Home Office

Rt Hon Chris Philp MP
Minister of State for Crime, Policing and Fire

2 Marsham Street
London SW1P 4DF
www.gov.uk/home-office

Mr Gus Hosein & Co-signatories
Privacy International
c/o sarahs@privacyinternational.org

DECS Reference: MIN/1105155/24

20 March 2024

Dear Mr Hosein & Co-Signatories,

Thank you for sending me a copy of your letter of 18 January to the Home Secretary about Facial Recognition (FR) Technology.

The Government is committed to empowering police to use new technologies, like FR, while maintaining public trust. Live FR can be used effectively and lawfully to catch criminals and has appropriate safeguards. There is a comprehensive legal framework that governs police use of facial recognition, which is regulated by the Information Commissioner's Office.

The legal framework consists of common law powers to detect and prevent crime, data protection, equality, and human rights law, that is underpinned by the College of Policing's national guidance, available at: https://www.college.police.uk/app/live-facial-recognition. This means that the police can only use it for a policing purpose, where necessary, proportionate and fair to do so.

The College of Policing national guidance sets out when the police can use live facial recognition and the categories of people they can look for. It also requires the police to automatically delete the biometric data of anyone the system does not match to a watchlist.

There are also existing safeguards in place to ensure facial recognition can operate fairly and without bias and FR will never replace the need for human judgement, insight, and empathy. This is not automated decision making; police officers will always make the decisions about whether and how to use any suggested matches.

I note the concerns you have outlined about inaccuracies and bias, however the technology used by the police forces that conduct Live FR deployments has been independently tested by the National Physical Laboratory. This was found to be very accurate and with no statistically significant demographic bias at the settings the police use. The testing of the algorithm by the provider of their technology (NEC) found that the chance of a false match is just 1 in 6000 people walking past the camera. True positive matches were 89%.

Recent trial deployments of Live FR have caught a number of wanted suspects, including, for example, a man who has been wanted for rape since 2017. Without the use of Live FR, he would not have been apprehended.

This factsheet (https://homeofficemedia.blog.gov.uk/2023/10/29/police-use-of-facial-recognition-factsheet/) provides further information on police use of facial recognition, including case studies, the legal framework and safeguards.

In reference to accessing the UK passport database, police forces can currently request facial recognition searches against the passport database on a limited basis in support of the most serious law enforcement investigations, of which the number of searches is low. The Home Office shares data with law enforcement agencies in line with its personal information charter to help in the prevention and detection of crime. This privacy information notice can be found at: https://www.gov.uk/government/organisations/home-office/about/personal-information-charter. Going further than this would require significant policy work and likely further consultation and scrutiny.

The Home Office is working closely with the National Police Chiefs' Council and industry to keep pace with the rapid developments and improvements in this technology and make sure forces can use it in an effective, fair, and proportionate way.

The Home Office has established a Joint Security and Resilience Centre which works with industry to help develop technical solutions to security challenges, including the adoption of AI technologies.

Thank you again for taking the time to write to us.

Yours sincerely,



Rt Hon Chris Philp MP