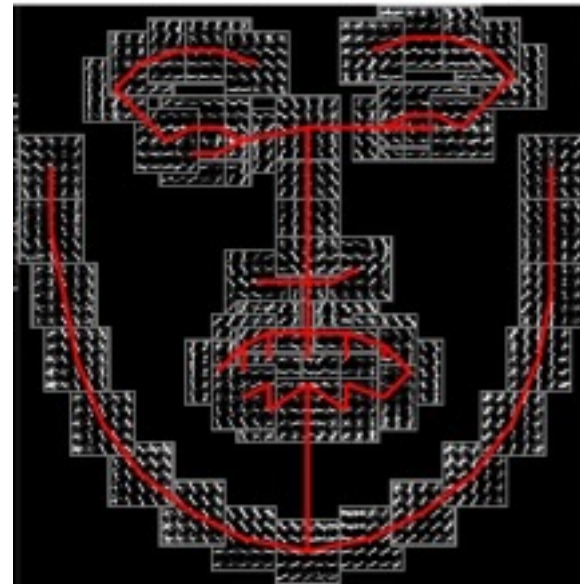




# Recognition Pipeline: Features



$F$



Zhu and Ramanan CVPR 2012

$$x = F(I, \varphi_F), x \in \mathbb{R}^D$$

feature extractor

assumptions

$y = \text{label (if we know it)}$

# Recognition Pipeline: Templates

class =  $y \in \mathbb{N}$

labeled training data =  $X_y = \{(x_1, y_1), \dots\}$

number of feature vectors =  $m = |\{(x_1, y_1), \dots\}| \geq 1$

model specific assumptions =  $\varphi_M$

model =  $M_y = f(X_y, \varphi_M)$

If the template is a learned model,  $m > 1$

# Recognition Pipeline: Matching

Matching: compare  $x_0$  to  $M_y$

$$s_y = R(x_0, M_y(X_y, \varphi_M), \varphi_R), s_y \in \mathbb{R}$$

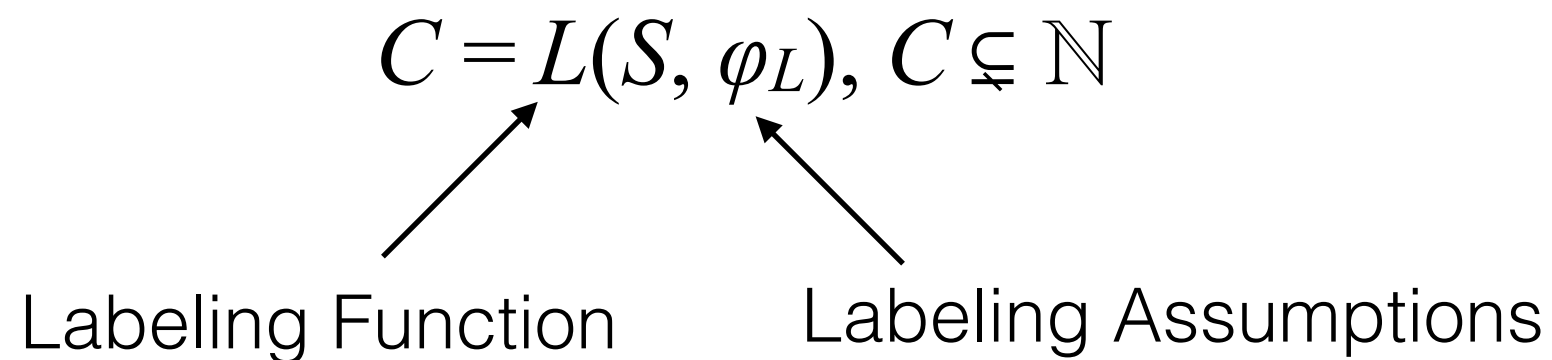
Similarity Score

Recog. Function

Matching Assumptions

# Recognition Pipeline: Labeling

Matching: assume  $x_0$  was compared to  $n$  models  $\{M_1, \dots\}$ ,  $n \geq 1$



Ranked set of labels =  $C = \{y_1^*, \dots\}$

Non-match label =  $y_0^*$



# Enrollment from the user's perspective

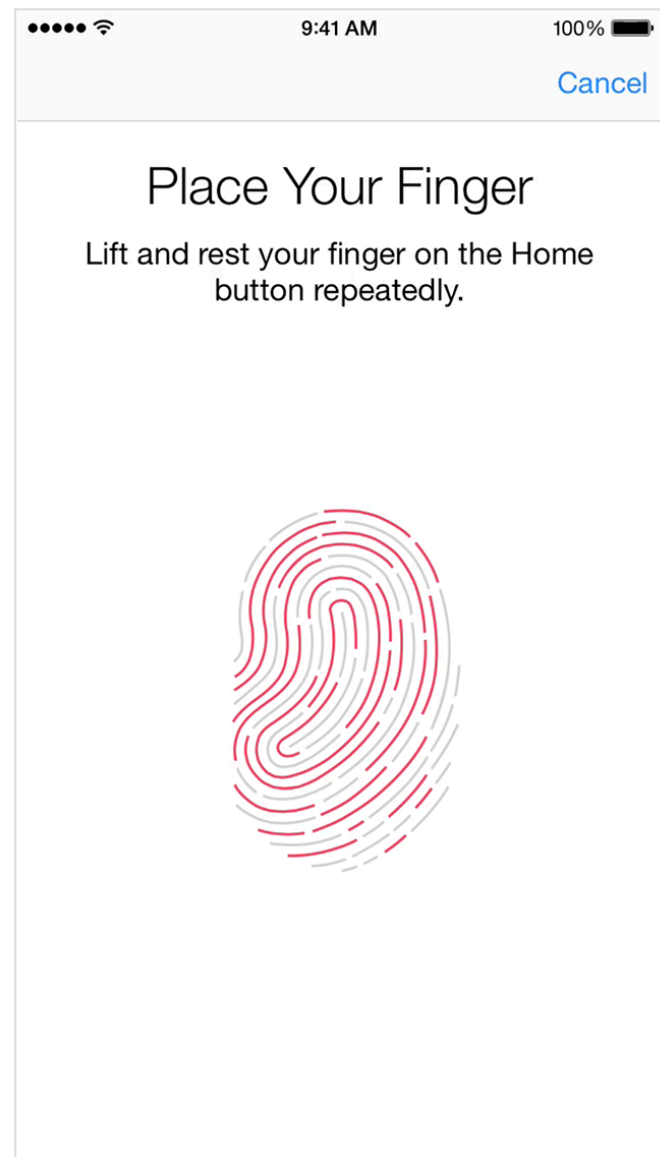


Image Credit: Apple, Inc.

## Multiple measurements

- Quality Control
- Select Best Samples
- Merge Samples

# Enrollment from the security engineer's perspective

- Is meta-data associated with the record?
- Are multiple templates stored for a user?
- Operator supervision?
- How is the template stored?
  - Encryption
  - Template Protection

