Abed Al Rahman
Achille Dubois
Sára Kubalíková
Yunhan Shi
BAI Taoyu

# Facial Recognition & Privacy

## By Biometric Watchdogs (Group-9)

# Outline

—

Introduction of FRT

Negatives of FRT

Survey

Proposed solution

# What is Facial Recognition ?

- FRT identifies individuals based on unique facial features.

Common Uses:

- Unlocking phones
- Security & surveillance
- Retail and marketing analytics
- Law enforcement & border control

# How Does FRT Work?

- Image capture
- Preprocessing
- Feature extraction
- Template creation
- Matching

# Our Research Goals

1. Analyze the ethical risks of facial recognition.

2. Investigate public opinion on FRT.

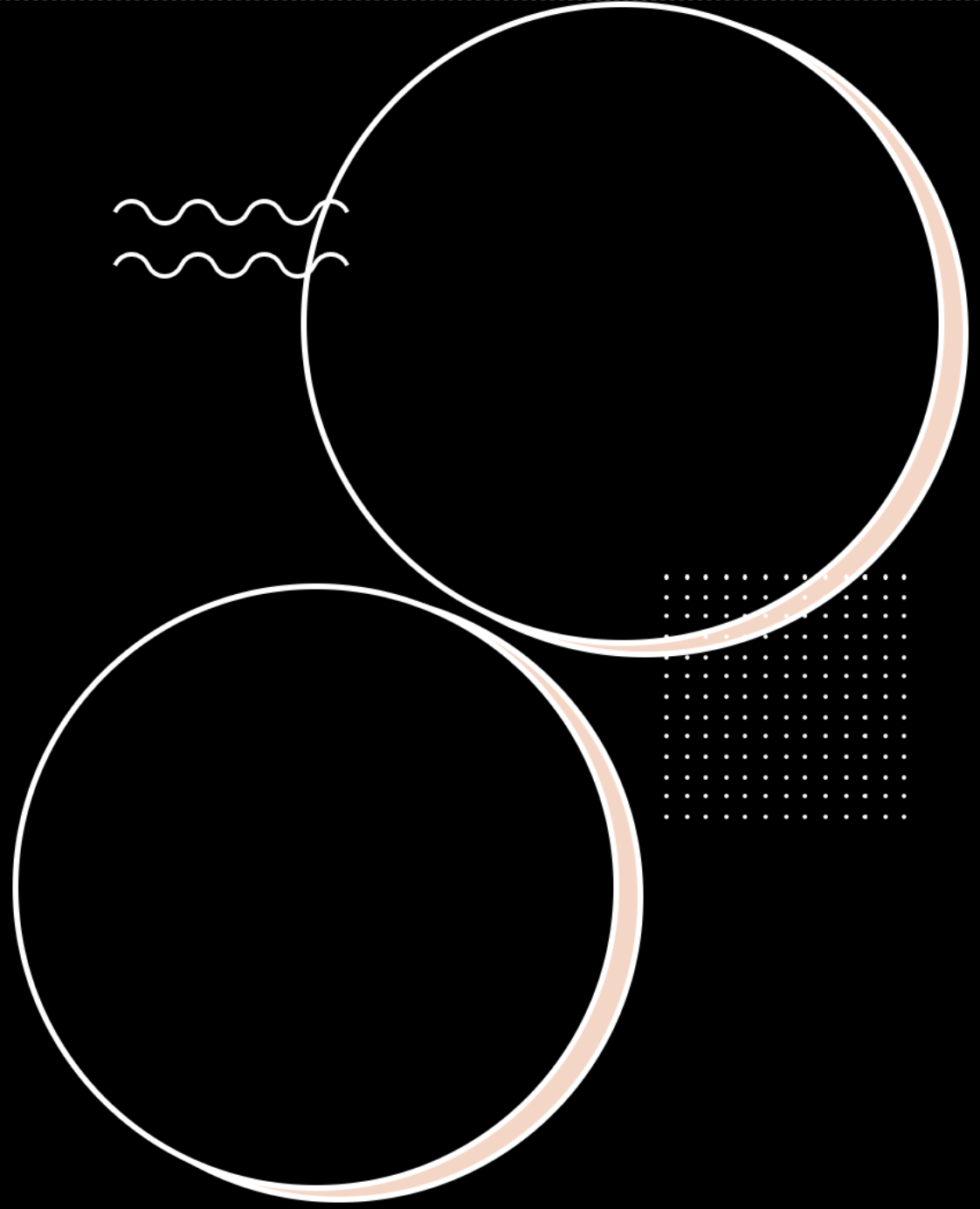
3. Propose a privacy-focused solution to protect users.

