User Verification
Why Facial Recognition isn't the Answer

OVERVIEW

Facial recognition is broadly promoted but is a significantly misunderstood approach for user verification. On the surface, facil recognition sounds simple; take a picture to verify a person's identity and store it as evidence. Unfortunately, using facial recognition causes a lot of larger problems as a result. From accuracy concerns to privacy issues, liability risks to regulatory compliance challenges, know the facts about facial recognition and why it is the **wrong approach** for addressing student verification issues in distance learning.

FACIAL RECOGNITION FLAWS

Inaccuracy

- Struggles to identify different genders
- Results differ by race and ethnicity
- Subject to environment limitations and image obstructions (lighting, facial hair, hats)

Privacy Concerns

- Creates large volumes of sensitive, personal data
- Background images lack required GDPR personal data consent

Costly

- Requires purchase of costly hardware for consistent results
- Necessitates large data storage
- Algorithms only work well for 1-2 years before replacement

Liability

- Facial recognition data is susceptible to hacking and security breaches
- Misuse, loss, or mismanagement of personal data can lead to lawsuits and fines

SUMMARY

Facial recognition technology can play an important role in identity verification, but only in proper circumstances such as airports and other government agencies with specialized equipment, and whom are shielded from privacy liability. Varied use environments and image technologies makes data inconsistent, equipment costs are impractical, and inaccuracies make results unreliable. Using facial recognition for student verification in distance learning scenarios, is not the best option.

Contact **CPaT** to learn more about our solution for user identificaiton.

Account Hacked Alert

WHAT THE EXPERTS ARE SAYING

"Biometrics are generally a good alternative to passwords, but authentication via face-scanning is a terrible idea."

- PC Magazine (Eddy, Max, 2019, November 27).

"It seems that facial recognition is being promoted as a solution for a problem that does not exist. That is why a number of jurisdictions around the world have moved to impose a moratorium on the use of the technology."

- European Union (Wojciech, W. 2019, October 28).

"The goal of "accuracy" implies a logic that irresistibly leads towards an endless collection of (sensitive) data to perfect an ultimately un-perfectible algorithm. In fact, there will never be enough data to eliminate bias and the risk of false positives or false negatives."

- European Union (Wojciech, W. 2019, October 28).

"We found empirical evidence for the existence of demographic differentials in the majority of contemporary face recognition algorithms that we evaluated."

- NIST (Grother, Patrick, Ngan, Mei., & Hanaoka, Kayee, 2019).

"With respect to race, false positive rates are highest in West and East African and East Asian people. We found false positives to be two to ten times higher in wome versus men."

- NIST (Grother, Patrick, Ngan, Mei., & Hanaoka, Kayee, 2019).

REFERENCES

- Grother, Patric., Ngan, Mei., & Hanaoka, Kayee. (2019). Face Recognition Vendor Test

  (FRVT) Part 3: Demographic Effects, *National Institute of Standards and Technology.*
  NIST.IR. 8280. Retrieved September 28, 2020, from
  https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

- Eddi, Max. (2019, November 27). *Facial Recognition is Tech's Biggest Mistake*. Pc Magazine.

  Retrieved September 28, 2020, from
  https://www.pcmag.com/opinions/facial-recognition-is-techs-biggest-mistake

- Wojciech, W. (2019, October 28). *Facial Recognition: A Solution in Search of a Problem.*

  European Data Protection Supervisor. Retrieved September 28, 2020, from
  https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en