# Authentication from the user's perspective

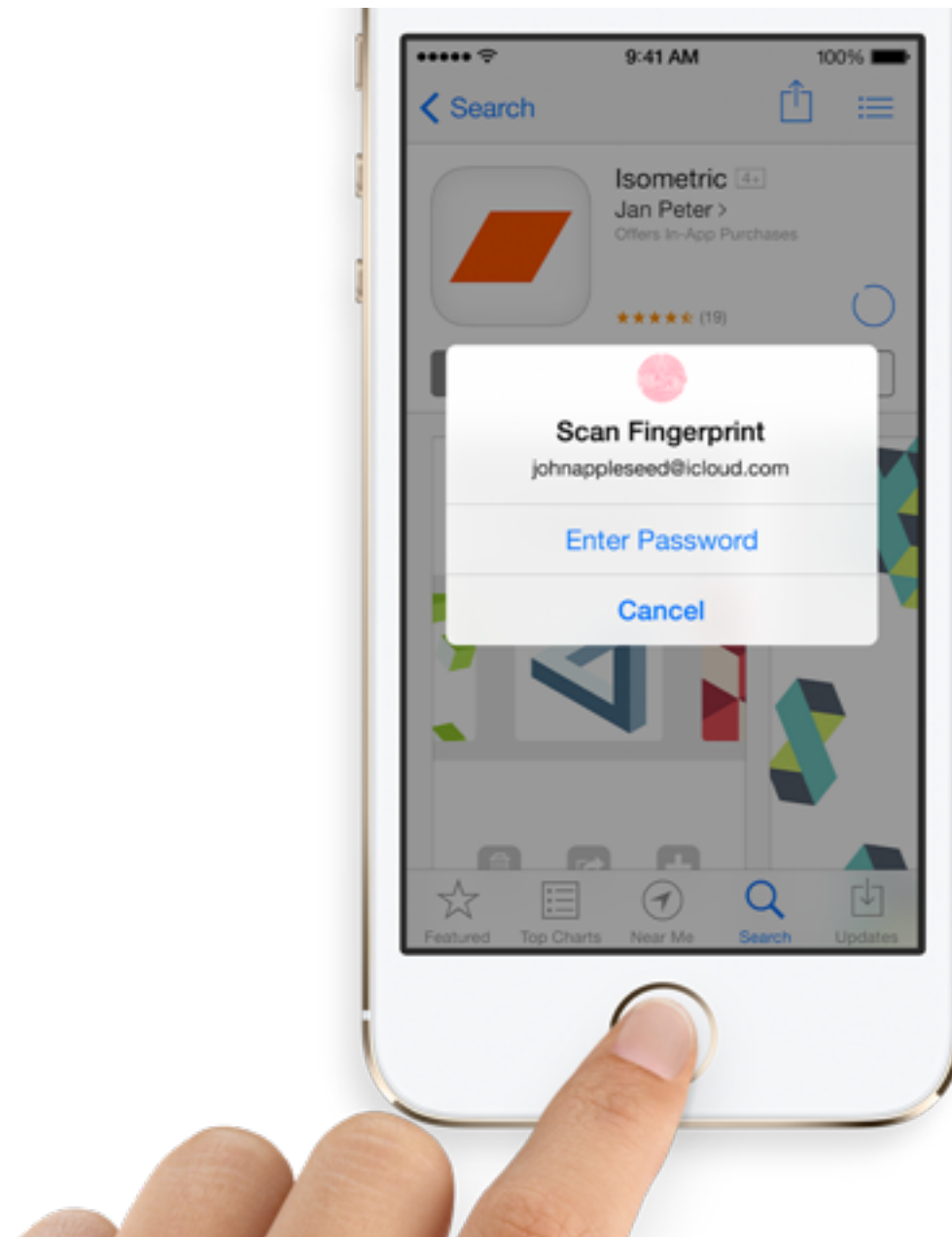


Image Credit: C. Zibreg, idownloadblog.com

# Authentication from the security engineer's perspective

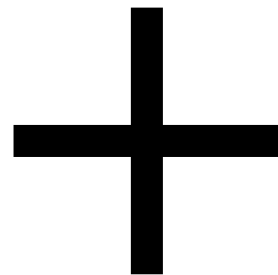
- How is the stored template retrieved?
  - On device
  - Local server
  - Cloud
- Operational matching threshold?
- How many attempts?
- Speed vs. Security Tradeoff?
- Auditing?



# Multi-Factor Authentication



Fingerprint scanner in Tel Aviv © BY 3.0 David Shankbone

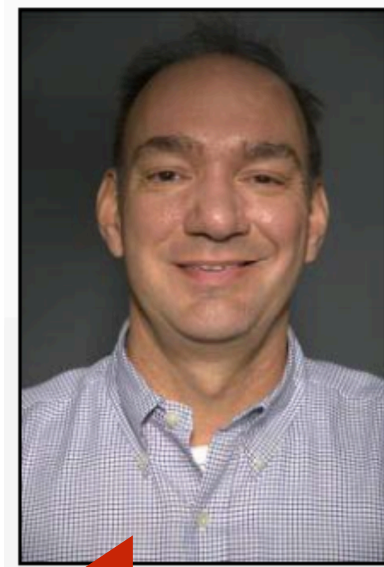


# Errors and Decision Making

# Error Statistics

False Match (Type I Error): an impostor sample matched a reference template

Impostor

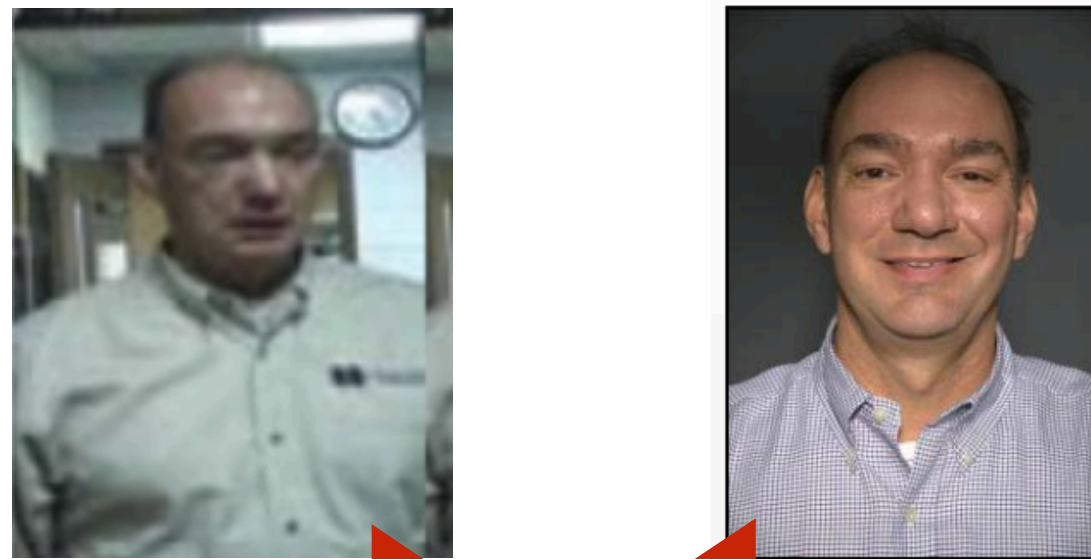


Decision: Match



# Error Statistics

False Non-match (Type II Error): a genuine sample did not match a reference template



Decision: ~~non-match~~



# Decisions

Similarity Score: Higher is better

Distance Score: Lower is better (0 for self match)

