AL YAMAMAH UNIVERSITY

Biometrics in Security

Ethical Implications & Privacy Risks

Biometrics

Biometrics are measurable physical or behavioral traits used to verify identity.

Ethical Challenges

Using biometric data without owner's consent is unethical.

The ***Islamic view*** aligns with the deontological perspective — actions must be inherently good

Privacy Concerns

Biometric data is unique and permanent, but theft is a significant risk.

1. Data ***theft*** during storage/ transmission.

2. Identity theft ***risk***.

Risks in Practice

Biometric data is unique and permanent, but theft is a significant risk.

1. **Spoofing & Impersonation:** Fake fingerprints or voice recordings.
2. **Integration Challenges:** Poor system integration increases vulnerabilities.

ADVANTAGES

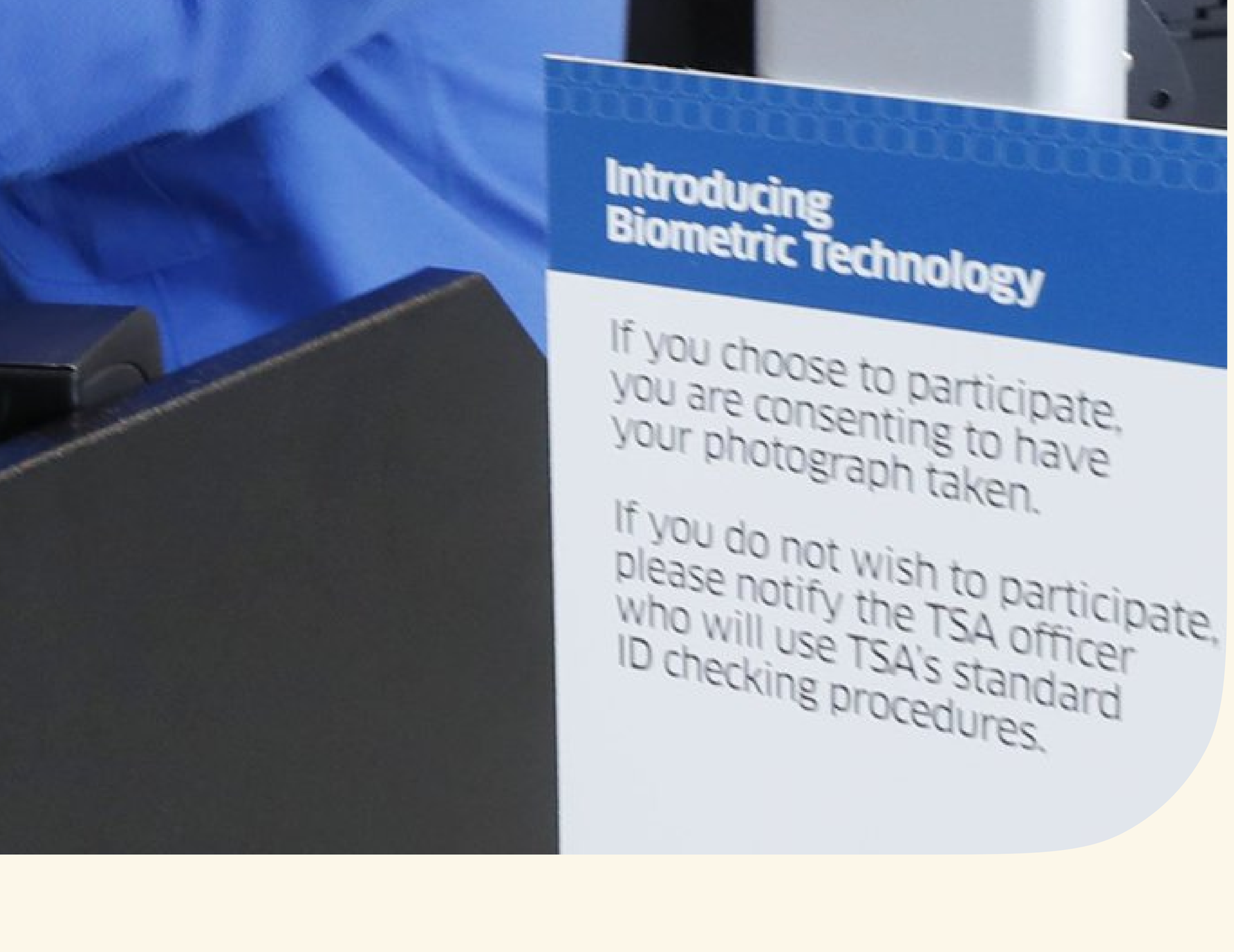
1. **Enhanced** security
2. **Accuracy** & reliability
3. **Real-time** authentication
4. **Convenience**
5. **Non-transferability**