# Privacy & Security Risks

- Mass surveillance without consent
- Data breaches and identity theft
- Unauthorized storage of biometric data
- Facial data cannot be changed if leaked

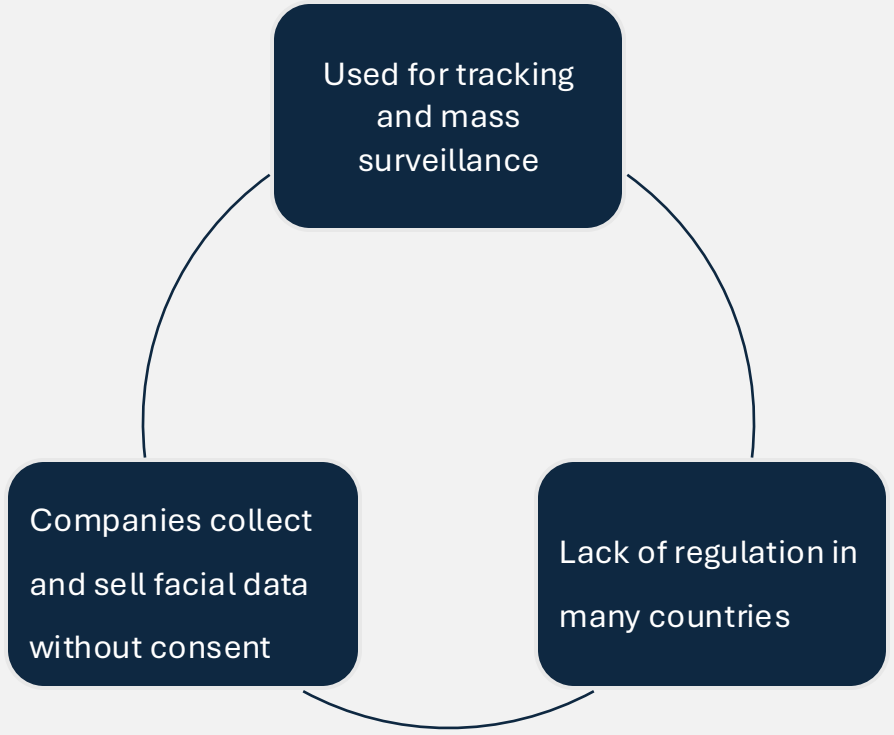
# Privacy & Security Risks

- Higher error rates for women and people of color
- Some systems misidentify minorities at higher rates
- Cases of wrongful arrests due to FRT errors



# Government & Corporate Misuse

The misuse of facial recognition by governments and companies raises major concerns about privacy, discrimination, and excessive surveillance



# Survey Findings

- We conducted a survey to understand public awareness and concerns about FRT.
- How many people answered...

**127 CityU Students**

**58% Undergraduate**

**42% Postgraduate**

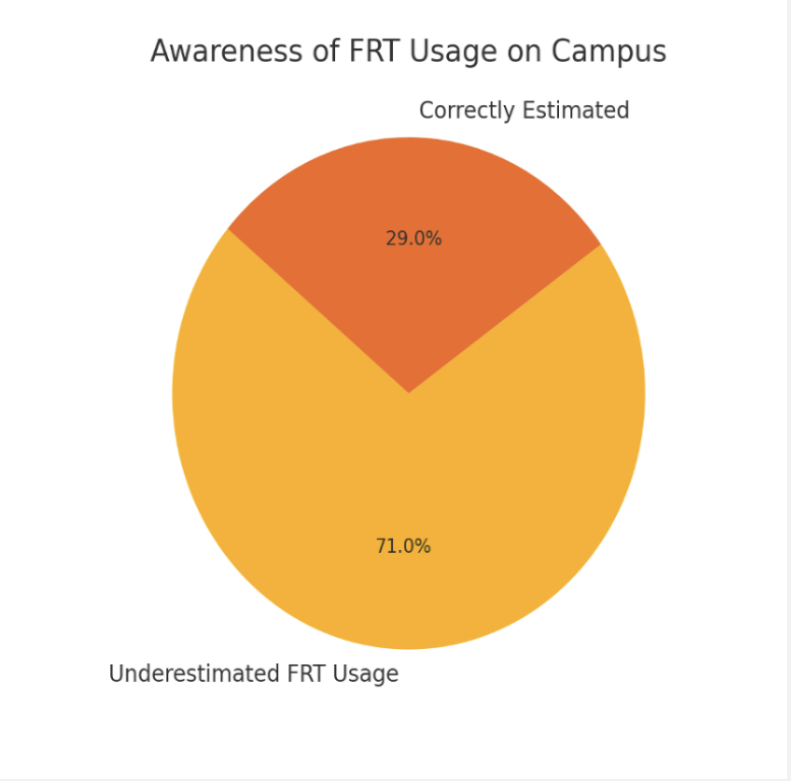
| | |
|---|---|
| **32% Engineering** | **28% business** |
| **22% Humanities** | **18% Science** |

