All images created using DALL- E 3

Navigating Ethics in Facial Recognition: A Comparative Review of Regulations in Law Enforcement

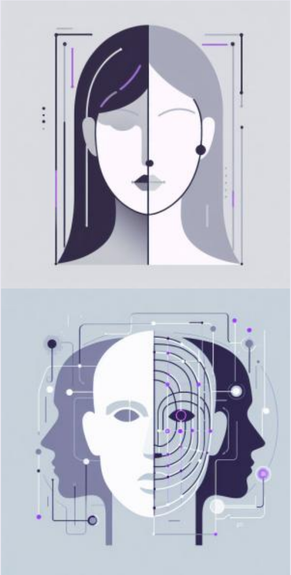
Analysis based on 'The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks' by D. Almeida, K. Shmarko & E. Lomas

> 'We will not sell facial recognition technology to police departments in the United States until we have a national law in place, grounded in human rights.' – Microsoft on lack of legislation

> 'We basically do not know how data are used by those who collect it, who has access and to whom it is sent, how long do they keep it, who is responsible at the end for the automated decision making.' – European Data Protection Supervisor on the lack of FRT accountability and transparency

> 'Clearview AI openly discloses information about scraping Facebook user profiles for images to build up its reference database. ' – provider of FRT to 600+ police departments across the USA

INTRODUCTION



Facial Recognition Technologies (FRT): an automated way for identifying individuals by analyzing and mapping their features and comparing them to other images using AI and algorithms.

Context

The development and rollout of FRT by law enforcement raises ethical concerns:

- To what extent is the surveillance of citizens acceptable?
- How can individual privacy rights and citizen safety be balanced?
- How can these technologies be globally?

Problem Addressed

Research focus on ethical concerns linked to the use of FRT by law enforcement, pros and cons of these technologies as well as current and potential ways to ensure accountability and the balance of individual privacy rights and citizen safety.

Accountability in law enforcement: the state is responsible for choices made regarding the rollout of technologies and their impact.

Problems Created by FRT:

- Accountability concerns
- Transparency concerns
- Privacy invasion
- Human rights violations

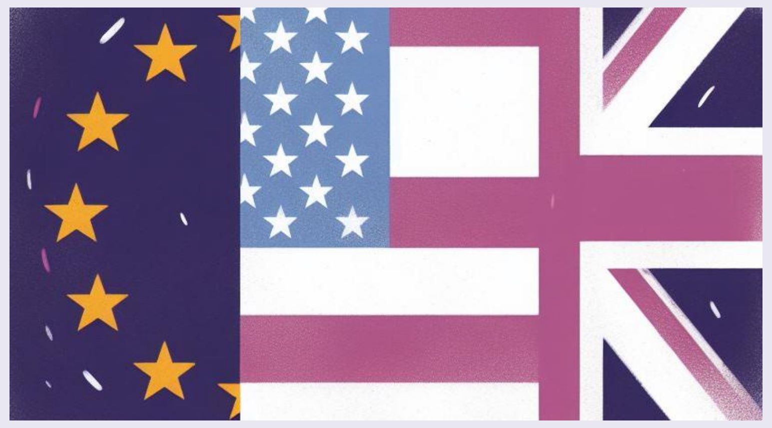
Problems Solved by FRT:

- Safety of citizens
- Altering power dynamics

RESEARCH

Research Method

Comparative Analysis of EU, UK and US regulatory frameworks on the use and misuse of FRT by authorities, drawing conclusions from legislation to court cases.



Analysis

/	EU	UK	US
Data Protection & Privacy	GDPR with PbD	Data Protection Act	Varies state-by-state
Human Rights	European Convention on Human Rights	Human Rights Act	Not compared to EU
Freedom of Information	Accountability differs state-by-state		Better than EU
Regulators (Data Protection Authority)	✓	✓	✗
Ability to sue	✓	✓	✓
DPIA	✓	✓	✗
FRT Deployment	Slower compared to the US	Slower compared to the US	Faster compared to EU & UK
Transparency	Better than US	Better than US	Worse than EU
Accountability	Good	Good	Bad

Privacy by Default and Design (PbD): critical focus on data protection when processing, right to know data held, right to be forgotten, only needed data to be collected, etc.

Data Protection Impact Assessment (DPIA): assessing risks in every step of data processing to ensure it is 'fair and lawful'.

EU & UK: critical focus on developing accountability requirements and personal data management , stricter regulations on biometric data (explicit consent, but exemption of law enforcement varies state by state), DPO exists, regulators required to investigate complaints with effective data protection interventions, privacy and human rights laws in place 'one strike and you're out' legislation, overall better unity amongst states.

Biometric data: 'physical or behavioral characteristics that uniquely identify an individual, including DNA, fingerprints, faces, and voice patterns.'

Data Protection Officer (DPO): mandatory for public authorities with core activity in large-scale, special data processing, required to advise on data protection compliance.

US: FRT heavily used by authorities but regulatory framework lacks, less emphasis on privacy and data protection, Publication Information Act exists but no regulators on privacy, heavy reliance on individual legal action

CONCLUSION

Main Finding

In the safe and successful use of FRT the following are critical:

- explanation of FRT use
- regulation
- accountability
- transparency
- audits
- documentation
- consideration of diversity, inclusion and equality
- publicly available DPIA and Human Rights Impact Assessments by all authorities
- global regulators able to investigate and sanction
- application in individual context

Recommendations

10 questions to answer when developing and deploying FRT for lawmakers and developers:

1. Who controls FRT development to prevent bias?
2. When/where is FRT usage ethical?
3. How to ensure fair consent and transparency in FRT use?
4. What justifies creating and using facial data banks?
5. How to ensure fairness in data bank use avoiding scraping?
6. What are FRT's limitations in different contexts?
7. How to hold FRT usage accountable?
8. How to enforce and explain FRT accountability?
9. Are complaint processes accessible to all?
10. Can counter-AI initiatives test law enforcement systems?

Created by Rafain Emőke (Data Science)