Civil Society Groups:

Live Facial Recognition Technology should not be used in public spaces

We, the undersigned civil society organisations, are calling on Parliament and relevant stakeholders to halt and ban the use of live facial recognition technology (LRFT) by the police and private companies entirely, as it poses significant and unmitigable risks to our society. We do not believe that LFRT can ever be safely deployed in public spaces and for mass surveillance purposes.

The rapid advances in the field of artificial intelligence and machine learning, and the deployment of new technologies that seek to analyse, identify, profile, and predict by police, have a seismic impact on the way society is policed.

The use of live facial recognition represents a huge shift in the relationship between the individual and the State. The implications come not solely from privacy and data protection perspectives, but from the larger ethical question for a democratic society permitting and seemingly condoning the rollout of such intrusive technology. LFRT also raises significant problems for our human rights, such as freedom of expression and freedom of assembly.

We are concerned that LFRT may be used in a broad range of public gatherings such as sporting events, music concerts, and protests, threatening protected rights. Further, deployments of this surveillance technology could mirror and exacerbate existing disproportionate policing practices towards minority communities.

Lack of clear legal and ethical framework

On 17 May 2021 the College of Policing launched a public consultation on its new national guidance which seeks to set standards around how police in England and Wales will use LFRT. The public consultation, which closed on 27 June 2021, formed part of the process to develop the new Authorised Professional Practice (APP) on the use of LFRT by the police.

Despite purporting to rectify the issues identified in the Court of Appeal's Judgment in R (Bridges) v Chief Constable of South Wales Police & Ors¹, the APP in fact falls foul of many of the issues that in Bridges led the Court to find the use of LFRT breached privacy rights, data protection laws, and equality laws.

Any claim that the APP implements the decision in Bridges thus falls down not only on its own terms, but by deeply entrenching the problems that the Court found made use of LFRT by South Wales police unlawful in the first place.

¹ R (Bridges) v Chief Constable of South Wales Police & Ors [2020] EWCA Civ 1058

Futher, the APP in our view does not preclude the use of LFRT for intelligence gathering purposes, which the Court found was an impermissibly wide discretion. We are also concerned that the APP allows police forces to use photos obtained from social media or third parties for identification purposes. The broad categories of individuals who may be added to watchlists – going as far as victims of and witnesses to crime – appear difficult to justify.

Lack of Parliamentary scrutiny

In a democratic society, it is imperative that intrusive technologies are subject to effective scrutiny. Police and the Home Office have, so far, completely bypassed Parliament on the matter of LFRT. We are not aware of any intention to subject LFRT plans to parliamentary consideration, despite the intrusiveness of this technology, its highly controversial use over a number of years, and the dangers associated with its use.

Members of Parliament and Peers must demand the opportunity to steer the debate on this significant step change in policing. Whether and how live facial recognition is used by our police forces – a move which fundamentally alters the relationship and balance of power between citizens and the State – should be a matter for Parliament. Should Parliament be afforded this opportunity, it will be evident that legislation attempting to regulate the use of this technology is insufficient – instead, its use in public spaces should be wholly prohibited.

We note that MPs in the House of Commons Science and Technology Committee called for the police use of LFRT to be suspended until further a legislative framework is applied to the technology.²

Being able to choose when and how to disclose one's identity, and to whom, is at the heart of a person's dignity and autonomy.

"Turning the human face into another object for measurement and categorisation by automated processes controlled by powerful companies and governments touches the right to human dignity – even without the threat of being used as a tool for oppression by an authoritarian state."⁵

Signatures:

- 1. Privacy International (PI)
- 2. Big Brother Watch
- 3. Defenddigitalme
- 4. Open Rights Group
- 5. Liberty

² UK House of Commons Science and Technology Committee, The work of the Biometrics Commissioner and the Forensic Science Regulator: Nineteenth Report of Session 2017–19 (HC 1970, 18 July 2019) https://www.publications.parliament.uk/pa/cm201719/cmselect/cmsetech/1970/197003

³ EDPS, Facial Recognition: A solution in search of a problem? (28 October 2019) <u>https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-</u> solution-search-problem_en

- 6. Migrants' Rights Network
- 7. Institute of Race Relations (IRR)
- 8. Migrants Organise
- 9. IT-Pol Denmark
- 10. Right to Remain
- 11. Digitalcourage
- 12. Statewatch
- 13. Joint Council for the Welfare of Immigrants (JCWI)
- 14. Panoptykon Foundation (Poland)
- 15. Homo Digitalis (Greece)
- 16. Citizen D (Slovenia)
- 17. UNJUST
- 18. luridicum Remedium z.s. (Czech Republic)
- 19. Worker Info Exchange
- 20. The Racial Justice Network (RJN)
- 21. Fair Trials
- 22. NoTechForTyrants
- 23. ARTICLE 19: Global Campaign for Free Expression
- 24. Irish Council for Civil Liberties
- 25. People & Planet
- 26. Hermes Center
- 27. info.nodes
- 28. StopWatch UK
- 29. Access Now
- 30. Amnesty International UK
- 31. European Digital Rights (EDRi)