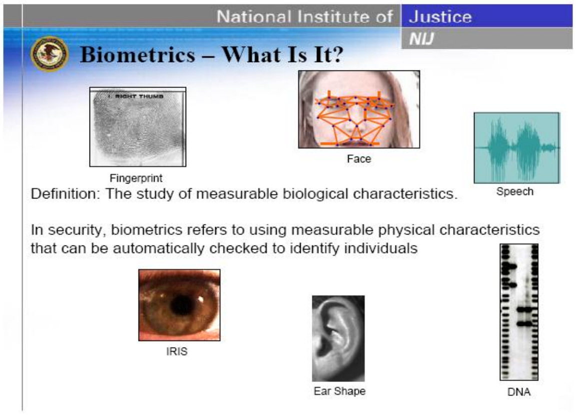
# Biometric Technologies: Security and Privacy

Dr. Rigoberto Chinchilla
School of Technology



National Institute of Justice
NIJ

## Biometrics – What Is It?

Definition: The study of measurable biological characteristics.

In security, biometrics refers to using measurable physical characteristics that can be automatically checked to identify individuals

1. RIGHT THUMB
Fingerprint
Face
Speech
IRIS
Ear Shape
DNA

## Why Biometrics?

- Reliable authorization and authentication are becoming “necessary” for many everyday actions (or applications)
  - – Pick in up a child from a daycare
  - – Boarding an aircraft
  - – Performing financial transactions
  - – Accessing facilities

## Why Biometrics?

- Regardless of the rationale for deploying biometrics, there are two common elements:
  - – The benefits of biometric usage and deployment are derived from having a high degree of certainty regarding an individual’s identity
  - – The benefits might lead directly or indirectly to cost savings or to reduced risk of financial losses for an individual or an institution (In the long run)

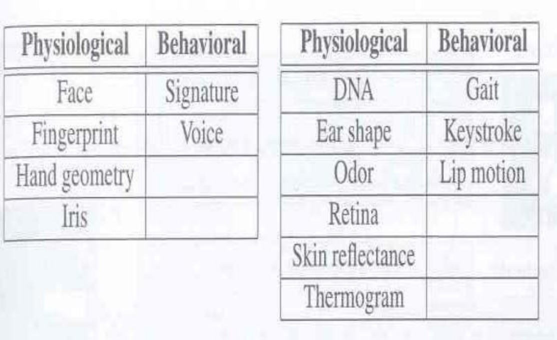
## Broad Biometric division

- Physiological Biometrics: Are physical characteristics generally measured at some point in time like fingerprint or hand geometry
- Behavioral Biometrics: Consist on the way some action is carried out and extend over time (signature or voice).
  - Behavioral biometrics are learned or acquired over time and are dependent on one's state of mind or even subject to deliberate alteration

## Broad Biometric division

- Loosely speaking:
  - Physiological biometrics are rich enough that one-time sampling may suffice for comparing biometric identifiers
  - Behavioral biometrics, any given sample may give no information about person's identity, but, is the temporal variation (behavioral influence) of the signal that contains the information
    - Typically more than one sample is needed

## Biometric identifiers

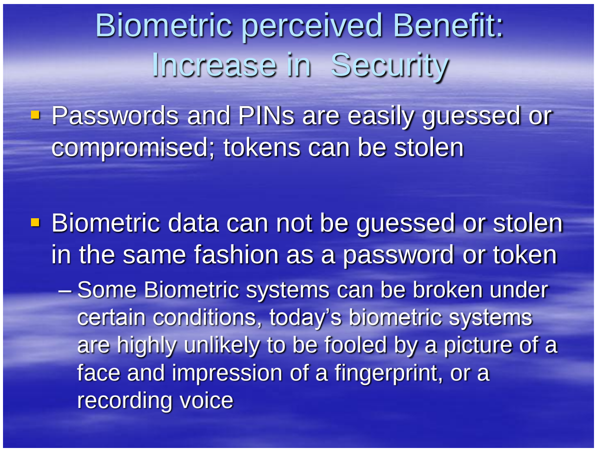


| Physiological | Behavioral |
|---|---|
| Face | Signature |
| Fingerprint | Voice |
| Hand geometry | |
| Iris | |

| Physiological | Behavioral |
|---|---|
| DNA | Gait |
| Ear shape | Keystroke |
| Odor | Lip motion |
| Retina | |
| Skin reflectance | |
| Thermogram | |

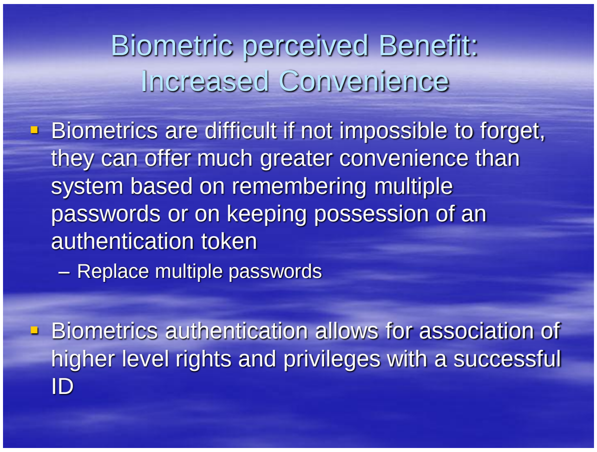
## Biometrics Drivers

- Powerful Computers
- Powerful Databases
- Security increased concerns (SEPT 11)
  - Fear !
- Dependency on computers for everything
- Digitalized images
- Digital Telecommunications
- High bandwidth availability



