Dr Kay L. Ritchie, Senior Lecturer in Cognitive Psychology at University of Lincoln — Written evidence (NTL0003)

Dr Kay Ritchie is a Senior Lecturer in the School of Psychology at the University of Lincoln. Kay is an expert in human face perception and face recognition. Her current work is focussed on human and computer face identification, as well as public attitudes towards the use of facial recognition technology.

Automatic facial recognition technology, policing, and the law

Section 1. The use of automatic facial recognition (AFR) technology in the application of the law

1. AFR has been integrated with CCTV and used by some police forces in the UK for a number of years. AFR is typically used by the police to match the digital representations captured by the technology with images present in a database [1]. In theory, this database could contain images of every citizen, or only images of individuals on a 'watchlist' [2].

2. Watchlists are created by authorities and contain information about a person of interest, typically fugitives and those deemed to require close surveillance [2].

3. There are two main types of deployment of AFR that are of use to police, and in both of these false positives are likely to occur. False positives refer to errors whereby a face algorithm, or a human that is using the algorithm to generate a list of potential matches to an image of a face, incorrectly matches a face from a database to an image used to search that database.

4. The first 'retrospective' use of AFR by police is to search databases of (e.g.) mugshots using an image of an unfamiliar face (e.g. from an ID photo, a CCTV image, or a smartphone).

5. The second use of AFR by police is 'live' where data streams from CCTV are monitored by face recognition algorithms in real time, and typically check each face that is detected in the CCTV stream against a 'watchlist' of people that the police would like to identify.

6. Trials of live AFR deployed on city streets by police in the UK (London Metropolitan Police Service and South Wales Police) have reported high numbers of false positives [2-3].

7. False positives can have serious consequences. In police investigation for example, high rates of false positives may lead to innocent individuals being suspected of crimes, and even wrongful conviction. Large proportions of false leads in an investigation can also lead to significant inefficiencies in the use of police resources.

Section 2. The reliability of AFR, impact upon the rule of law, and trust in the rule of law and its application

8. In recent years, there has been a rapid improvement in the performance of facial recognition algorithms through the use of 'Deep Convolutional Neural Networks'[4].

9. Different AFR algorithms are optimised to perform most accurately with different types of images, therefore an algorithm which performs well with high quality images may not perform as well with blurry or pixelated images such as those captured by older CCTV systems.

10. Demographic biases in AFR have been a cause for concern in recent reports because they contravene the fundamental human right that citizens should be treated equally

11. A recent independent report has shown that algorithms may produce different levels of false positives for faces of different ethnicities. Some algorithms gave rise to between 10 and 100 times more false positives for Asian and African American faces compared to Caucasian faces. However other algorithms showed no differences in accuracy between faces of different ethnicities [5].

12. My group's recent survey of public opinion about the use of AFR in criminal justice settings is the first to survey the public in the UK, USA, Australia and China [6]. Both our survey, and another survey of the UK public only [7], showed that support for the use of AFR depends greatly on what the technology is used for, and who it is used by.

13. Our survey showed that trust is a major concern for the public – trust is highest for the police, followed by government, and lowest for private companies [6]. Differences in the accuracy of AFR across different demographics was of concern to the public surveyed.

14. To better understand the reliability of AFR, and the impact of its use on trust in the rule of law, I submit the following as evidence to the Justice and Home Affairs Committee:

a. State-of the art face recognition algorithms have improved markedly in recent years and now make very few errors **when comparing high quality images where the image is a recent likeness of the person** [4].[1]

b. **When image quality is not optimal**, as is true of some CCTV images, even the very best state-of-the-art **algorithms make substantial proportions of false positive responses** [4].

c. The Justice and Home Affairs Committee, and police users of algorithms, should be aware of **differences in the accuracy of an algorithm depending on its optimisation, and for different demographics of people** [5].

d. **The public are concerned about the use of AFR** [6-7], **and only support its use by certain users and under certain circumstances** e.g. by the police to search for people who are on a watchlist, but not to search for people who are not on a watchlist [6].

[1] *It should be noted that the technologies attaining high levels of performance in current international benchmark tests [4] will sometimes take years to come to market and so these reports do not represent current operational accuracy*

Section 3. AFR in the existing legal framework – the need for legislation

15. Although the use of face images in investigative settings by police is not regulated, the use of images as evidence in legal proceedings is more regulated by various rules of evidence and procedure (e.g. PACE (1978) in England and Wales).

