17th May 2024

To: John Edwards, Information Commissioner
Information Commissioner's Office

Dear Commissioner,

We are writing as a coalition of groups who campaign on ending violence against women, racial justice issues and digital and human rights to express our grave concern over reports that Metropolitan Police Service ('MPS') staff members have been accessing an online, private facial recognition search engine. A report from Liberty Investigates in *i News* has revealed that MPS computers accessed the website of PimEyes, a vast facial recognition search engine, 2,337 times in just 90 days.[1] This represents a serious failure of oversight, and is likely to be unlawful under data protection law.

It is reasonable to assume that of these 2,337 hits, some, if not all of these will be MPS staff using PimEyes' technology to identify members of the public. We find the MPS' suggestion to *The i* that staff have not used this website to perform facial recognition searches unconvincing, particularly given the MPS' previous use of Clearview AI,[2] and its continued investment in facial recognition surveillance technology as a policing tool.[3]

The MPS did not publicly disclose that its officers were using PimEyes to identify individuals, and the force's policy documents make no mention of the use of private facial recognition databases. After the force was contacted by Liberty Investigates, it confirmed that it had blocked access to PimEyes from its devices, suggesting that the use of the technology lacked appropriate oversight.

The MPS already has access to its own, internal retrospective facial recognition software, based on custody images, with policies overseeing its use. However, the possibility that the force is circumventing these policies to use a private company's software is deeply alarming and warrants further investigation from your Office.

PimEyes allows users, in this case police officers, to find images of anyone from across the internet. This could include photos from media articles, personal blogs, dating websites, employment profiles, and other publicly available websites. The returned facial images are provided alongside the URLs where they are hosted, giving the user access to highly revealing contextual information about the searched individual. This could include the searched individual's name, details about their place of work, or indications of the area in which they live. PimEyes has been repeatedly linked to the stalking and harassment of women,[4] and has been the subject of a previous legal complaint to your Office, although you declined to take further action.[5]

Although PimEyes states that its service is "not intended for the surveillance of others", there are no safeguards that prevent this.[6] The service enables privacy intrusion and stalking on a scale previously unimaginable. Police officers work with highly vulnerable people, and any misuse of

1 Met Police officers accessed controversial facial recognition site 2,000 times - Cahal Milmo, Mark Wilding, i News, 6 May 2024: https://inews.co.uk/news/met-police-accessed-facial-recognition-site-3041656?ico

2 Leaked: List of police, govt, uni orgs in Clearview AI's facial-recognition trials – Katyanna Quach, the Register, 29 August 2021: https://www.theregister.com/2021/08/29/in_brief_ai/

3 Croydon: Met Police to continue facial recognition despite concerns – BBC, 12 February 2024: https://www.bbc.co.uk/news/uk-england-london-68274090

4 Biometric Britain – Big Brother Watch, May 2023, pg. 85-88: https://bigbrotherwatch.org.uk/wp-content/uploads/2023/05/Biometric-Britain.pdf

5 Big Brother Watch files legal complaint against facial recognition "search engine", PimEyes – Big Brother Watch, 8 November 2022: https://bigbrotherwatch.org.uk/press-releases/pimeyes-press-release/

personal data must be scrutinised. We have serious concerns that police officers could be exploiting this technology to track victims, witnesses and suspects, absent of scrutiny and for their own purposes. The Casey Review found that the MPS is institutionally sexist and there have been a large number of harrowing recent instances where MPS officers have exploited their position to abuse women.[7] We are concerned that officers may have used PimEyes on MPS devices to identify vulnerable women.

We urge you to ensure that the data rights of the British public are safeguarded and to open an investigation into this potential violation of data protection law.

Yours sincerely,

Indy Cross, CEO, Agenda Alliance
Ilyas Nagdee, Racial Justice Director, Amnesty International UK
Madeleine Stone, Senior Advocacy Officer, Big Brother Watch
Andrea Simon, Executive Director, End Violence Against Women Coalition
Baljit Banga, CEO, Hibiscus
Sam Grant, Advocacy Director, Liberty
Sara Chitseko, Programme Manager, Open Rights Group
Gus Hosein, Executive Director, Privacy International
Michael Buraimoh, Race on The Agenda
Estelle du Boulay, Director, Rights of Women
Abigail Ampofo, Interim CEO, Refuge
Jo Todd CBE,Chief Executive,Respect
Chris Jones, Director, Statewatch
Habib Kadiri, Executive Director, Stop Watch
Emma Lingley-Clark, Interim CEO, Suzy Lamplugh Trust
Farah Nazeer, CEO, Women's Aid

6 Stalking fears over PimEyes facial search engine – BBC, 8 November 2022: https://www.bbc.co.uk/news/technology-63544169

7 Baroness Casey Review: An independent review into the standards of behaviour and internal culture of the Metropolitan Police Service – Baroness Casey of Blackstock, March 2023: https://www.met.police.uk/SysSiteAssets/media/downloads/met/about-us/baroness-casey-review/update-march-2023/baroness-casey-review-march-2023a.pdf