Rt Hon Yvette Cooper MP,
Secretary of State for the Home Department
2 Marsham Street
London
SW1P 4DF

26 July 2024

Sent by email

Dear Home Secretary,

We write to you as the #SafetyNotSurveillance coalition - a group of organisations working at the intersections of human rights, racial justice and technology.

In the King's Speech, it was announced that the Government would "seek to establish the appropriate legislation to place requirements on those working to develop the most powerful artificial intelligence models". A priority within this must be to protect people's rights and to safeguard against the harms of AI systems in policing.

AI is rapidly expanding into all areas of public life, but carries particularly high risks to people's rights, safety and liberty in policing contexts.

Many AI systems have been proven to magnify discrimination and inequality. In particular, so-called 'predictive policing' and biometric surveillance systems are disproportionately used to target marginalised groups including racialised, working class and migrant communities. These systems criminalise people and infringe human rights, including the fundamental right to be presumed innocent.

As signatories, we include individuals with lived experience of the harms of Artificial Intelligence (AI) systems in policing. As such, we, the undersigned, call on the government to protect people's rights and prevent uses of AI which exacerbate structural power imbalances. AI systems in policing should be regulated by:

1. PROHIBITING 'PREDICTIVE POLICING' & BIOMETRIC SURVEILLANCE SYSTEMS

a) 'Predictive policing' systems which use AI, data and algorithms to identify, profile and target individuals, groups and locations, attempting to 'predict' certain criminal acts, or the 'risk' of certain criminalised acts should never be used, and should be prohibited.

These data-based 'predictions', profiles and 'risk' assessments influence, inform, or otherwise lead to policing and criminal justice outcomes, including surveillance, questioning, stop and search, fines, and even arrest. Automated 'predictions', profiles and 'risk' assessments can also lead to civil punishments, including the denial of welfare, housing, or other essential services, as well as harmful outcomes through immigration enforcement and increased surveillance from state agencies.

‘Predictive policing’ systems exacerbate structural imbalances of power. They are used to monitor and control people in public spaces, with the worst harms often falling on racialised and migrant communities, who are labelled as ‘threats’ to the state.

These systems have been proven to reproduce and reinforce discrimination and inequality, along the lines of, but not limited to: racial and ethnic origin, nationality, socio-economic status, disability, gender and migration status. Data reflecting existing inequalities and prejudices is used to recreate and reinforce these inequalities. These systems criminalise people and engage and infringe human rights, including the right to a fair trial and the presumption of innocence, the right to private and family life, and data protection rights.

These systems must therefore be prohibited.

2. ENSURING SAFEGUARDS, TRANSPARENCY & ACCOUNTABILITY FOR ALL OTHER USES

a) All data-based, automated and AI systems in policing which are *not* prohibited should be regulated to protect people’s rights and safeguard against harms.

All systems should be independently classified as 1. Prohibited uses, and 2. Non-prohibited uses, subject to strict transparency and accountability obligations.

b) A legislative framework creating transparency, accountability, accessibility and redress should underpin the use of all data-based, automated and AI systems in policing.

All systems which influence, inform or impact policing decisions should be subject to strict transparency and accountability obligations including:

1. **Consistent public transparency.** Details of all data-based, automated and AI systems, including technical specifications, developer details, the data they use, how they are used and what decisions they influence and inform should be held on a publically available register.
2. **Restricted data sharing.** The sharing of personal data between public authorities, private actors and law enforcement should be restricted to ensure the right to privacy and other fundamental rights are protected. Transparency must be sufficient to ensure the protection of fundamental rights.
3. **Engagement with affected communities.** Stakeholder engagement with those affected by the AI should be a mandatory prerequisite to the introduction of all data-based, automated and AI systems.
4. **Independent oversight.** All data-based, automated and AI systems in policing should be independently assessed for compatibility with existing legislation, including international human rights standards.

5. **Mandatory accessibility requirements.** It should be mandatory that all data-based, automated and AI providers and users comply with accessibility requirements.
6. **No profiling or labelling.** No decisions that amount to profiling or labelling of individuals or communities should take place through AI or other systems.
7. **Meaningful human involvement in decisions.** No decision about someone's legal rights should be made by an automated or AI-system alone, as these kinds of decisions pose particularly high risk to people's rights and safety.
8. **Meaningful human review.** Everyone should have the right to prompt and meaningful human review of any automated or AI decision made about them and decisions should be provided in a clear and accessible format to non-experts.
9. **Written decisions by a human.** People should have a right to a written decision by a human which explains the data-based, automated or AI system outcome. Decisions should be provided in a clear and accessible format.
10. **Clear route to challenge and robust redress.** There must be a clear route to challenge any AI or automated decision and robust redress for individuals and groups affected by AI systems in policing. These mechanisms must include support for whistleblowers.

Signed:

Open Rights Group
CAGE
Liberty
No Tech for Tyrants
Northern Police Monitoring Project
StopWatch
Bristol Copwatch
Racial Justice Network
Big Brother Watch
Runnymede Trust
Healing Justice LDN
StateWatch
UNJUST CIC
Prevent Watch
Community Policy Forum
The 4Front Project
Netpol (Network for Police Monitoring)