HOUSE OF LORDS

John Edwards,
Information Commissioner
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

18th December 2023

Dear John

RE: The Information Commissioner's Office's regulation of facial recognition surveillance

We are group of cross-party parliamentarians, writing in relation to our concerns over the use of facial recognition surveillance in the UK, and the response your Office has had to the expansion of this technology.

The UK stands at a critical moment as the use of AI rapidly increases across different sectors in the UK, posing a range of novel challenges. Many of these AI-powered systems, like facial recognition technology, involve processing of personal data which is highly intrusive and can have very serious consequences for the individuals affected. As the Information Commissioner, your Office plays a crucial role in protecting the rights of people in the UK from a range of privacy incursions across many sectors.

Facial recognition surveillance involves the processing, en masse, of the sensitive biometric data of huge numbers of people – often without their knowledge. It poses a serious risk to the rights of the British public and threatens to transform our public spaces into ones in which people feel under the constant control of corporations and the government. There are also serious impacts that can arise from misidentifications due to poor accuracy and bias. We were alarmed by your recent admission at the Science, Innovation and Technology Committee's evidence session that you are "not aware of specific instances in the UK of people being misidentified and detained as a result";[1] we have documented many such cases where individuals have been misidentified and apprehended by police pending further intrusive checks, often including biometric checks. To date, of 3,337 facial recognition flags by South Wales Police and the Metropolitan Police Service, just 362 have been true matches, while over 65 people have faced wrongful interventions from police officers as a result of a false facial recognition flag.[2] We are concerned by your Office's approach to the expansion of this surveillance technology and discrepancies between this approach and those of other European data regulators.

Two recent decisions made by your Office are particularly concerning, and appear to privilege the interests of private companies over the data rights of the public. Facial recognition companies PimEyes and Facewatch have both been the subject of detailed legal complaints, which have outlined how the companies' systems violate the data rights and privacy of potentially millions of people in the UK. Your Office's decision not to take firm enforcement action over these companies' failures to respect data protection law and safeguard sensitive personal data is deeply worrying.

PimEyes is a publicly available facial recognition search engine, that allows anybody with an internet connection to search for images of any individual across the open internet. The technology can link a face to a name, address, job, political and religious beliefs with ease, through the contextual information surfaced by a PimEyes search. Disturbingly, journalists and campaigners have uncovered a series of examples of the technology being used to harass and track women.[3]

The Baden-Württemberg data protection authority in Germany has initiated legal proceedings against PimEyes, citing concerns over the company's processing of biometric data, the lack of consent from data subjects, an opt-out option that places the onus on the data subject to protect their data from being made accessible to an indefinite number of people, and the possibility of third party abuse.[4] The ICO's decision, then, to not take regulatory action against PimEyes is deeply concerning to us and requires further explanation. We cannot understand why the Commissioner considers it acceptable or appropriate for such an invasive and dangerous tool to continue to be freely available in the UK.

We are similarly concerned by the decision not to take firm enforcement action against Facewatch, a private company that provides live facial recognition to British retailers. Using this technology to scan shoppers is disproportionate and unnecessary, and the consequences of being misidentified or wrongly placed on a watchlist could be serious. Members of the public could be prevented from making essential purchases, including food, be subject to intrusive interventions, or be brought into dangerous confrontations with security staff. All of these things could happen even when an individual has never done anything wrong. It represents a radical transfer of power from ordinary people to companies in our public spaces.

Your Office's own investigation found that Facewatch had violated data protection law on eight counts. That is, tens of thousands of people – perhaps more – had been unlawfully scanned. But worryingly, the ICO declined to take further regulatory action – such as fining Facewatch for those breaches – which would have had a deterrent effect on unscrupulous operators. Your approach seems to put the UK out of step with other jurisdictions: in Spain, the data protection regulator found that a supermarket's use of live facial recognition violated data protection law and fined the retailer €2.5 million.[5]

Although the ICO's Deputy Commissioner for Regulatory Supervision stated that the ICO's decision to allow Facewatch to continue scanning shoppers is not a "green light to the blanket use of this technology", we fear that in reality your light-touch approach will open the floodgates to privatised policing on our high-streets, powered by intrusive surveillance technology. Indeed, since the ICO's Facewatch decision was publicised, we have been alarmed by new and suggested uses of facial recognition surveillance, including bouncers in bars using live facial recognition to identify those accused of "disorder"[6] and the proposed use of the passport photo database for facial recognition searches in relation to low-level crime.[7]

The UK must not become an outlier when it comes to the protection of the public's data rights. As the independent regulator for data protection, you have enormous responsibility in our increasingly data-driven society. We urge you to reconsider your permissive approach to facial recognition surveillance, and to take assertive regulatory action to protect the information rights of everyone in the UK.

HOUSE OF LORDS

Yours sincerely,

pp

Lord Clement-Jones
Lord Alton
Apsana Begum MP
Baroness Bennett
Ian Byrne MP
Alistair Carmichael MP
Baroness Shami Chakrabarti
Wendy Chamberlain MP
Daisy Cooper MP
David Davis MP
Baroness Fox
Marcus Fysh MP
Chris Green MP
Baroness Harris of Richmond
Kim Johnson MP
Baroness Jones of Moulsecoomb
Caroline Lucas MP
Baroness Ludford
John McDonnell MP
Lord Skidelsky
Jamie Stone MP
Lord Strasburger
Lord Strathcarron
Zarah Sultana MP
Lord Vaux of Harrowden
Valerie Vaz MP
Nadia Whittome MP
Mick Whitley MP

[1] Oral evidence: Governance of artificial intelligence, HC 945, House of Commons Science, Innovation and Technology Committee, 25 October 2023, Q649: https://committees.parliament.uk/oralevidence/13728/pdf/

[2] Figures obtained through the South Wales Police and the Metropolitan Police Force's deployment records. False positives matches have led to over 65 wrongful interventions by police officers, including of a 14-year-old boy in school uniform in Romford in 2019. The boy was surrounded by officers, had his fingerprints taken, and was eventually released when police admitted it was a false

match. For more details, see: https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/#facial-recognition-uk

[3] Biometric Britain: The Expansion of Facial Recognition Surveillance – Big Brother Watch, 23rd May 2023, p. 84-4: https://bigbrotherwatch.org.uk/wp-content/uploads/2023/05/Biometric-Britain.pdf

[4] PimEyes: LfDI opens fine proceedings - LfDI Baden-Württemberg, 21st December 2022 (translated from German): https://www.baden-wuerttemberg.datenschutz.de/pimeyes-lfdi-eroeffnet-bussgeldverfahren/

[5] Spanish DPA Fines Supermarket Chain 2,520,000 EUR for Unlawful Use of Facial Recognition System - Privacy & Information Security Law Blog, Hunton Andrews Kurth, 30th July 2021: https://www.huntonprivacyblog.com/2021/07/30/spanish-dpa-fines-supermarket-chain-2520000-eur-for-unlawful-use-of-facial-recognition-system/

[6] Southampton bouncers to wear facial recognition cameras - Timothy Edgley, Southern Daily Echo, 23rd October 2023: https://www.dailyecho.co.uk/news/23876664.southampton-bouncers-wear-facial-recognition-cameras; Red Card Scheme: https://www.gosouthampton.co.uk/redcard/

[7] UK passport images database could be used to catch shoplifters - Aletha Adu and Rajeev Syal, the Guardian, 2nd October 2023: https://www.theguardian.com/uk-news/2023/oct/02/uk-passport-images-database-could-be-used-to-catch-shoplifters