JUSTICE SUB-COMMITTEE ON POLICING

FACIAL RECOGNITION: HOW POLICING IN SCOTLAND MAKES USE OF THIS TECHNOLOGY

WRITTEN SUBMISSION FROM DR KAY RITCHIE, UNIVERSITY OF LINCOLN AND DR DAVID WHITE, UNSW SYDNEY

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.

Dr David White is a Scottish cognitive psychologist currently working as a Senior Lecturer at the School of Psychology, UNSW Sydney. He has carried out large-scale evaluations of face identification systems used by the Australian Passport Office to protect against identity fraud. He is an expert in accuracy of humans and computer algorithms.

False positives in face recognition search, and public attitudes towards the use of facial recognition technology

Section 1. False positives in face recognition search

1. 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.

2. 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.

3. 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 [1].

4. There are two main types of deployment of face recognition software that are of use to police, and in both of these false positives are likely to occur.

5. First ‘retrospective’, that the Justice Sub-Committee has indicated is currently used by Police Scotland, 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).
6. Second is ‘live’ where data streams from CCTV are monitored by face recognition algorithms in real time, and typically checking each face that is detected in the CCTV stream against a ‘watchlist’ of people that the police would like to identify if and when they appear.

**Retrospective searches using Face Recognition Technology**

7. The ‘retrospective’ capability is currently used in a variety of settings by organisations worldwide to identify unfamiliar faces. Dr White has worked closely with the Australian Passport Office in recent years to improve how this capability is used to protect passports against identity fraud and so is an expert on the accuracy of these systems.

8. To better understand the likelihood of false positives in this type of use, we submit the following as evidence to the Justice Sub-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 [2].

   B. **When image quality is not optimal**, as is almost always true of CCTV images, even the very best state-of-the-art algorithms make substantial proportions of false positive responses [2, 3].

   C. A typical solution to mitigating the risk of false positive responses generated by these computer system is to ensure that the ‘candidate lists’ of potential matches are filtered by human adjudicators, who ultimately decide if the person-of-interest does match a face from the database. This is standard practice in police use of face recognition and the public would expect this oversight.

   D. However, the fact that humans must review the output of face recognition searches is very problematic, because decades of psychological research show that people are very poor at identifying unfamiliar faces by comparing images and make large proportions of errors [e.g. 4].

   E. 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 [5].

---

1 It should be noted that the technologies attaining high levels of performance in current international benchmark tests [1] will sometimes take years to come to market and so these reports do not represent current operational accuracy.
F. The Justice Sub-Committee, and police users of algorithms, should be aware of differences in the accuracy of an algorithm for different demographics of people [1].

**Live searches using Face Recognition Technology**

9. Regrettably, there is very little systematic testing of operational deployments using ‘live’ face recognition technology. However, reports of operational tests that are available [6, 7] suggest that false positives are very common, and may happen on as many as 50-90% occasions. Unfortunately, these statistics do not consider that the face recognition systems used in these tests only return ‘potential matches’ that must be reviewed by humans. But, as noted above, people reviewing these candidate lists typically perform very poorly and so are likely to make many false positives when basing their identification judgments on images alone.

10. Given the recent advances in face recognition technology – with error rates halving roughly every 2 years [2] – it is likely that ‘live’ deployments of this technology will be become more feasible in future than they currently are. However, it is unlikely that these will be so accurate that they do not require human review. Human accuracy in unfamiliar face matching will, therefore, continue to limit the overall accuracy of face identification processes used by police.

**Section B. Public attitudes towards the use of facial recognition technology**

11. As mentioned above, humans are error-prone in making identity judgements by comparing images of unfamiliar faces. We are, however, experts at recognising people who are familiar to us. It is likely that people tend to overestimate their face recognition abilities, and those of others including professionals such as border control officers, by conflating unfamiliar face recognition ability with familiar face recognition [8].

12. Bearing this in mind, and referring to recent high profile criticisms of facial recognition technology accuracy [e.g. 7], it is relevant to consider public attitudes towards the use of this technology. It is possible that the public may prefer the thought of human reviewers to algorithm decisions.

13. A recent survey of people in the UK found that almost half of people surveyed want the ability to opt out of the use of facial recognition technology, and that more than half of the people surveyed want governmental restrictions on police use of this technology [9].

14. Our recent work (as yet unpublished) surveyed public attitudes to the use of facial recognition technology in the criminal justice systems in the UK, China and Australia and found converging views across the three countries [10].
The public in the UK, China and Australia were concerned about privacy, the accuracy of the technology, and the lack of existing regulation [10]. We therefore submit the following as evidence to the Justice Sub-Committee:

G. **There is a need for public consultation** on the use of facial recognition technology by the police [9, 10].

H. The public need and want to understand more about the **accuracy of the systems used, and the ways in which they will be used** [10].

I. **There is a need for regulation** (legislation and guidelines in PACE) before facial recognition technology is put into wider use [9, 10].

We are happy to provide further information on any of the points mentioned in this submission.

Dr Kay Ritchie, University of Lincoln, UK
Dr David White, University of New South Wales, Australia

REFERENCES