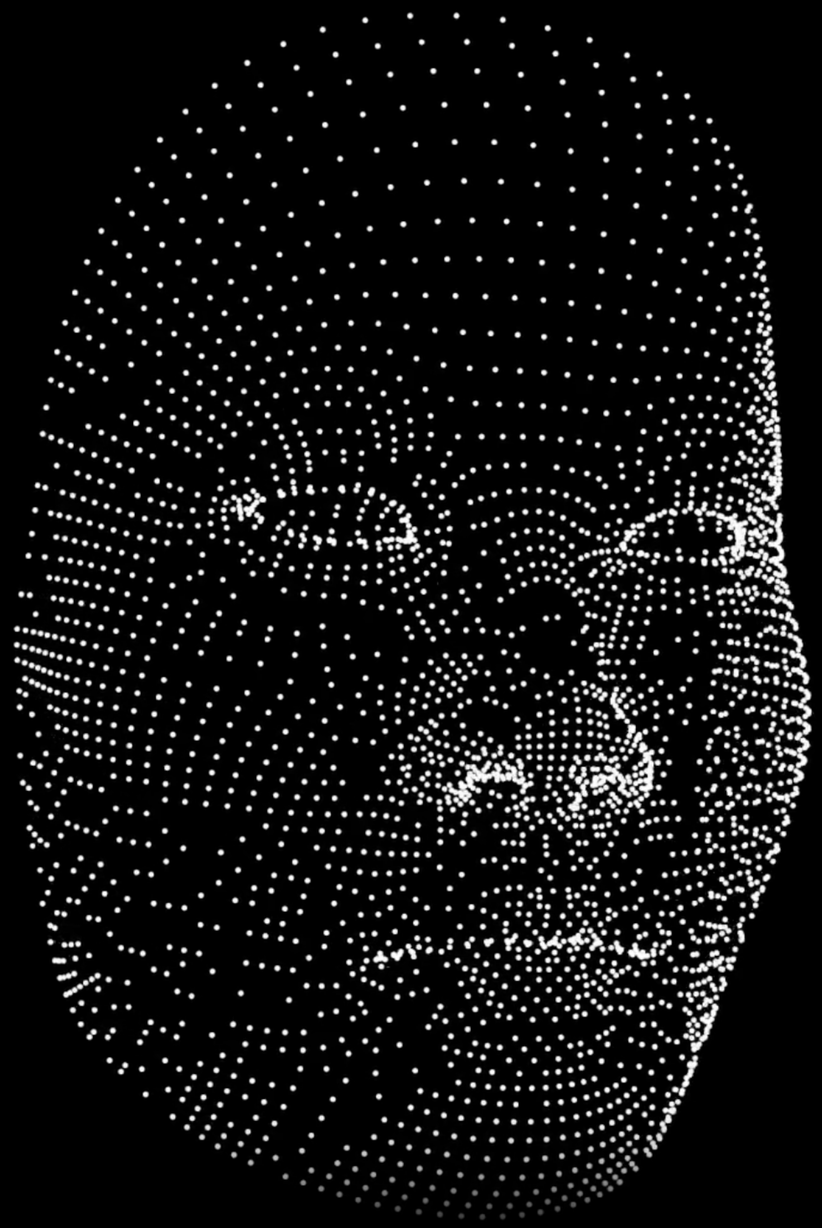
DISADVANTAGES

1. **Cannot be changed** if compromised
2. **Risk** of spoofing
3. **Risk** of improper handling

Real-life Applications

TSA uses face id for quick verification in airports.


Introducing
Biometric Technology
If you choose to participate,
you are consenting to have
your photograph taken.
If you do not wish to participate,
please notify the TSA officer
who will use TSA's standard
ID checking procedures.



iPhone Face ID

Ethics & Best Practices

Balance innovation with responsibility.

1. Use data only for intended purposes.
2. Securely store and transmit the biometric data.
3. Educate users about privacy risk.

Thank You!