

AI & Transparency : The case of Facial Recognition Technology

Lorelien Hoet
Director Government Affairs EU





Microsoft has adopted facial recognition principles

1. Fairness

2. Transparency

3. Accountability

4. Non-discrimination

5. Privacy protection:
notice & consent

6. Lawful surveillance

Transparency/Intelligibility : data quality

The New York Times

Facial Recognition Is Accurate, if You're a White Guy

By STEVE LOHR FEB. 9, 2018



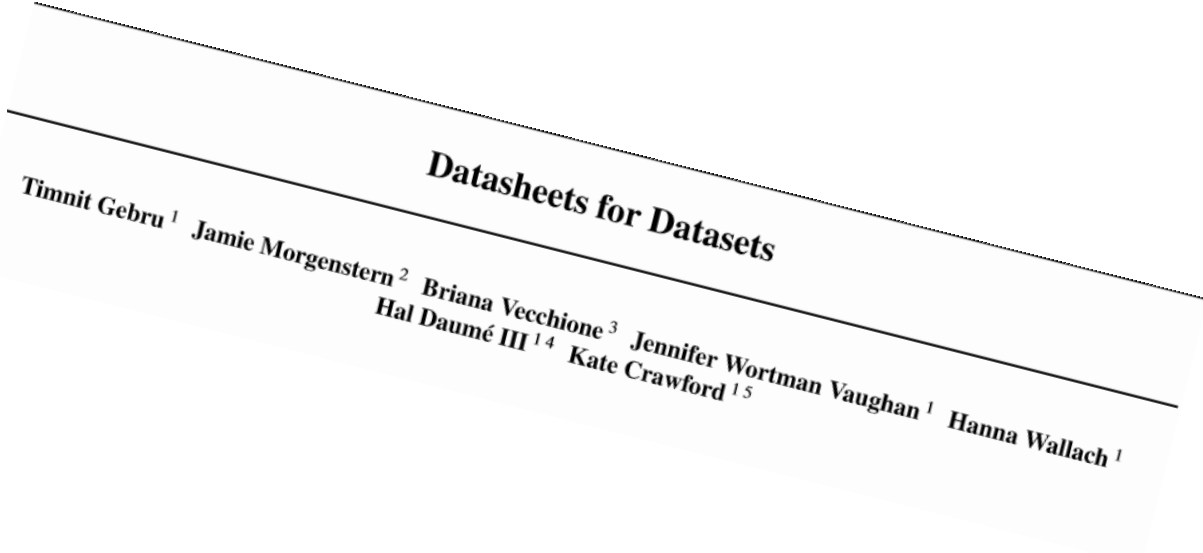
Gender was misidentified in up to 1 percent of lighter-skinned males in a set of 385 photos.

Gender was misidentified in up to 12 percent of darker-skinned males in a set of 318 photos.



Gender was misidentified in up to 7 percent of lighter-skinned females in a set of 296 photos.

Gender was misidentified in 35 percent of darker-skinned females in a set of 271 photos.



Transparency/Intelligibility : about how the system works

Transparency Note

Azure Cognitive Services: Face API

Last Updated 3/29/19

- Awareness about the accuracy
- Full FRT lifecycle
- Improve robustness & safety
- Easier identification & fixing of bugs
- 3rd party testing for FRT online services

Transparency/Intelligibility : about the outcome

- Different use cases
- Different levels of human controls

South Wales Police use of facial recognition ruled lawful

By Jenny Rees
BBC Wales home affairs correspondent

© 4 September 2019

[f](#) [t](#) [t](#) [✉](#) [Share](#)



Transparency/Intelligibility : about the outcome

➤ Different models

Simple
models



Complex
models

Research being done on :

- LIME “local interpretable model-agnostic explanations”
- Counterfactual explanations
- BETA “black-box explanations through transparent approximations”

➤ Different audiences

Transparency : about the use of FRT



- Proactive & reactive communication
- Feedback loop

Statement from Elizabeth Denham, Information Commissioner, on the use of live facial recognition technology in King's Cross, London.

“ Scanning people’s faces as they lawfully go about their daily lives, in order to identify them, is a potential threat to privacy that should concern us all. That is especially the case if it is done without people’s knowledge or understanding.