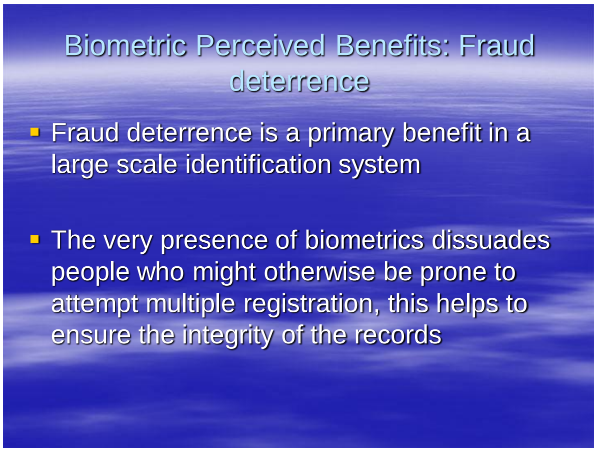
## Biometric perceived Benefit: Increase in Security

- Passwords and PINs are easily guessed or compromised; tokens can be stolen
- Biometric data can not be guessed or stolen in the same fashion as a password or token
  - Some Biometric systems can be broken under certain conditions, today's biometric systems are highly unlikely to be fooled by a picture of a face and impression of a fingerprint, or a recording voice



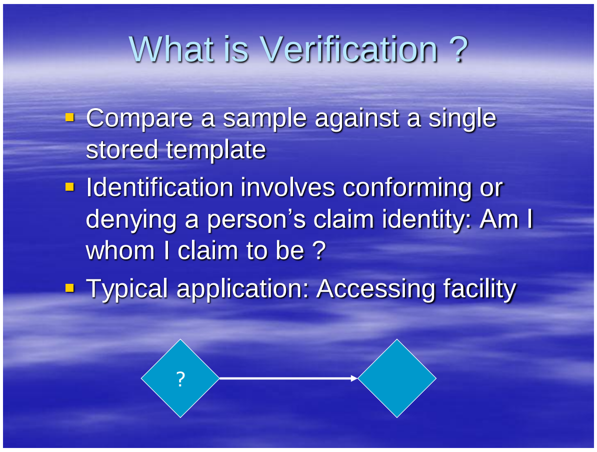
## Biometric perceived Benefit: Increased Convenience

- Biometrics are difficult if not impossible to forget, they can offer much greater convenience than system based on remembering multiple passwords or on keeping possession of an authentication token
  - Replace multiple passwords
- Biometrics authentication allows for association of higher level rights and privileges with a successful ID



## Biometric Perceived Benefits: Fraud deterrence

- Fraud deterrence is a primary benefit in a large scale identification system
- The very presence of biometrics dissuades people who might otherwise be prone to attempt multiple registration, this helps to ensure the integrity of the records

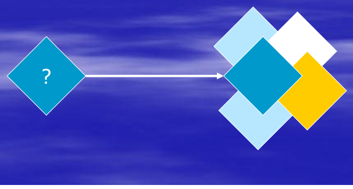


## What is Verification ?

- Compare a sample against a single stored template
- Identification involves conforming or denying a person's claim identity: Am I whom I claim to be ?
- Typical application: Accessing facility

## What is Identification ?

- Search a sample against a database of templates.
- Typical application: identifying fingerprints
  - – See CSI TV series



## Biometric Identification

- Positive Identification: A given individual is a member of the database
  - – False accept: An intruder enters the system (False Match FMR)
  - – False reject: A legitimate subject is denied from service (False Non-Match FNMR)
- Negative Identification: (Screening) This amounts to determining that a subject is not in some negative databases ("most wanted list")
  - – False negative: Missing a match
  - – False positive : False detection of a match

## How biometric matching works ?

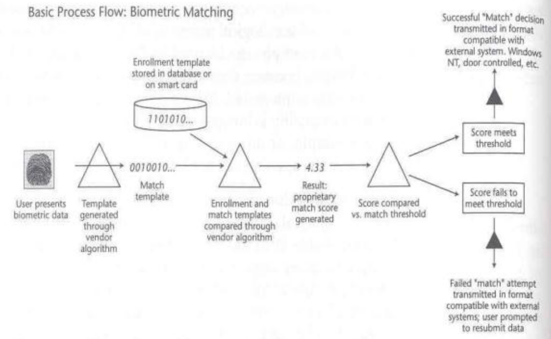
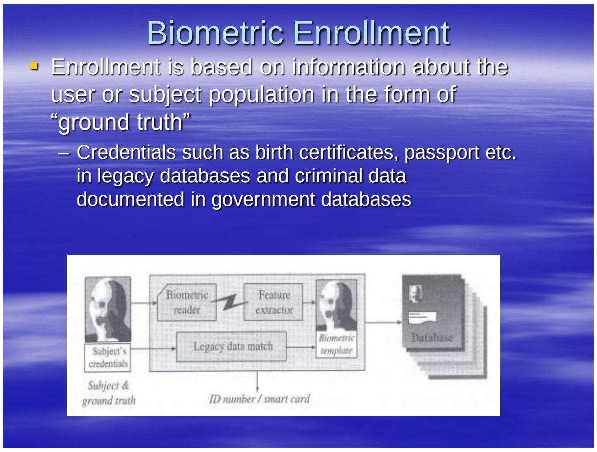

