

Rt. Hon. James Cleverly MP
Secretary of State for Home Department
Home Office
Direct Communications Unit
2 Marsham Street
London
SW1P 4DF
United Kingdom

Cc:
Chris Philp MP
Minister of State (Minister for Crime, Policing and Fire)

18 January 2024

Dear Mr Cleverly,

Re: The danger posed to UK society by Facial Recognition Technology

We are writing to you, as organisations who campaign to defend privacy and freedom of expression in the UK, in light of the UK government's rapid expansion of facial recognition technology (FRT) throughout public spaces in the UK and the threats that this poses to society.¹

We are alarmed by recent statements from the Home Office endorsing an expansion in the use of live facial recognition surveillance technology in both the public and private sectors. It is also deeply concerning that at least 45 UK territorial police forces have been confirmed as using retrospective FRT, despite previous police denials to this effect.² Private companies have also been rolling out this surveillance technology within retail spaces unchecked.³ Now, plans to allow UK police forces access the UK's passport database to enhance their use of facial recognition systems have been revealed.⁴ These developments pose serious threats to fundamental human rights, particularly the right to privacy.

The indiscriminate use of this dystopian biometric technology to identify people in public spaces is a form of mass surveillance often carried out without individual's knowledge or consent. Credible international studies have repeatedly found FRT systems have algorithmic biases and issues with inaccuracies which can misidentify people; particularly women, black people and people from other ethnic minorities.⁵

¹ Thompson, F., "Government looking to expand use of facial recognition technology", The Independent, 31 August 2023.

<https://www.independent.co.uk/news/uk/politics/government-home-office-ministry-of-defence-chris-philp-mod-b2402785.html>

² Wilding, M., and Milmo, C., "Police chiefs claim retrospective facial recognition searches show 'immense potential'. But campaigners say databases contain 'hundreds of thousands' of innocent individuals", Liberty Investigates and the i, 25 September 2023,

<https://libertyinvestigates.org.uk/articles/hundreds-of-thousands-of-innocent-people-on-police-databases-as-forces-expand-use-of-facial-recognition-tech/>

³ Townsend, M., "Major UK retailers urged to quit 'authoritarian' police facial recognition strategy, The Guardian", 28 October 2023, <https://www.theguardian.com/technology/2023/oct/28/major-uk-retailers-urged-to-quit-authoritarian-police-facial-recognition-strategy>

⁴ Klovig Skelton, S., <https://www.computerweekly.com/news/366554287/Policing-minister-wants-to-use-UK-passport-data-in-facial-recognition>, Computer Weekly, 5 October 2023, <https://www.computerweekly.com/news/366554287/Policing-minister-wants-to-use-UK-passport-data-in-facial-recognition>

⁵ Bhuiyan, J., "First man wrongfully arrested because of facial recognition testifies as California weighs new bills", The Guardian, 27 April 2023, <https://www.theguardian.com/us-news/2023/apr/27/california-police-facial-recognition-software>; Collins, T., "Facing gender bias in facial recognition technology", Help Net Security, 27 August 2020, ; <https://www.helpnetsecurity.com/2020/08/27/facial-recognition-bias/>; Kasim, H., "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match", The New York Times, 6 January 2021, <https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html>

This is all happening within a democratic vacuum without specific legislation to restrict its use and provide sufficient safeguards against such risks, which fails to satisfy international human rights standards. Instead, police forces and the private sector continue to wrongly justify their use of FRT through a patchwork of legislation including common law policing powers and data protection legislation, which fails to adequately address the use of the technology.⁶

Furthermore, the expansion of FRT puts the UK out of step with the rest of the democratic world. Recently Members of the European Parliament voted overwhelmingly in favour of placing a full ban on the use of live FRT in public spaces and the EU's AI Act introduces significant restrictions on its use.⁷ Bans have also been introduced in numerous US states⁸, with Vice President Kamala Harris singling out the risk FRT poses to the public ahead of the UK's recent AI Safety Summit.⁹

Recently, over 65 UK parliamentarians called for an "immediate stop" to the use of live facial recognition in public spaces in the UK, citing concerns over a lack of legal basis, poor accuracy and bias, and risks to privacy and freedom of expression.¹⁰ Additionally, over 47,000 people have called on the Met Police to stop their use of live facial recognition surveillance.¹¹

Furthermore, a YouGov survey conducted in June 2023 indicates there is a concerning lack of knowledge regarding whether FRT is currently deployed in constituencies across the UK.¹² In response, Privacy International's campaign 'The End of Privacy in Public' aims to gather more information on this matter by encouraging members of the public to use their constituent power and write to demand their MP find out if facial recognition cameras are being deployed in their local area.¹³ There must be more publicly available information on how FRT is being deployed.

We are calling on you as Home Secretary to put an immediate end to this radical expansion of the use of FRT in order protect the fundamental freedoms of all members of UK society. Such highly intrusive technologies must be subject to strong, legally enforceable safeguards, and where necessary, outright bans. To this end, we politely request a meeting with your Office at your next earliest convenience to discuss these concerns in more detail.

Yours sincerely,

Gus Hosein, Privacy International

Silkie Carlo, Big Brother Watch

Habib Kadiri, StopWatch

Camden CopWatch

Jen Persson, Defend Digital Me

⁶ Privacy International, "UK MPs Asleep at the Wheel as Facial Recognition Technology Spells the End of Privacy in Public", 7 November 2023, <https://privacyinternational.org/long-read/5155/uk-mps-asleep-wheel-facial-recognition-technology-spells-end-privacy-public>

⁷ Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM/2021/206 final. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206>

⁸ Sheard, N., and Schwartz, A., "The Movement to Ban Government Use of Face Recognition", Electronic Frontier Foundation, 5 May 2022, <https://www.eff.org/deeplinks/2022/05/movement-ban-government-use-face-recognition>

⁹ Wintour, P., "Kamala Harris to call for urgent action on AI threat to democracy and privacy", The Guardian, 1 November 2023, <https://www.theguardian.com/technology/2023/nov/01/kamala-harris-to-call-for-urgent-action-on-ai-threat-to-democracy-and-privacy>

¹⁰ Big Brother Watch, "65 parliamentarians call for "immediate stop" to live facial recognition surveillance", 6 October 2023, <https://bigbrotherwatch.org.uk/2023/10/65-parliamentarians-call-for-immediate-stop-to-live-facial-recognition-surveillance/>

¹¹ See: <https://you.38degrees.org.uk/petitions/stop-the-met-police-using-facial-recognition-surveillance>

¹² Privacy International, "UK MPs Asleep at the Wheel as Facial Recognition Technology Spells the End of Privacy in Public", 7 November 2023, <https://privacyinternational.org/long-read/5155/uk-mps-asleep-wheel-facial-recognition-technology-spells-end-privacy-public>

¹³ See: <https://privacyinternational.org/campaigns/end-privacy-public>

Sam Grant, Advocacy Director, Liberty

Chris Jones, Statewatch