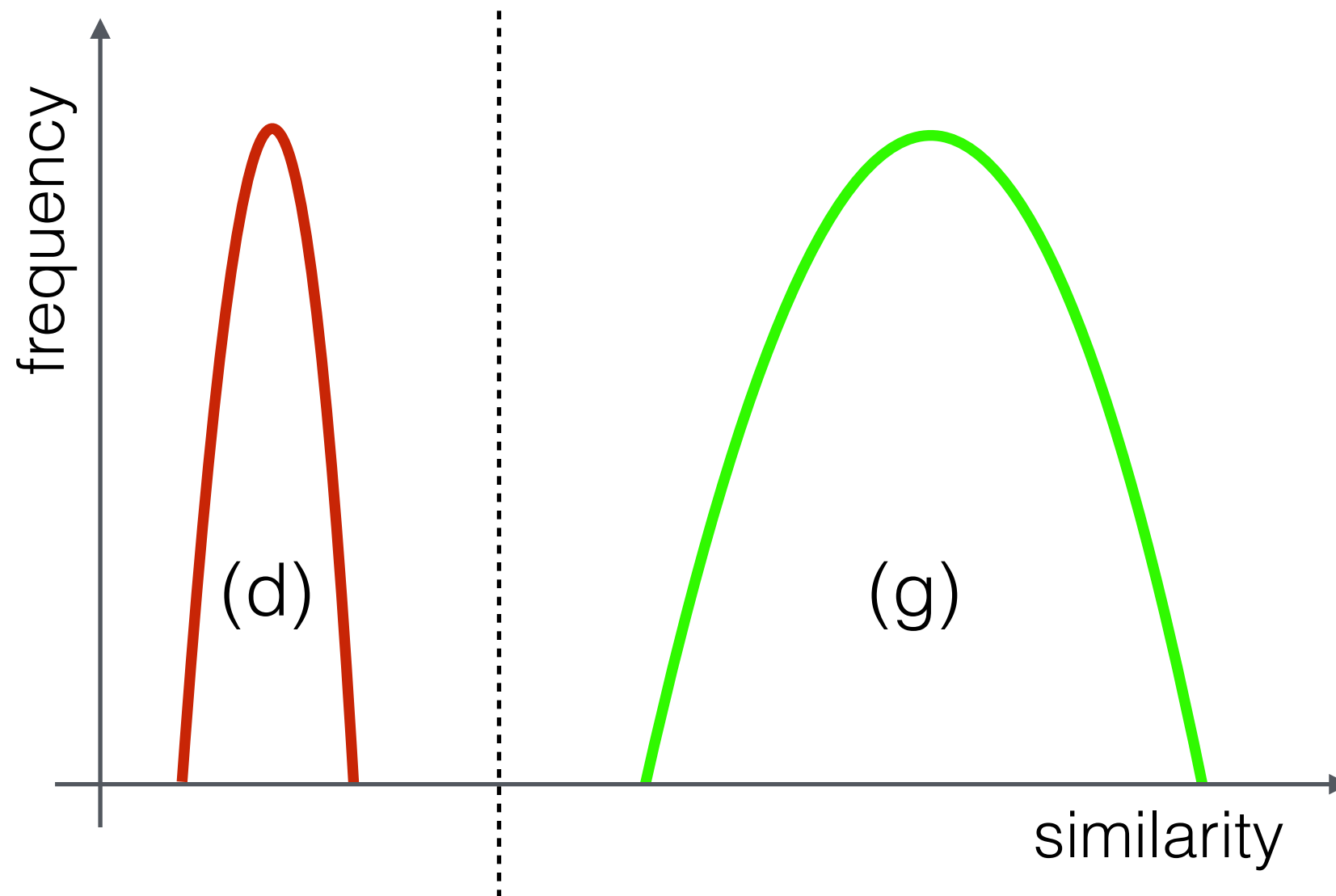
Decision Threshold:  $\tau$

Similarity Score Match:  $s_y > \tau$

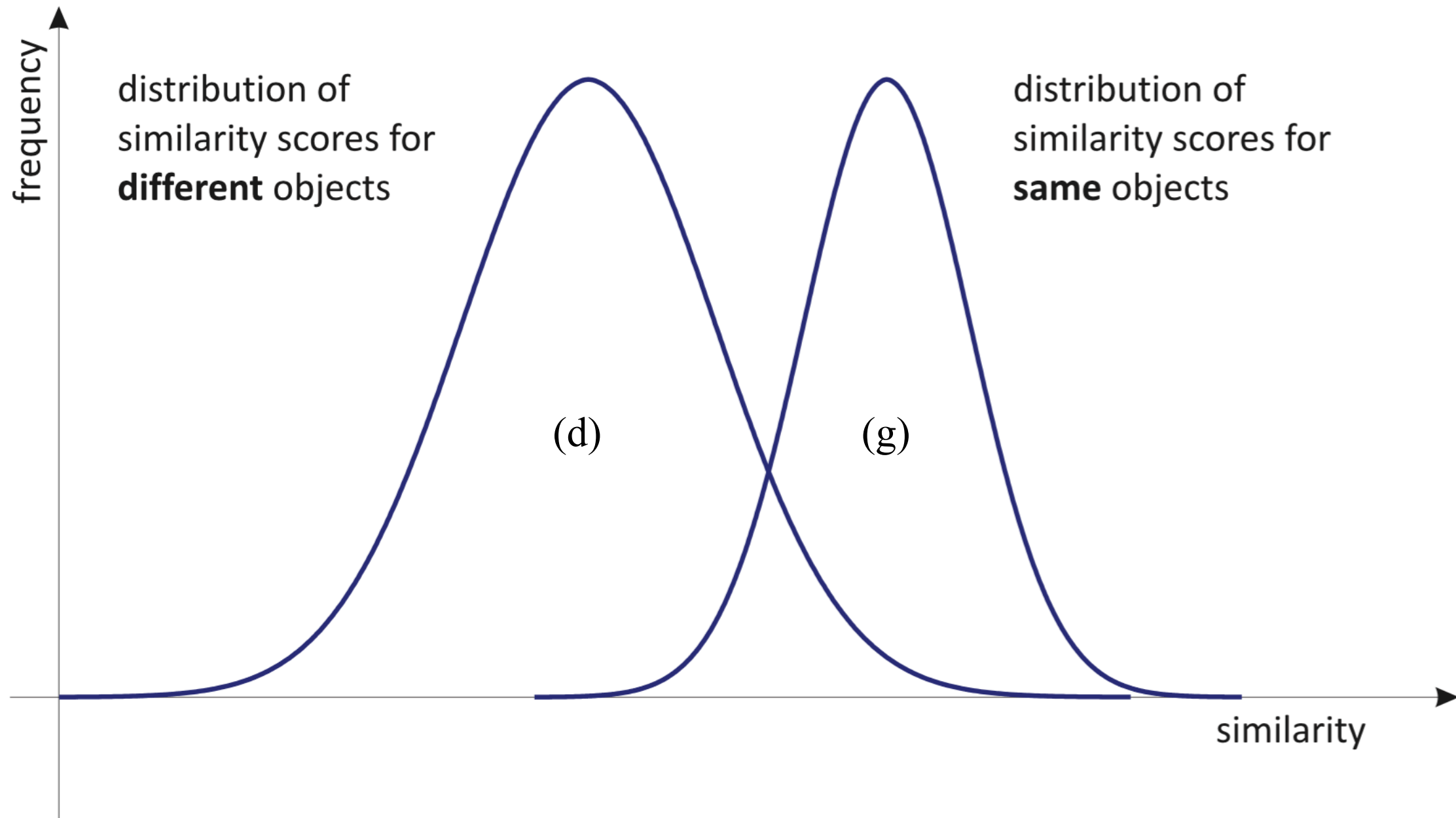
Distance Score Match:  $s_y < \tau$

# Score Distributions

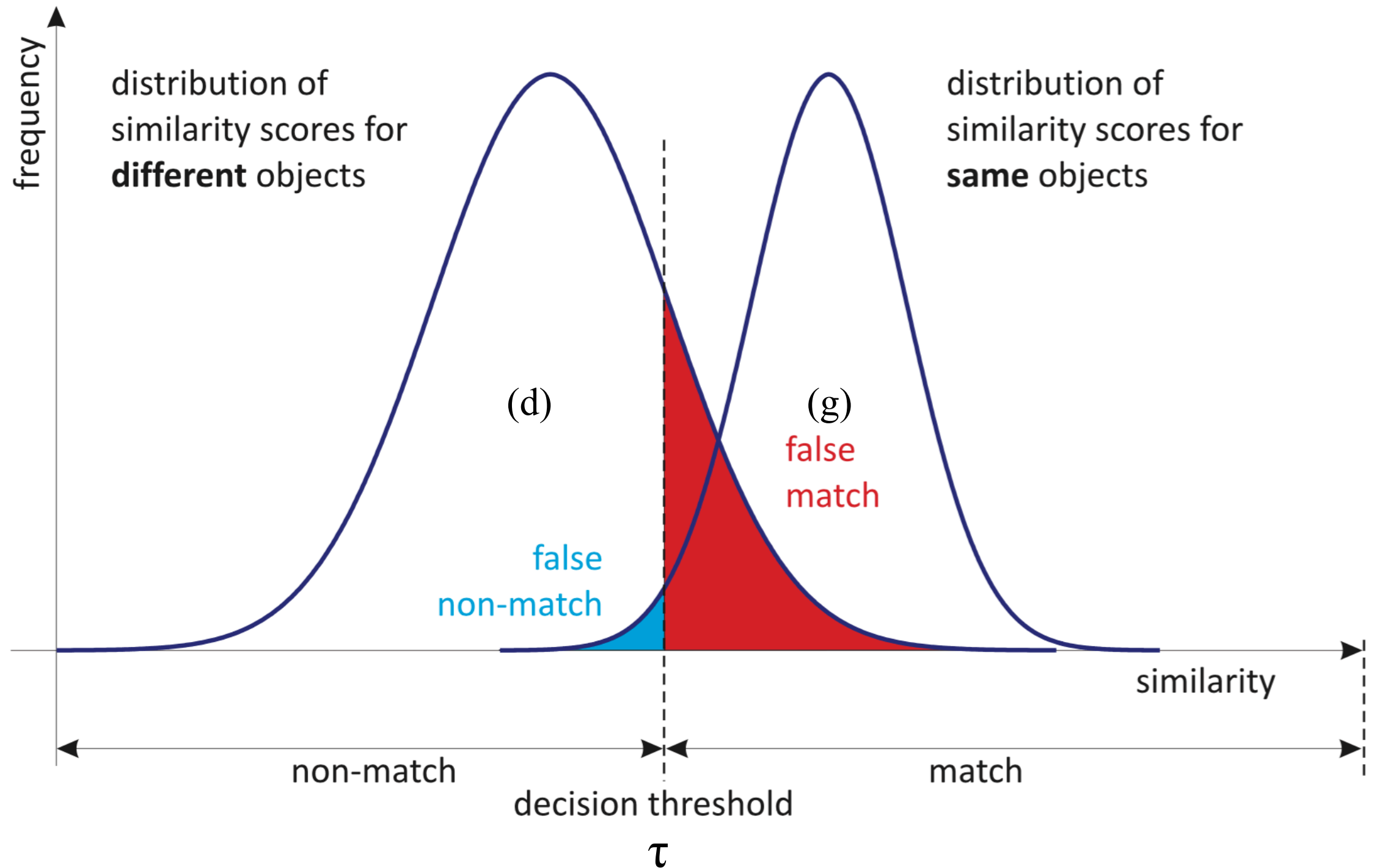
Ideal World: different (d) and same (g)  
score distributions well-separated



# Score Distributions



# Score Distributions



# False Non-Match Rate

If we know  $g$ :

$$g_{\text{FNM}}(\tau) = \int_{-\infty}^{\tau} g(s) ds$$

but typically, we don't...



# False Non-Match Rate

$$\hat{g}_{\text{FNM}}(\tau) = \text{FNMR}(\tau) = \frac{\text{Number of false non-matches for } \tau}{\text{Number of all genuine comparisons}}$$

Calculate with a benchmark data set



Image Credit: NIST



Image Credit: U. Bologna

# False Match Rate

If we know  $d$ :

$$d_{\text{FM}}(\tau) = \int_{-\infty}^{\tau} d(s) ds$$

but typically, we don't...

# False Match Rate

$$\hat{g}_{\text{FM}}(\tau) = \text{FMR}(\tau) = \frac{\text{Number of false matches for } \tau}{\text{Number of all impostor comparisons}}$$

Calculate with a benchmark data set

# Measurement Trade-Offs

Problem 1: Biometric Verification – Why am I rejected?

Large throughput volume is a problem.

- Example: frequent flyer verification from face image
- Assume a system where each person is 1:1 verified at an airport kiosk with 5,000 people per hour (14hr/day) requesting access (Newark Airport hourly passenger volume)
- The system has an FMR of 0.1% and an FNMR of 2%

100 people per hour will fail to be verified

1,400 people per day will fail to be verified

# Measurement Trade-Offs

Problem 2: Biometric (Mis)Identification – Why am I delayed as a “suspect”?

Large watch lists exacerbate the problem.

