Merykokeb Belay

Mary Kryslette Bunyi

Maryam Khalid Shah

**Case Proposal:**

**Using Facial Recognition Technology (FRT) for Law Enforcement**

In 2017, Ed Bridges was on his lunch break in Cardiff city center when his image was captured by ‘AFR Locate’ – an automatic facial recognition (AFR) software being used by the South Wales Police (SWP) that would automatically scan the faces of people and compare them to images on a database of persons of interest[[1]](#footnote-1). SWP first used this software during the 2017 UEFA Champions League Final in order to identify troublemakers[[2]](#footnote-2), and had been testing it at other large events across the area since then.

A few months later when Mr. Bridges’ image was captured again at a peaceful protest, he brought the case to court with the help of Liberty, a civil rights group, arguing that the use of the tool breached his data protection and equity laws as well as his rights to privacy[[3]](#footnote-3). After the High Court of London ruled against Mr. Bridges, his subsequent appeal was upheld by the Court of Appeals on the following three points: there was no clear guidance on where AFR Locate could be used and who could be put on a watchlist, a data protection impact assessment was deficient and the force did not take reasonable steps to find out if the software had a racial or gender bias[[4]](#footnote-4).

Responding to the ruling, SWP said that it was committed to carefully developing and using the technology which had resulted in 61 people being arrested for offences including violence and robbery, while causing no unlawful arrest[[5]](#footnote-5).

***Ethical implications***

The South Wales case brings up ethical issues around algorithmic accountability and equity. We want to examine how the decision and the process to implement this technology excluded members of the public. We also want to assess how the design and ‘hand-off’ process lacked sufficient oversight and input from the police force, but more importantly, the residents who would be subject to this technology. Is the lack of public accountability a missed opportunity to engage with stakeholders and residents? Does this technology take away limited public resources that could have been invested towards less invasive interventions? How does the police force’s disregard for machine-generated bias reflect power imbalances in decision making? Additionally, how does this disregard affect the implementation, outcome, and effectiveness of this technology? Given AFR Locate’s high rate of false positives, is it fair to subject people to this type of surveillance?

The case also raises important questions on the issue of inflicting private harm for the greater public good. To what extent should privacy be sacrificed in the name of national security? Where does one draw the line between intrusion and intelligence gathering? In view of pressures after the massive intelligence failure blamed for the 9/11 attacks[[6]](#footnote-6), how can law enforcement agencies proactively preclude the emergence of threats while preventing surveillance creep? How should AFR technology be governed to safeguard civil liberty while considering the urgency of countering criminal elements before they are able to carry out crimes? Who should be involved in the oversight process? How can the public have a greater voice in asserting their rights and demanding accountability without compromising confidential intelligence operations?

**Bibliography**

Bethan, Martin, and Andrew Dawson. *An Evaluation Of South Wales Police’s Use Of Automated Facial Recognition*. Cardiff University, 2018. <https://crimeandsecurity.org/s/AFR-Report-Digital.pdf>.

Rees, Jenny. “South Wales Police use of facial recognition ruled lawful”. *BBC News*, September2019. <https://www.bbc.com/news/uk-wales-49565287>.

Rees, Jenny. “Facial recognition use by South Wales Police ruled unlawful”. *BBC News*, August2020. <https://www.bbc.com/news/uk-wales-53734716>.

Shead, Sam. 2020. "UK Court Finds Facial Recognition Technology Used by Police Was Unlawful." *CNBC*, August 20, 2020. <https://www.cnbc.com/2020/08/11/swp-facial-recognition-unlawful.html>.

U.S. National Commission on Terrorist Attacks upon the United States. *9/11 Commission Report: The Official Report of the 9/11 Commission and Related Publications,* by Thomas H. Kean and Lee Hamilton, Y 3.2:T 27/2/FINAL, Washington, D.C.: GPO, 2004. <https://govinfo.library.unt.edu/911/report/index.htm>.

1. Shead, Sam. 2020. "UK Court Finds Facial Recognition Technology Used by Police Was Unlawful." *CNBC*, August 20, 2020.  [↑](#footnote-ref-1)
2. Bethan, Martin, and Andrew Dawson. *An Evaluation Of South Wales Police’s Use Of Automated Facial Recognition*. [↑](#footnote-ref-2)
3. Rees, Jenny. “South Wales Police use of facial recognition ruled lawful”. *BBC News*, September2019. [↑](#footnote-ref-3)
4. Rees, Jenny. “Facial recognition use by South Wales Police ruled unlawful”. *BBC News*, August2020. [↑](#footnote-ref-4)
5. Rees, Jenny. “Facial recognition use by South Wales Police ruled unlawful”. *BBC News*, August2020. [↑](#footnote-ref-5)
6. U.S. National Commission on Terrorist Attacks upon the United States. *9/11 Commission Report: The Official Report of the 9/11 Commission and Related Publications,* by Thomas H. Kean and Lee Hamilton, Y 3.2:T 27/2/FINAL, Washington, D.C.: GPO, 2004. [↑](#footnote-ref-6)