16. The admissibility of an identification by AFR has yet to be considered by a court in England or Wales.

17. The UK's surveillance camera commissioner and a surveillance camera code [8] do not mention AFR.

18. In the UK, the Data Protection Act 2018 states that any identification 'decision' made by an algorithm must be checked by a human.

19. English courts admit the opinions of investigating police and those recognised as experts, and allow experts to make claims about similarities between images, as well as categorical identifications [9].

20. Our recent survey of public opinion found that the public are more supportive of the use of AFR in courts to secure convictions when it is used in conjunction with other evidence, as opposed to without other evidence [6].

21. I submit the following as evidence to the Justice and Home Affairs Committee:

e. The fact that humans must review the output of face recognition searches is problematic, because decades of psychological research shows that **people are very poor at identifying unfamiliar faces by comparing images** and make large proportions of errors [e.g. 10].

f. In recent tests that have directly tested performance of professional staff that are required to review candidate lists – and decide in the person of interest is present in the candidate list – **Australian passport issuance officers made false positives on 40% of occasions** [11].

g. However, **combining algorithm and human judgements may yield the highest accuracies** for the most challenging conditions including identification across changes in pose and lighting as well as identification from blurry images and videos [12, 13].

Section 4. Guiding principles for the use of AFR in the application of the law.

22. I submit the following as evidence to the Justice and Home Affairs Committee:

h. Developers, system designers, vendors, and users of AFR should do more to **publicise the use, data privacy, and accuracy of AFR**.

i. Users of AFR (including the police) should **justify their use case and know the capacity of their system**

j. **There is a need for further public consultation** on the use of facial recognition technology by the police [6, 7].

k. **There is a need for regulation** (legislation and guidelines in PACE), **and the government should provide clear legislation** for the use of AFR in the application of the law before facial recognition technology is put into wider use [6].

I am happy to provide further information on any of the points mentioned in this submission.

6 August 2021

REFERENCES

1. Centre for Data Ethics and Innovation. (2020) Snapshot series: Facial recognition technology.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/905267/Facial_Recognition_Technology_Snapshot_UPDATED.pdf

2. Fussey, P., & Murray, D. (2019). Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology. University of Essex Human Rights Centre. http://repository.essex.ac.uk/24946/

3. Davies, B., Innes, M., & Dawson, A. (2018). An Evaluation of South Wales Police's Use of Automated Facial Recognition. Cardiff University.
https://crimeandsecurity.org/feed/afr

4. Grother, P., Ngan, M., & Hanaoka, K. (2021). Face Recognition Vendor Test Part 2: Identification. National Institute of Standards and Technology, US.
https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf

5. Grother, P., Ngan, M., & Hanaoka, K. (2019). Face Recognition Vendor Test Part 3: Demographic Effects. National Institute of Standards and Technology, US.
https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

6. Ritchie, K. L. et al (in revision). Public attitudes towards the use of automatic facial recognition technology in criminal justice systems around the world.
https://792cc68a-8daa-4129-ba89-a6bb517c1620.filesusr.com/ugd/ac0889_0dfc98060f8048218868fa7b27332d1c.pdf

7. Ada Lovelace Institute (2019). Beyond face value: Public attitudes to facial recognition technology.
https://www.adalovelaceinstitute.org/wp- content/uploads/2019/09/Public-attitudes-to-facial-recognition- technology_v.FINAL_.pdf

8. Home Office. Surveillance camera code of practice. (2013).
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf

9. Attorney-General's Reference (No. 2 of 2002). England and Wales court of appeal (criminal division)
https://www.casemine.com/judgement/uk/5b46f1ed2c94e0775e7ee3e9

10. Ritchie, K. L. et al. (2015). Viewers base estimates of face matching accuracy on their own familiarity: Explaining the photo-ID paradox. *Cognition, 141*, 161-169.
https://www.sciencedirect.com/science/article/abs/pii/S0010027715000980

11. White, D. et al. (2015). Error rates in users of automatic face recognition software. *PLoS One*, *10*(10), e0139827.
https://journals.plos.org/plosone/article/metrics?id=10.1371/journal.pone.0139827

12. White, D. et al (2020). Evaluating face identification expertise: Turning theory into best practice. https://socialsciences.org.au/workshop/evaluating-face-identification-expertise-turning-theory-into-practice/

13. Phillips, P. J. et al. (2018). Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms. *Proceedings of the National Academy of Sciences, 115*(24), 6171-6176. https://www.pnas.org/content/115/24/6171