- Example: Faces checked against terrorist watch list
- Assume a system that checks each person’s face against a watch list of 1,000 suspects. Assume Newark Airport: 5,000 people per hour/14hr day
- The system has an FMR of 0.1%

Over 70,000 false matches will occur per day from 1K watch list

- Note: 2011 US TSC TSDB list was > 450K



# Measurement Trade-Offs

Problem 3: Biometric Identification – “Who can I be today?”

Biometric databases are a security problem.

Example 3: Faces checked against government database>

- Criminals gain access to a large face database, and start looking for someone their gang can use to steal an identity.
- With an FMR of 0.01%, a single face will match  $(.001 * 6,000,000) = 6,000$  people in the DC area. With a “gang” of 10 or 100 what can they do?
- Note: Colorado DMV records have fingerprint, photo and all driving information

# Measurement Trade-Offs

Biometric "Dictionary"



Enrollment Data



Verification Algorithm

System Parameter:  
 $FMR = 1/X$  Attempts

Doppelganger Attack

Match?

**YES**  
Doppelganger  
Detected

**NO**  
Try another print  
from the "Dictionary"

# Measurement Trade-Offs

False Matches During Duplicate Checks Require Additional Processing.

Number of False Hits ***Per Search***  
(*i.e.*, each person being checked)

<b>FAR</b>	<b>50 Million</b>	<b>500 Million</b>
1%	500,000	5M
0.1%	50,000	500,000
0.01%	5,000	50,000
0.001%	500	5,000
0.0001%	50	500

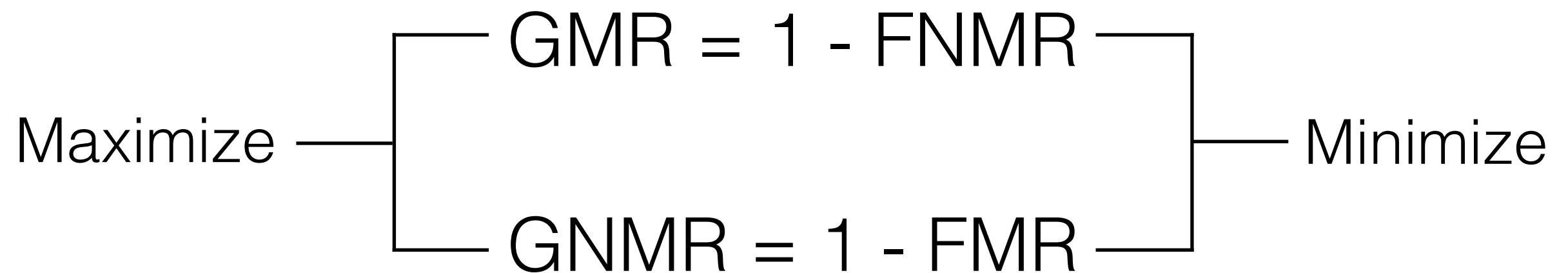
Total *false matches* that must be resolved in determining duplicates

<b>FAR</b>	<b>50 Million</b>	<b>500 Million</b>
1%	25Trillion	25000Trillion
0.1%	2.5Trillion	2500Tillion
0.01%	250Billion	250Trillion
0.001%	25Billon	2.5Trillion
0.0001%	2.5Billion	250Billion