# Survey Findings

**Can the students correctly estimate the usage of FRT on Campus ?**

Clearly **NO !**

More than 70% underestimate the usage

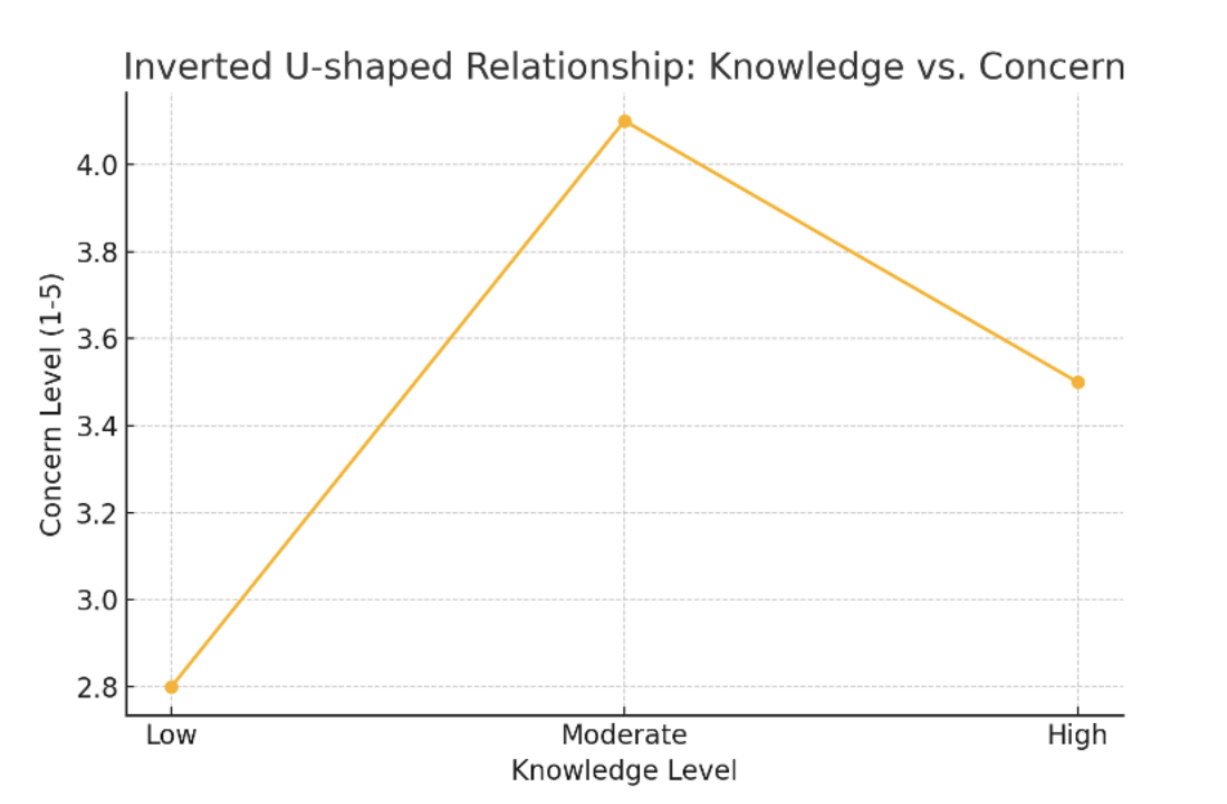


# Survey Findings: Key Words

## Another interesting statistic

The more concerned people about facial recognition are not the ones who know the most about the topic