Basic Process Flow: Biometric Matching
Enrollment template stored in database or on smart card
1101010...
User presents biometric data
Template generated through vendor algorithm
0010010...
Match template
Enrollment and match templates compared through vendor algorithm
4.33
Result: proprietary match score generated
Score compared vs. match threshold
Score meets threshold
Score fails to meet threshold
Successful "Match" decision transmitted in format compatible with external system. Windows NT, door controlled, etc.
Failed "match" attempt transmitted in format compatible with external systems; user prompted to resubmit data

**Figure 2.2** Biometric matching: process flow.

## Biometric Enrollment

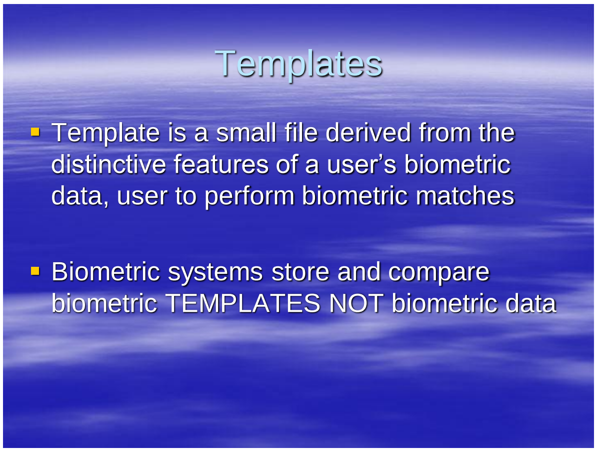
- Enrollment is the process by which a user's biometric data is initially acquired, assessed, processed and stored in the form of a template for ongoing use in a biometric system
- Quality enrollment is a critical factor in the long-term accuracy of biometric systems. Low quality enrollments may lead to a high error rates including false match rate and false non-match rate.



## Biometric Enrollment

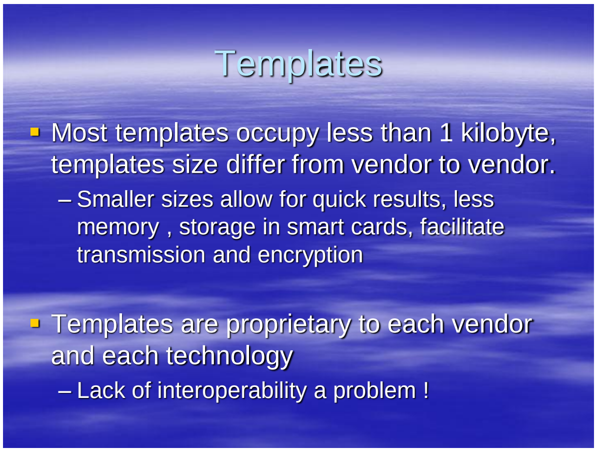
- Enrollment is based on information about the user or subject population in the form of "ground truth"
  - – Credentials such as birth certificates, passport etc. in legacy databases and criminal data documented in government databases

Biometric reader
Feature extractor
Legacy data match
Biometric template
Database
Subject's credentials
Subject & ground truth
ID number / smart card



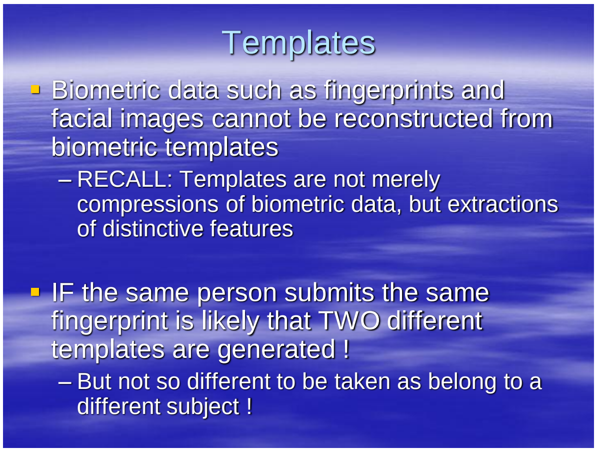
## Templates

- Template is a small file derived from the distinctive features of a user's biometric data, user to perform biometric matches
- Biometric systems store and compare biometric TEMPLATES NOT biometric data



## Templates

- Most templates occupy less than 1 kilobyte, templates size differ from vendor to vendor.
  - – Smaller sizes allow for quick results, less memory , storage in smart cards, facilitate transmission and encryption
- Templates are proprietary to each vendor and each technology
  - – Lack of interoperability a problem !



## Templates

- Biometric data such as fingerprints and facial images cannot be reconstructed from biometric templates
  - – RECALL: Templates are not merely compressions of biometric data, but extractions of distinctive features
- IF the same person submits the same fingerprint is likely that TWO different templates are generated !
  - – But not so different to be taken as belong to a different subject !

## Templates

- Why two templates will never be exactly the same even if they belong to the same person ?
  - Slight changes in
    - Position
    - Pressure, distance

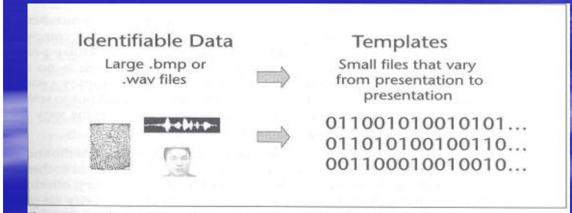


Figure 2.3 Biometric templates versus identifiable biometric data.