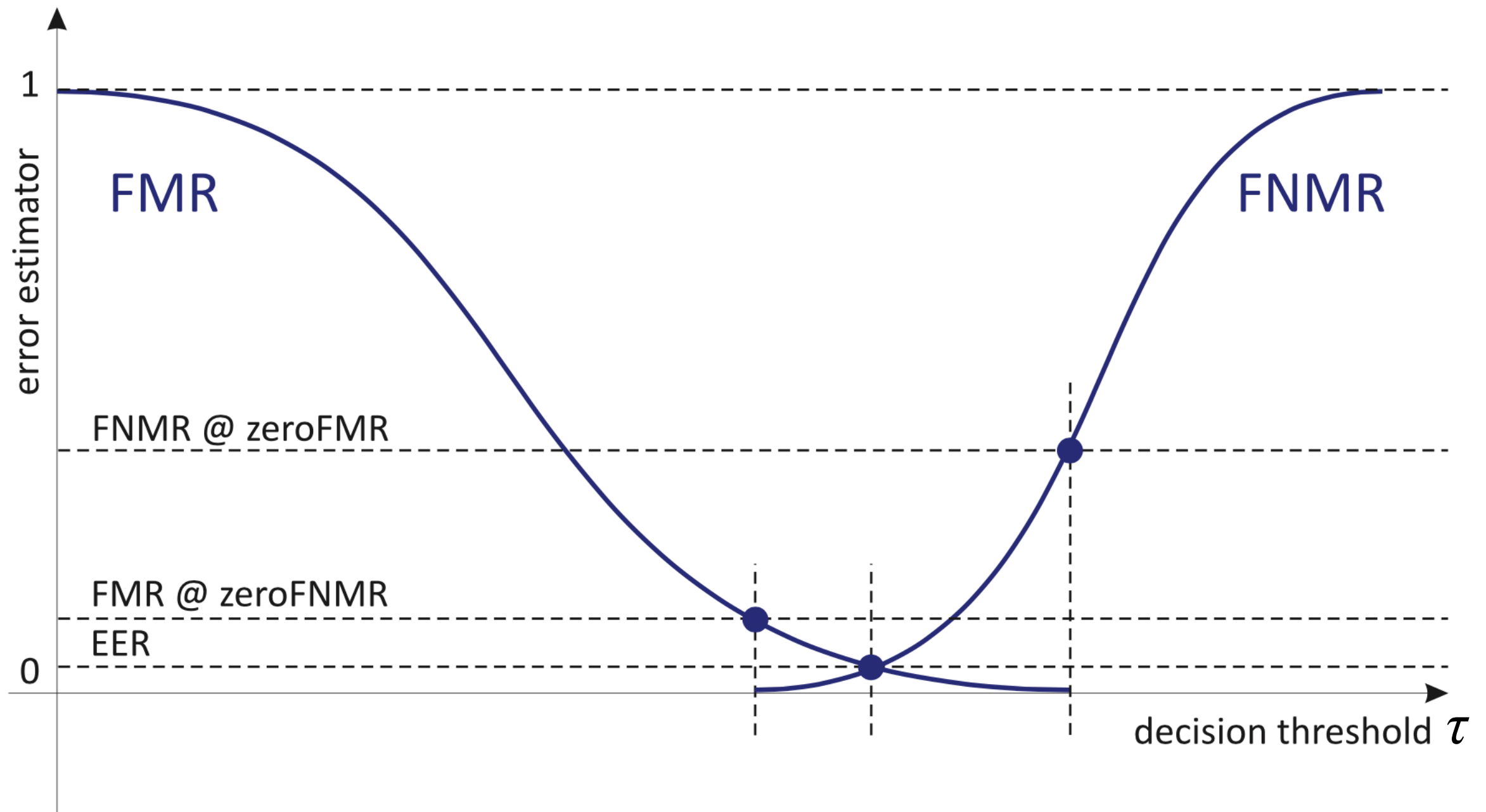
Two ways to address these false hits are:

- Manually? (Note: 2.5 Billion minutes is about 4,750 years!)
- *Automatically use another biometric and hope to reduce FAR*

# Correct Decisions



# Error estimators as a function of $\tau$

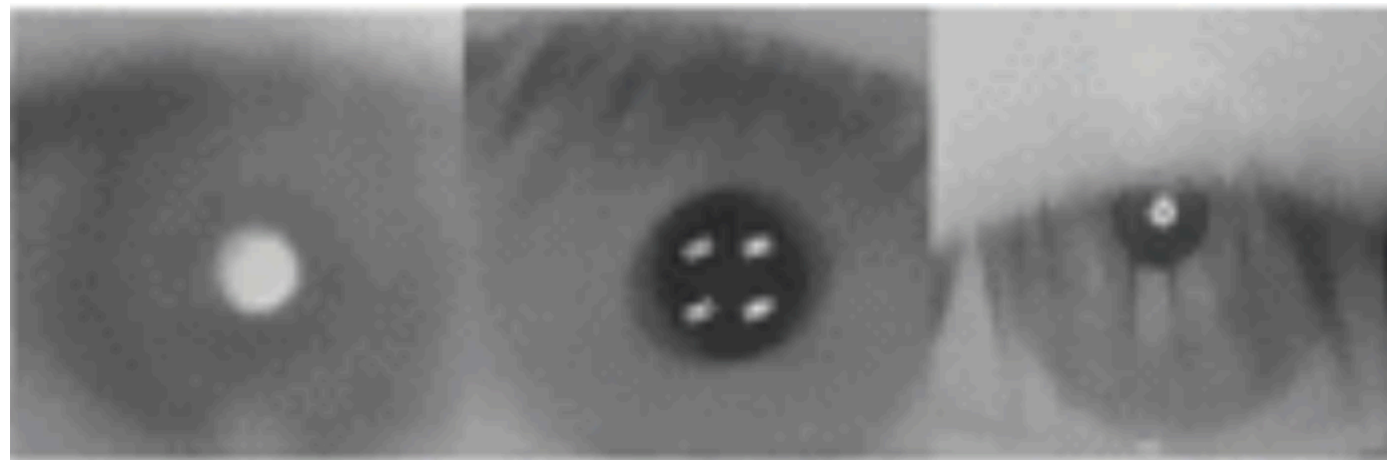




# Failure to Acquire

Falsely rejected biometric samples

Problem at acquisition time:



Wei et al., "Robust and Fast Assessment of Iris Image Quality," ICB 2006

# Failure to Enroll

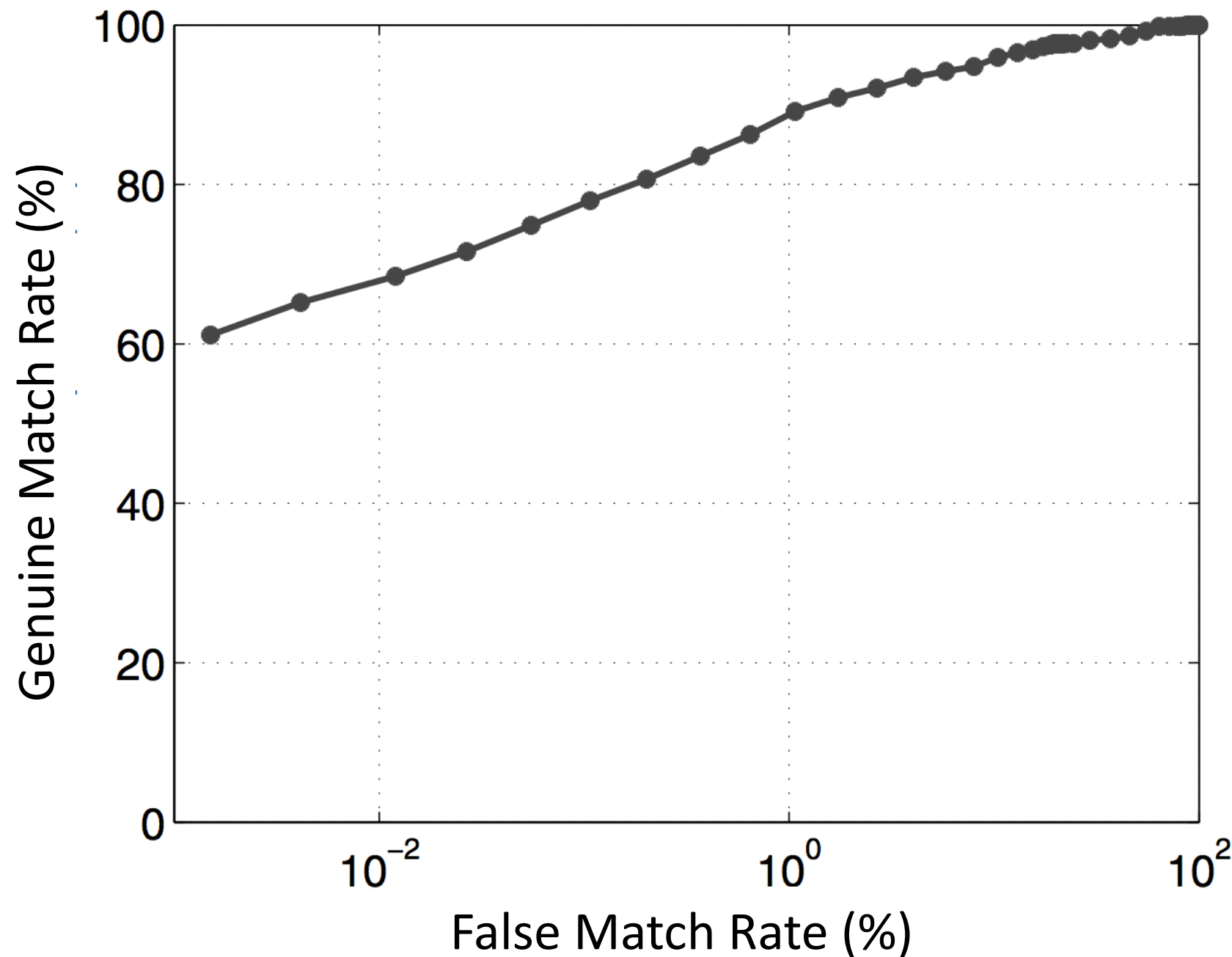
Falsely rejected biometric samples at enrollment time