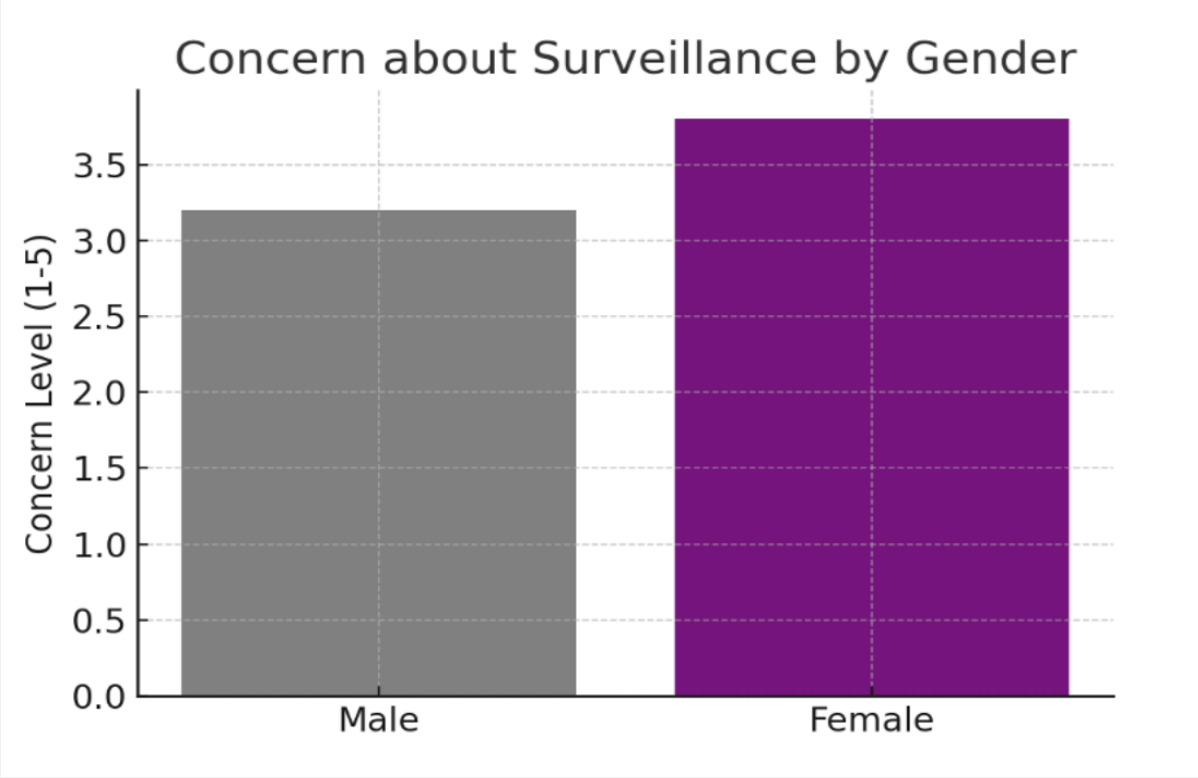
Also, the people with a high knowledge about Facial recognition are more concerned than the people with a low one



# Survey Findings

Female participants reported 18% higher concern levels about surveillance than male peers

though no significant gender differences emerged in protective behaviors



# Why Current Protections Are Not Enough

- Many laws don’t cover biometric data properly.
- Users can’t control where their facial data is stored.
- Companies refuse to delete biometric data upon request.

# Introducing 'RemoveMe'

A privacy tool that:

- Tracks and removes unauthorized facial data
- Scans databases and alerts users
- Files legal removal requests

# How 'RemoveMe' Works

1. **Scan:** Detects where your face is stored online.
2. **Notify:** Alerts you if your data is in unknown databases.
3. **Request Removal:** Automates legal requests to delete biometric data.
4. **Monitor:** Continues scanning for future threats.