## Biometric Matching

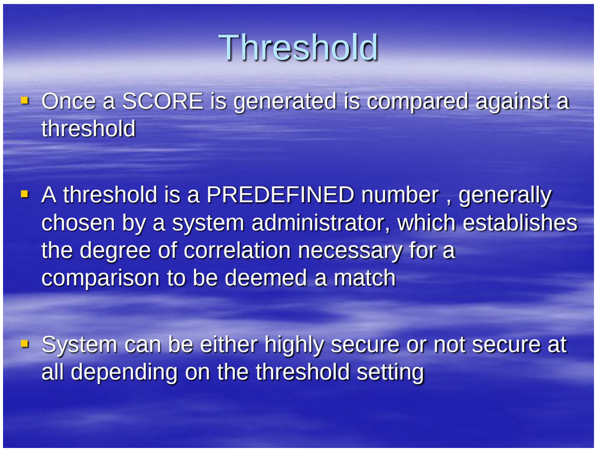
- The comparison of biometric templates to determine the degree of similarity or correlation is called matching
- The process of matching biometric templates results in a SCORE, which in most systems, is compared against a threshold
  - If the score exceeds the threshold, the result is a match, if the score falls below the threshold, the result is a non-match

## Scoring

- Biometric matches are based on scores
  - Score : A number indicating the degree of similarity or correlation resulting from the comparison of the enrollment and verification templates
  - There is no standard scale (0-100% or -1 to +1), scores may vary from technology to technology and from vendor to vendor

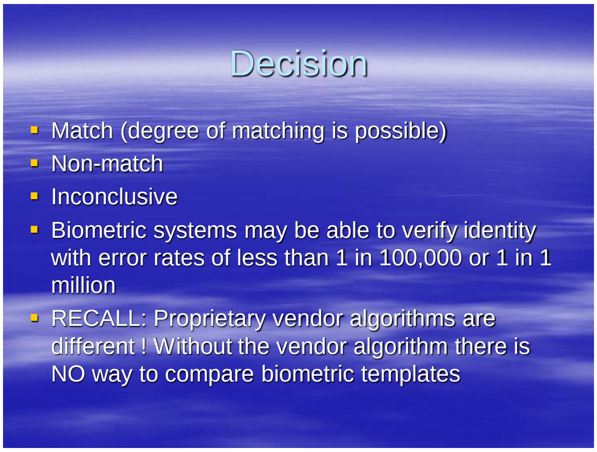
## Scoring

- Biometric matches are based on scores
  - Most strengths and weaknesses of biometric systems have to do with the scoring algorithm/system
  - Biometric systems do not rely completely in a “match/no match” decisions , because DIFFERENT templates are generated from the SAME subject there is no 100% correlation all the time



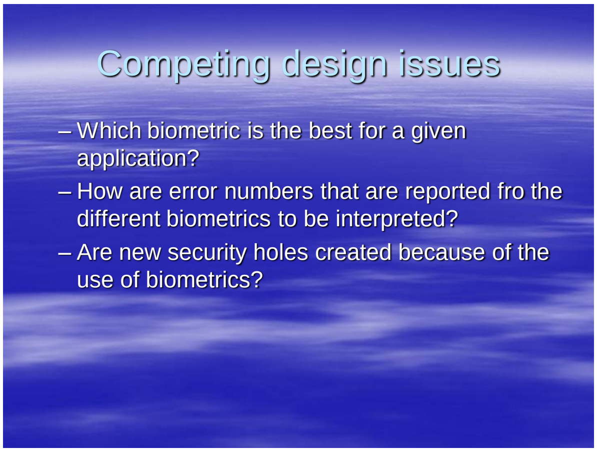
## Threshold

- Once a SCORE is generated is compared against a threshold
- A threshold is a PREDEFINED number , generally chosen by a system administrator, which establishes the degree of correlation necessary for a comparison to be deemed a match
- System can be either highly secure or not secure at all depending on the threshold setting



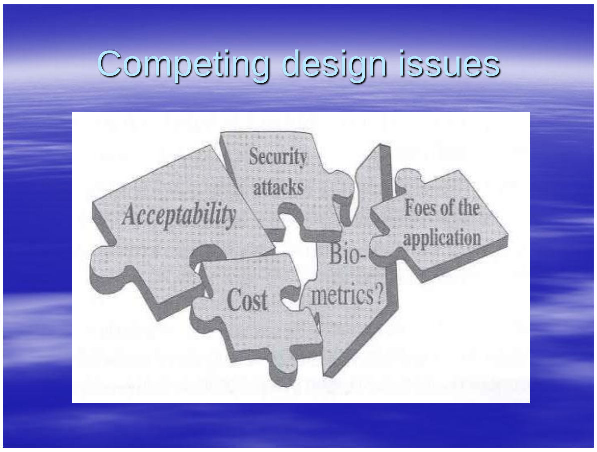
## Decision

- Match (degree of matching is possible)
- Non-match
- Inconclusive
- Biometric systems may be able to verify identity with error rates of less than 1 in 100,000 or 1 in 1 million
- RECALL: Proprietary vendor algorithms are different ! Without the vendor algorithm there is NO way to compare biometric templates

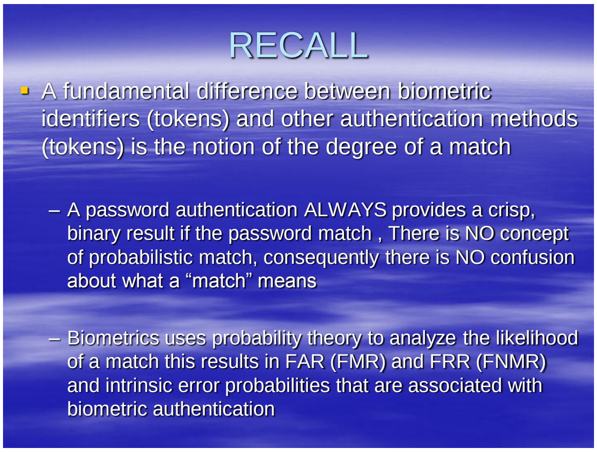


## Competing design issues

- – Which biometric is the best for a given application?
- – How are error numbers that are reported fro the different biometrics to be interpreted?
- – Are new security holes created because of the use of biometrics?