“Immigration Delay Disease”

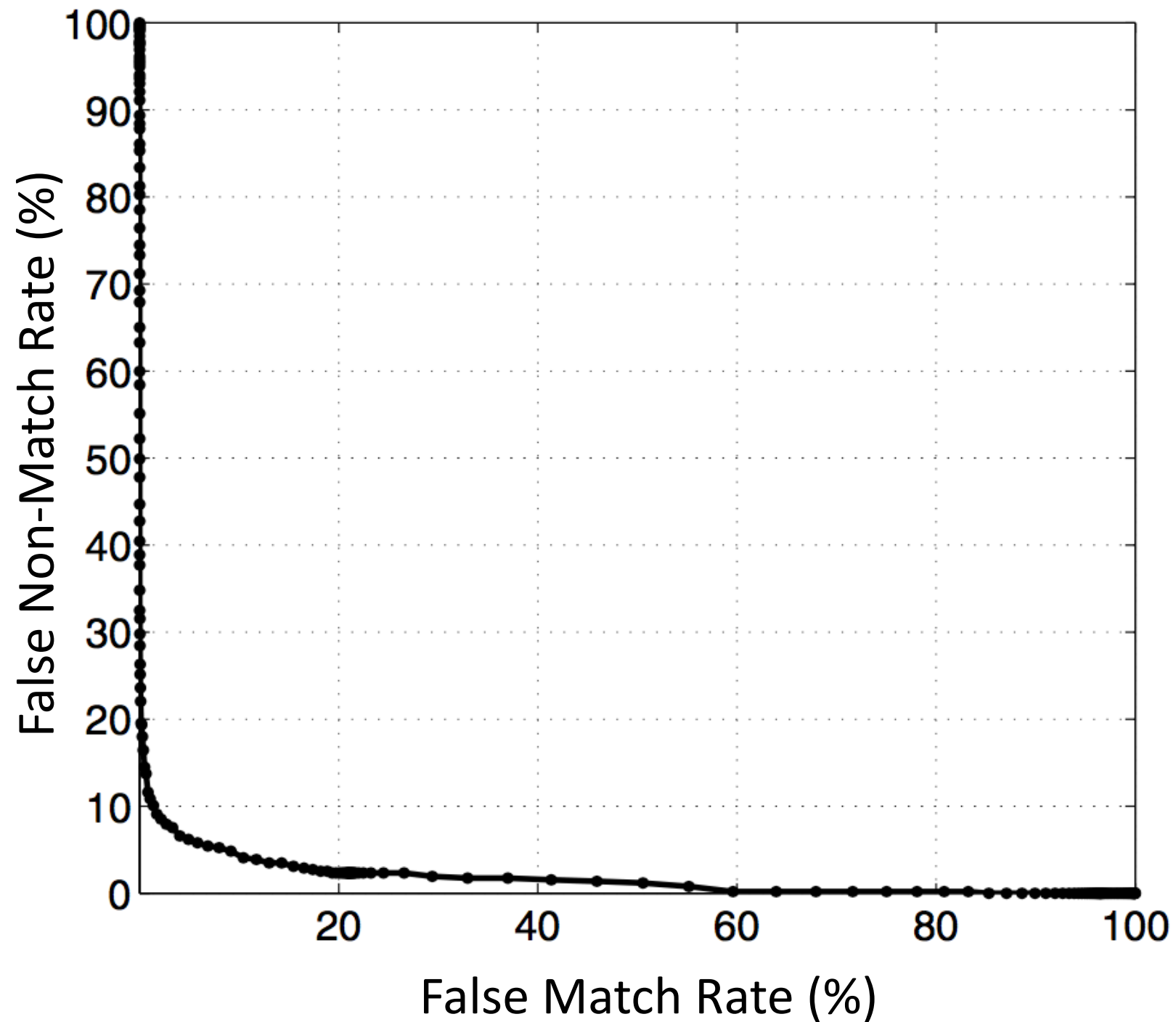


Image Credit: Eli Sprecher, American Journal of Human Genetics

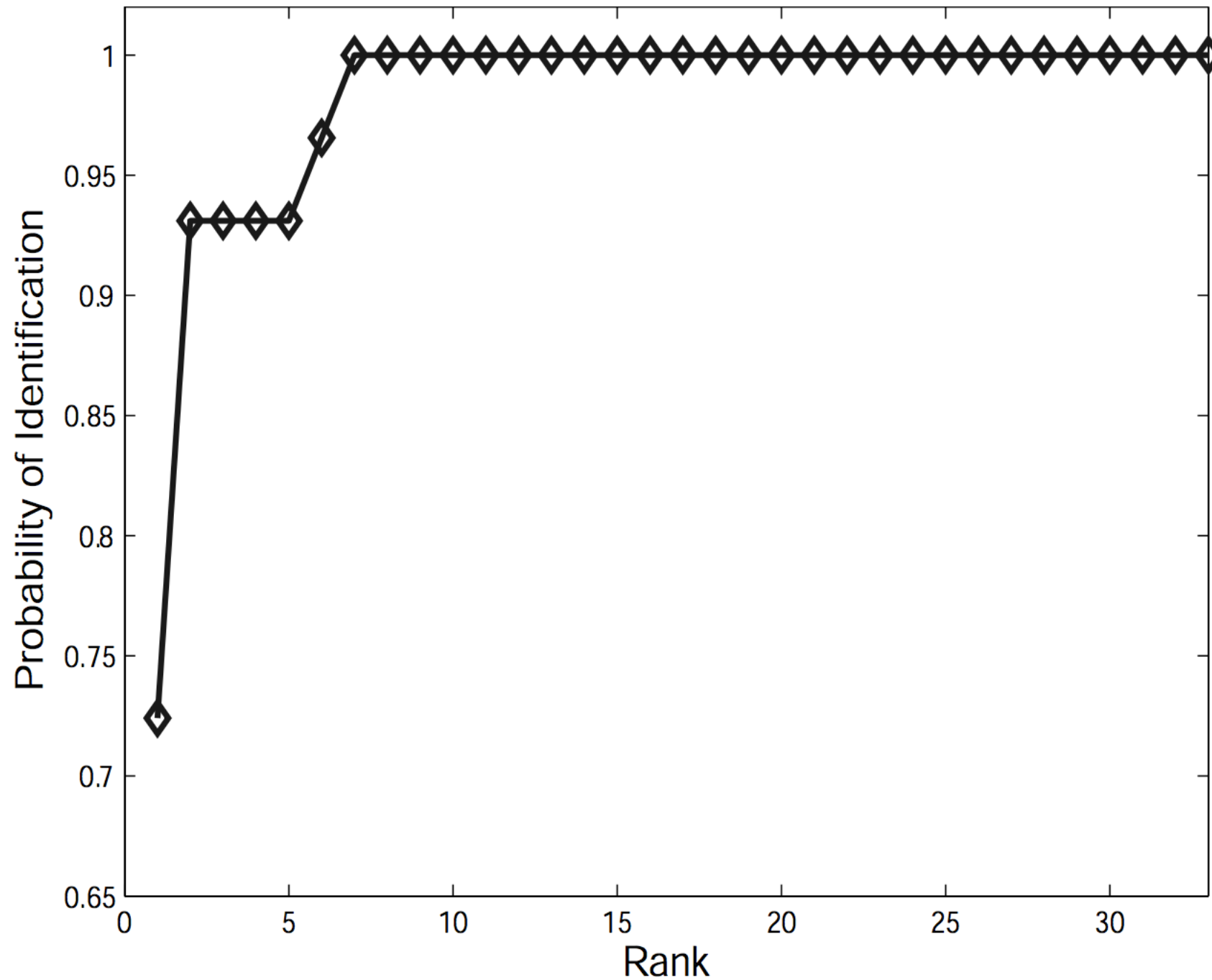
# Receiver Operating Characteristic Curve (ROC)