# Why 'RemoveMe' is Needed

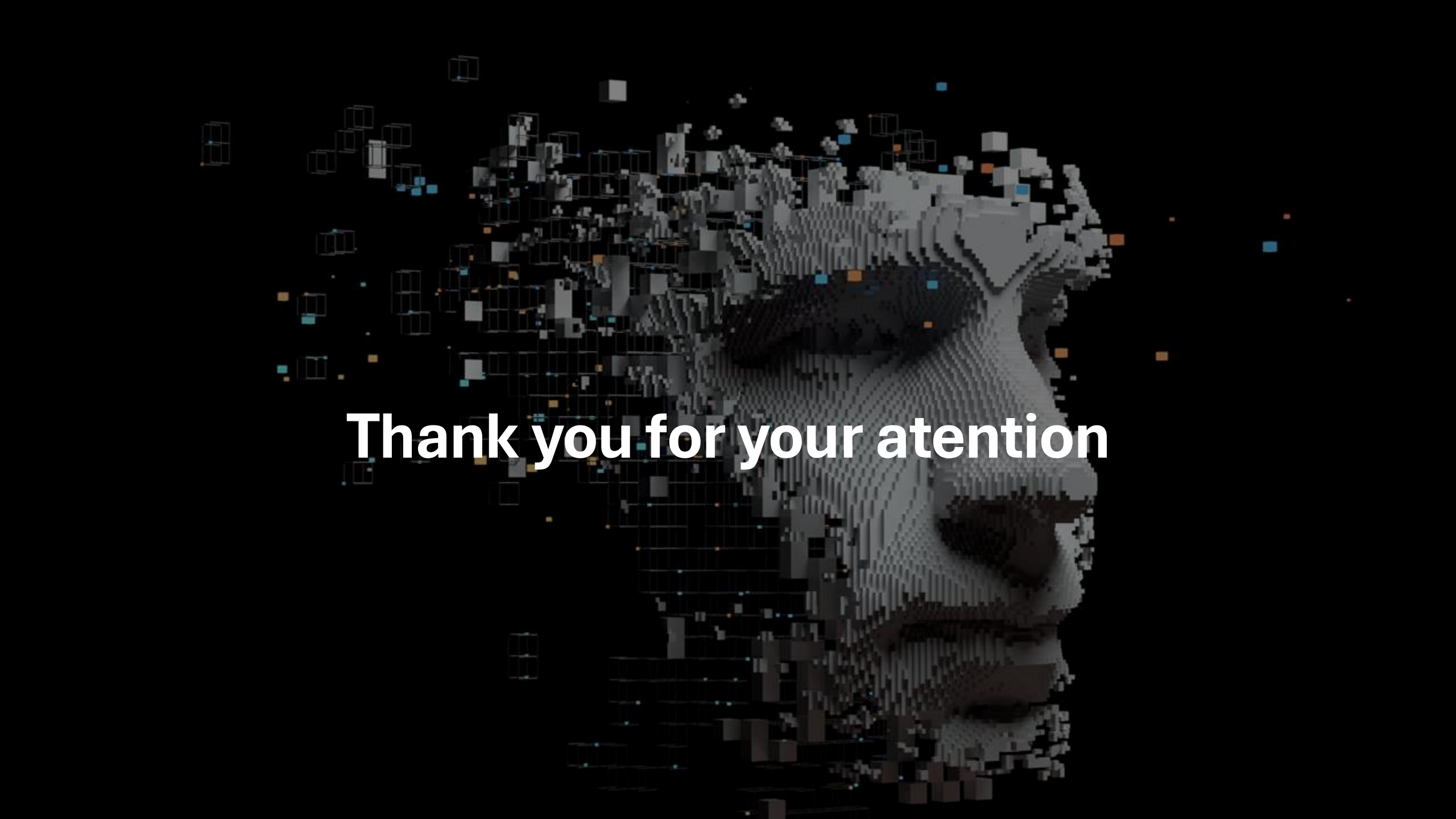
- 84% of surveyed participants said they would use a service like this.
- Most people **don’t know** where their biometric data is stored.
- RemoveMe helps enforce privacy rights and prevent **data misuse**.
- Without intervention, facial recognition could become **a tool for unchecked surveillance**.

# How 'RemoveMe' Can Be Implemented

- Partnering with **privacy advocacy groups** to push for legal action.
- Lobbying for **stricter biometric data protection laws** worldwide.
- Encouraging **companies to comply** with removal requests via legal pressure.

# Conclusion

- Facial recognition has benefits but also **serious risks**.
- Public awareness is **low**, but concern is **high**.
- With tools like **RemoveMe** and better privacy laws, we can ensure technology serves people—not the other way around.


Thank you for your atention