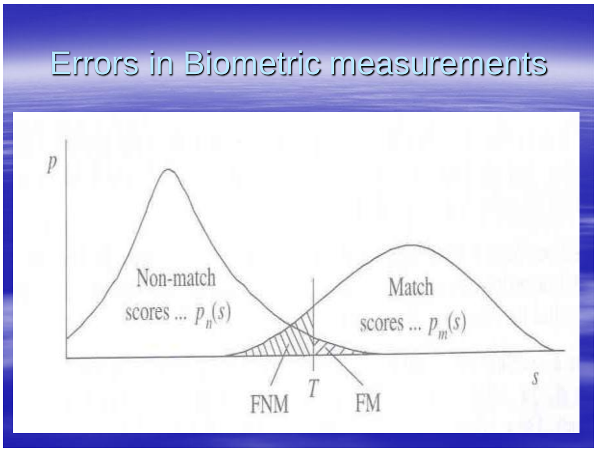


## Competing design issues

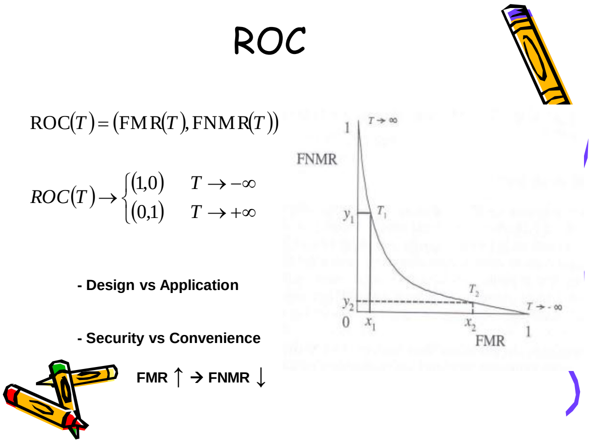


## RECALL

- A fundamental difference between biometric identifiers (tokens) and other authentication methods (tokens) is the notion of the degree of a match
  - A password authentication ALWAYS provides a crisp, binary result if the password match , There is NO concept of probabilistic match, consequently there is NO confusion about what a “match” means
  - Biometrics uses probability theory to analyze the likelihood of a match this results in FAR (FMR) and FRR (FNMR) and intrinsic error probabilities that are associated with biometric authentication



## Errors in Biometric measurements



## ROC

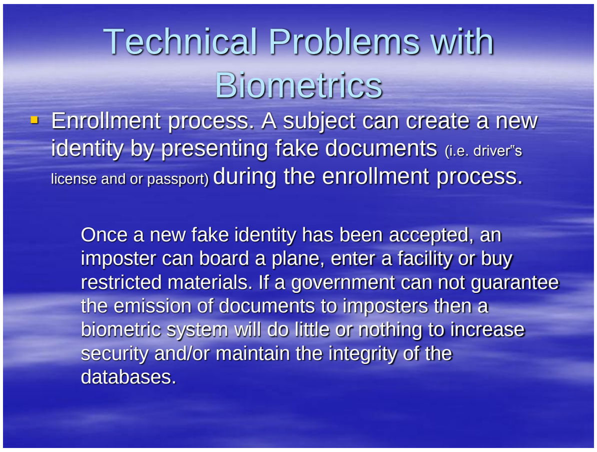
$$ROC(T) = (FMR(T), FNMR(T))$$

$$ROC(T) \rightarrow \begin{cases} (1,0) & T \rightarrow -\infty \\ (0,1) & T \rightarrow +\infty \end{cases}$$

- Design vs Application

- Security vs Convenience

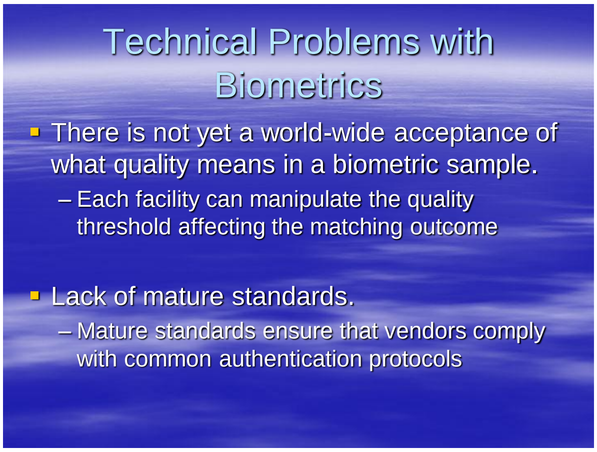
FMR ↑ → FNMR ↓



## Technical Problems with Biometrics

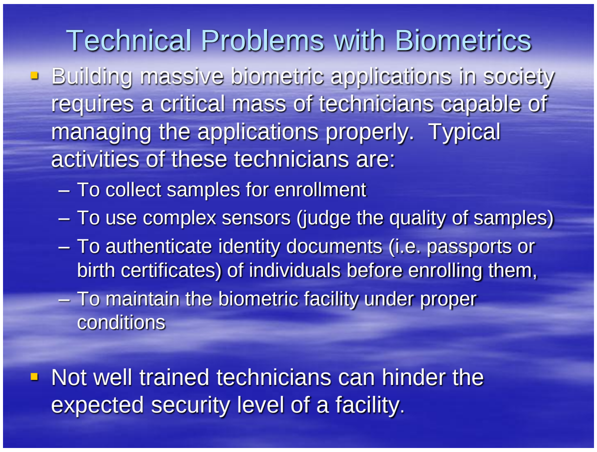
- Enrollment process. A subject can create a new identity by presenting fake documents (i.e. driver"s license and or passport) during the enrollment process.