# Detection Error Tradeoff Curve (DET)



# Cumulative Match Curve (CMC)





# Rise of Machine Learning

Why the sudden surge in ML vision applications?



NVIDIA\_GeForce\_GTX\_780-Top © BY 2.0 GBPublic\_PR



New Samsung DDR4 © BY-NC-SA 2.0 SamsungTomorrow



G.B Huang et al., Labeled Faces in the Wild

Advances in  
parallel  
computing

Large  
Memories

Web-scale  
Data

**Additional error statistics...**

# Accuracy

Accuracy =

| genuine matches | + | genuine non-matches |

---

| genuine matches | + | genuine non-matches | + | false matches | + | false non-matches |

Error =  $E = 1 - \text{Accuracy}$

# Cross Validation

$N$  training samples

$$X_y = \{(x_1, y_1), \dots, (x_N, y_N)\}$$

Empirical error on the training set

$$M_y = f(X_y, \varphi_M), \text{ s.t. } E_{train} \text{ is minimized}$$

How do we estimate?

# Cross Validation

Leave one out:

$$f_n = (x_1, y_1), \dots, (x_{n-1}, y_{n-1}), \text{---} (x_n, y_n) \text{---}, (x_{n+1}, y_{n+1}), \dots (x_N, y_N)$$

$$e_n = E_{\text{val}}(f) = e(f(x_n), y)$$

$$E_{cv} = \frac{1}{N} \sum_{n=1}^N e_n$$

# Cross Validation

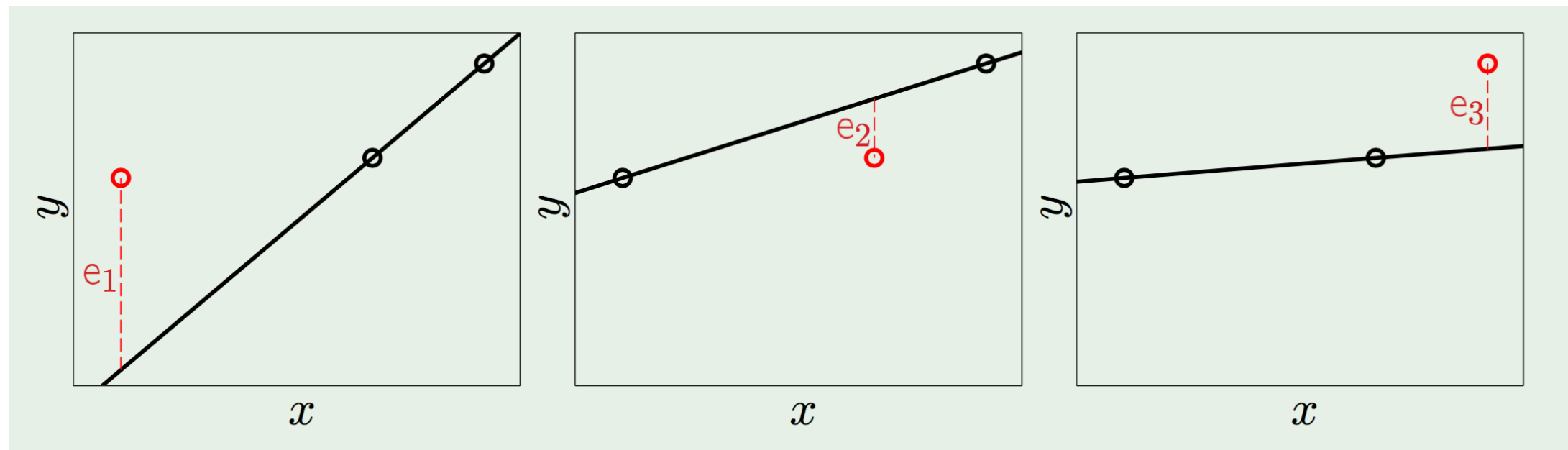


Image Credit: Y. Abu-Mostafa, *Learning from Data*

$$E_{cv} = \frac{1}{3} (e_1 + e_2 + e_3)$$



# Cross Validation

Without Validation

With Validation