Once a new fake identity has been accepted, an imposter can board a plane, enter a facility or buy restricted materials. If a government can not guarantee the emission of documents to imposters then a biometric system will do little or nothing to increase security and/or maintain the integrity of the databases.



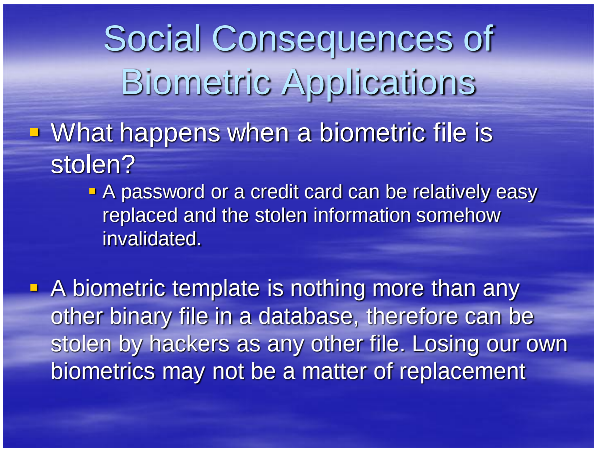
## Technical Problems with Biometrics

- There is not yet a world-wide acceptance of what quality means in a biometric sample.
  - Each facility can manipulate the quality threshold affecting the matching outcome
- Lack of mature standards.
  - Mature standards ensure that vendors comply with common authentication protocols



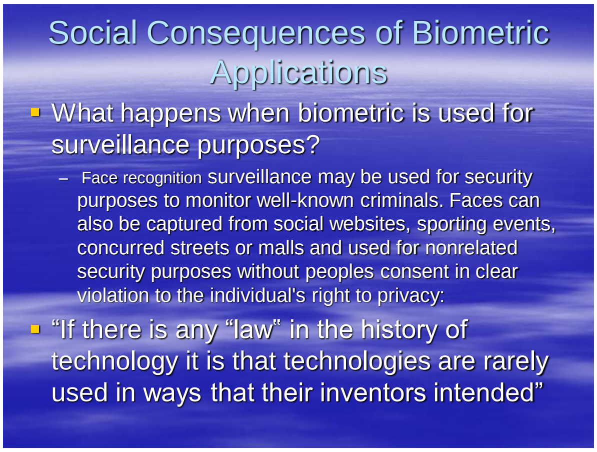
## Technical Problems with Biometrics

- Building massive biometric applications in society requires a critical mass of technicians capable of managing the applications properly. Typical activities of these technicians are:
  - To collect samples for enrollment
  - To use complex sensors (judge the quality of samples)
  - To authenticate identity documents (i.e. passports or birth certificates) of individuals before enrolling them,
  - To maintain the biometric facility under proper conditions
- Not well trained technicians can hinder the expected security level of a facility.



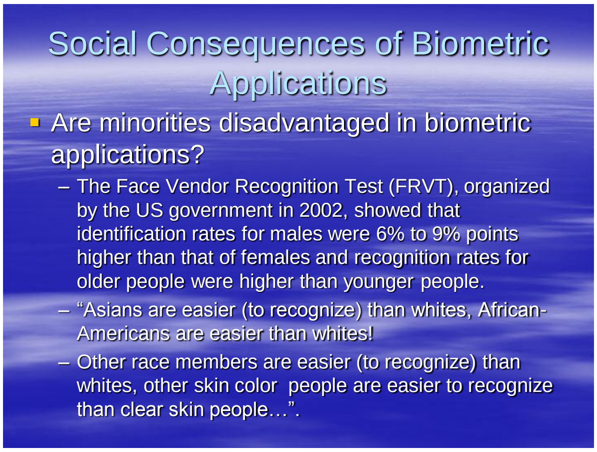
## Social Consequences of Biometric Applications

- What happens when a biometric file is stolen?
  - A password or a credit card can be relatively easy replaced and the stolen information somehow invalidated.
- A biometric template is nothing more than any other binary file in a database, therefore can be stolen by hackers as any other file. Losing our own biometrics may not be a matter of replacement



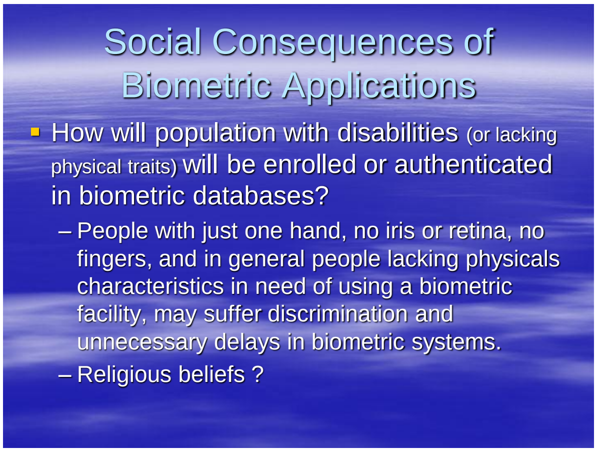
## Social Consequences of Biometric Applications