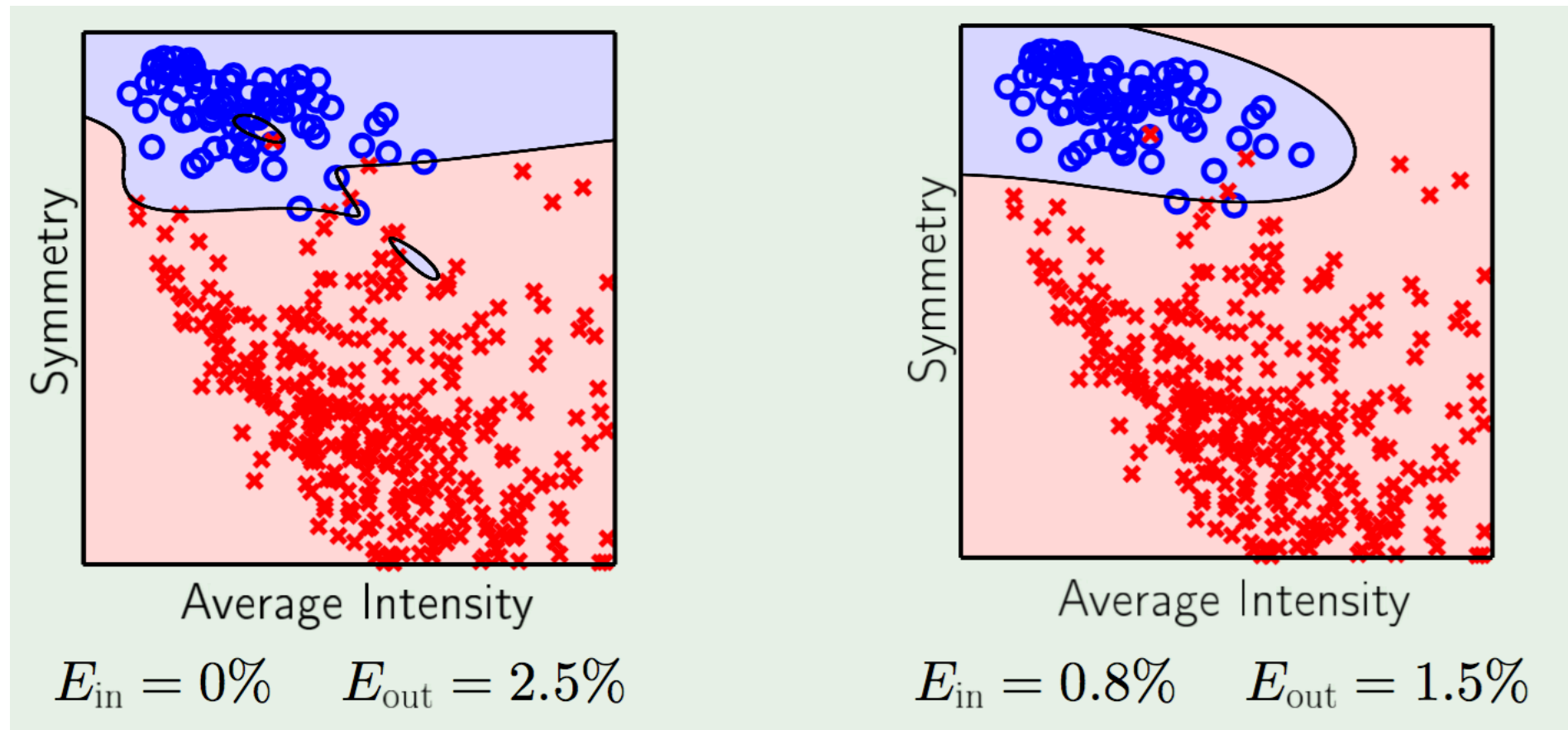


Image Credit: Y. Abu-Mostafa, *Learning from Data*

(MNIST)

# $K$ -Fold Cross Validation

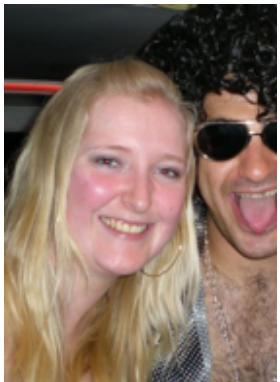
Generalize:  $\frac{N}{K}$  training sessions on  $N - K$  points each

Typical procedure is 10-fold cross validation:  $K = \frac{N}{10}$

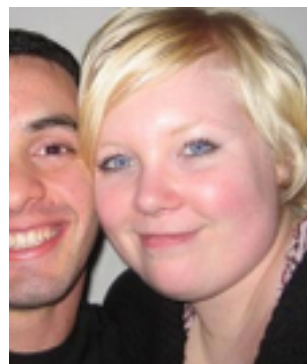
# Recall

$$\text{Recall} = \frac{\{\text{Relevant Images}\} \cap \{\text{Retrieved Images}\}}{\{\text{Relevant Images}\}}$$

Probe



Gallery

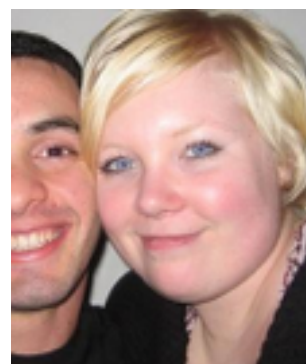
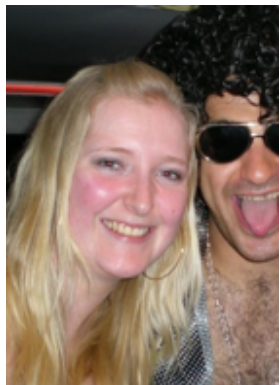


**Recall = 50%**

# Precision

$$\text{Precision} = \frac{\{\text{Relevant Images}\} \cap \{\text{Retrieved Images}\}}{\{\text{Retrieved Images}\}}$$

Probe



**Precision = 33%**



# F-measure

What's wrong with accuracy?

Sliding window detector



11 faces, and  
1,000 negative windows

A “no” detector will be  
98.9% accurate!

# F-measure

Calculate harmonic mean of precision and recall:

$$F_1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$



# Area Under the Curve

0.9 - 1.0 = excellent  
0.8 - 0.9 = good  
0.7 - 0.8 = fair  
0.6 - 0.7 = poor  
0.5 - 0.6 = fail

\*use when you can't  
pick a threshold

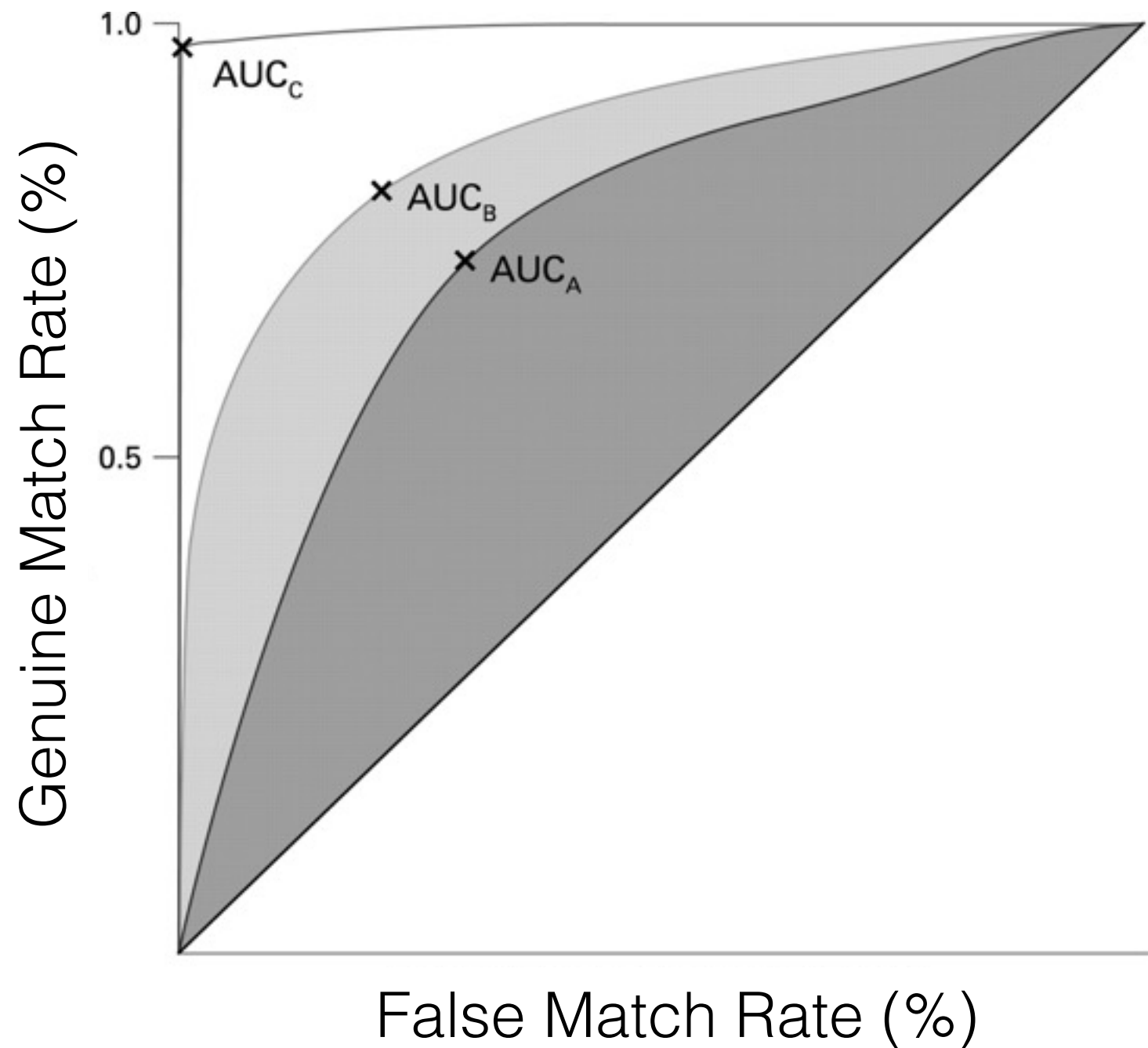


Image adapted from figure appearing in the Journal of Clinical Pathology