- What happens when biometric is used for surveillance purposes?
  - Face recognition surveillance may be used for security purposes to monitor well-known criminals. Faces can also be captured from social websites, sporting events, concurred streets or malls and used for nonrelated security purposes without peoples consent in clear violation to the individual's right to privacy:
- “If there is any “law“ in the history of technology it is that technologies are rarely used in ways that their inventors intended”



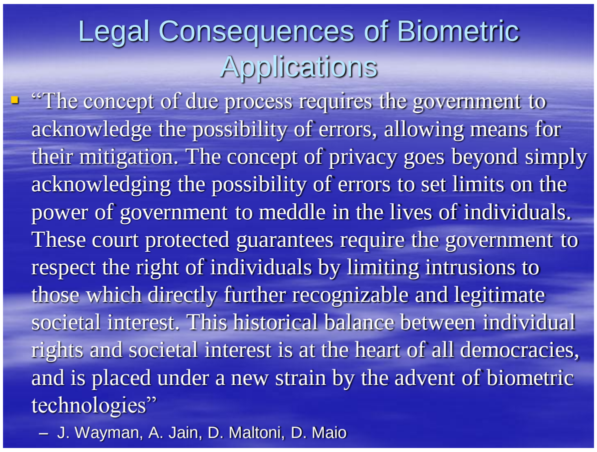
## Social Consequences of Biometric Applications

- Are minorities disadvantaged in biometric applications?
  - The Face Vendor Recognition Test (FRVT), organized by the US government in 2002, showed that identification rates for males were 6% to 9% points higher than that of females and recognition rates for older people were higher than younger people.
  - "Asians are easier (to recognize) than whites, African-Americans are easier than whites!
  - Other race members are easier (to recognize) than whites, other skin color people are easier to recognize than clear skin people…".



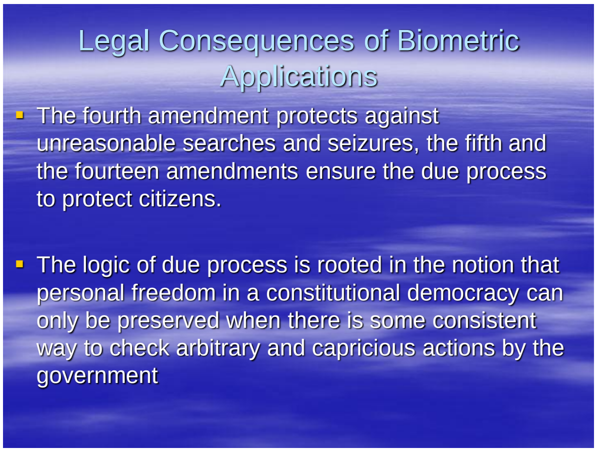
## Social Consequences of Biometric Applications

- How will population with disabilities (or lacking physical traits) will be enrolled or authenticated in biometric databases?
  - People with just one hand, no iris or retina, no fingers, and in general people lacking physicals characteristics in need of using a biometric facility, may suffer discrimination and unnecessary delays in biometric systems.
  - Religious beliefs ?



## Legal Consequences of Biometric Applications

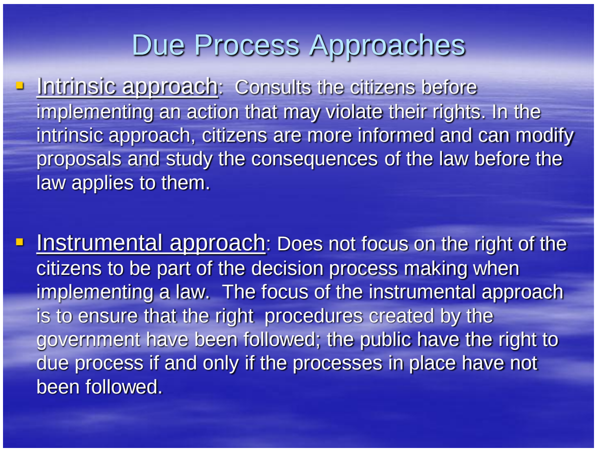
- "The concept of due process requires the government to acknowledge the possibility of errors, allowing means for their mitigation. The concept of privacy goes beyond simply acknowledging the possibility of errors to set limits on the power of government to meddle in the lives of individuals. These court protected guarantees require the government to respect the right of individuals by limiting intrusions to those which directly further recognizable and legitimate societal interest. This historical balance between individual rights and societal interest is at the heart of all democracies, and is placed under a new strain by the advent of biometric technologies"
  - J. Wayman, A. Jain, D. Maltoni, D. Maio



## Legal Consequences of Biometric Applications

- The fourth amendment protects against unreasonable searches and seizures, the fifth and the fourteen amendments ensure the due process to protect citizens.

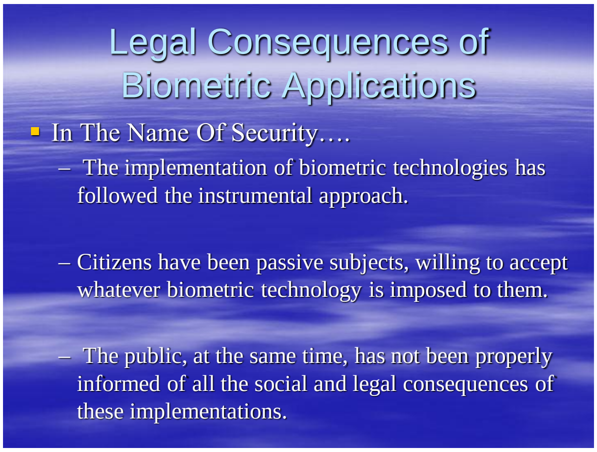
- The logic of due process is rooted in the notion that personal freedom in a constitutional democracy can only be preserved when there is some consistent way to check arbitrary and capricious actions by the government



## Due Process Approaches

- Intrinsic approach: Consults the citizens before implementing an action that may violate their rights. In the intrinsic approach, citizens are more informed and can modify proposals and study the consequences of the law before the law applies to them.

- Instrumental approach: Does not focus on the right of the citizens to be part of the decision process making when implementing a law. The focus of the instrumental approach is to ensure that the right procedures created by the government have been followed; the public have the right to due process if and only if the processes in place have not been followed.

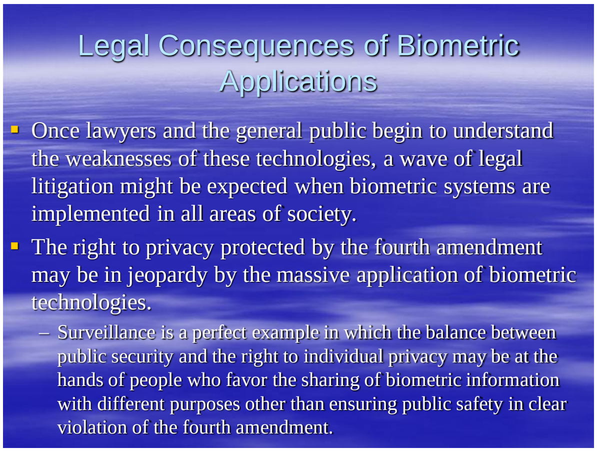


## Legal Consequences of Biometric Applications

- In The Name Of Security….
  - The implementation of biometric technologies has followed the instrumental approach.

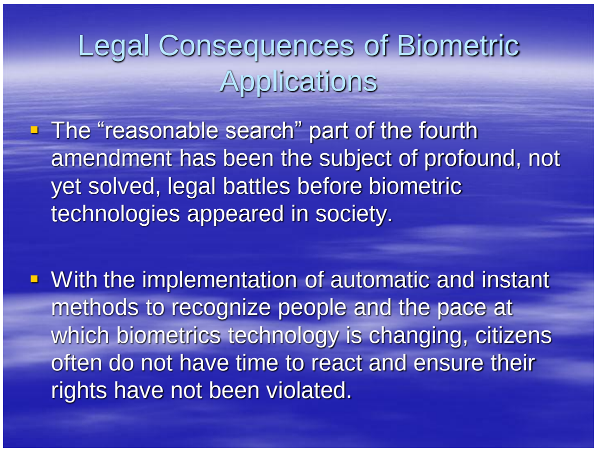
  - Citizens have been passive subjects, willing to accept whatever biometric technology is imposed to them.

  - The public, at the same time, has not been properly informed of all the social and legal consequences of these implementations.



## Legal Consequences of Biometric Applications

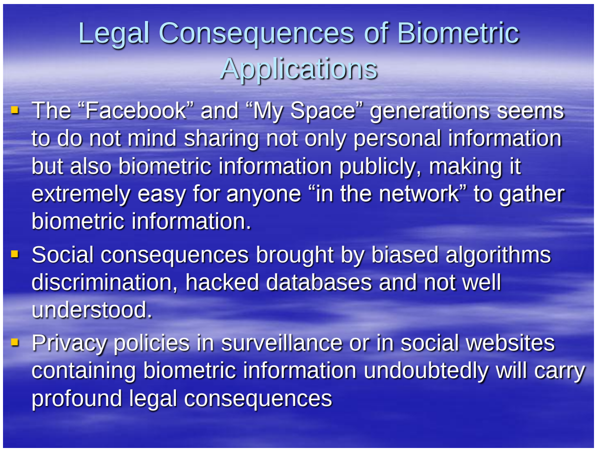
- Once lawyers and the general public begin to understand the weaknesses of these technologies, a wave of legal litigation might be expected when biometric systems are implemented in all areas of society.
- The right to privacy protected by the fourth amendment may be in jeopardy by the massive application of biometric technologies.
  - Surveillance is a perfect example in which the balance between public security and the right to individual privacy may be at the hands of people who favor the sharing of biometric information with different purposes other than ensuring public safety in clear violation of the fourth amendment.



## Legal Consequences of Biometric Applications

- The “reasonable search” part of the fourth amendment has been the subject of profound, not yet solved, legal battles before biometric technologies appeared in society.

- With the implementation of automatic and instant methods to recognize people and the pace at which biometrics technology is changing, citizens often do not have time to react and ensure their rights have not been violated.



## Legal Consequences of Biometric Applications

- The “Facebook” and “My Space” generations seems to do not mind sharing not only personal information but also biometric information publicly, making it extremely easy for anyone “in the network” to gather biometric information.
- Social consequences brought by biased algorithms discrimination, hacked databases and not well understood.
- Privacy policies in surveillance or in social websites containing biometric information undoubtedly will carry profound legal consequences

Questions ?