2nd April 2025

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

Rt Hon Peter Kyle MP
Secretary of State for Science, Innovation and Technology
Department for Science, Innovation and Technology
100 Parliament Street
London
SW1A 2BQ

Law enforcement use of Automated Decision-Making

Dear Secretaries of State,

We are writing to you as human rights, racial justice and civil liberties groups and academics with common concern about the weakening of safeguards for solely automated decisions in the law-enforcement context under clause 80 of the Data (Use and Access) ('DUA') Bill. If passed as written, the DUA Bill will undermine faith in law enforcement and dilute crucial data protection safeguards. We urge you to bring our concerns with clause 80 to the attention of your colleagues currently considering the Bill.

Currently, sections 49 and 50 of the Data Protection Act 2018 prohibit solely automated decisions from being made in the law enforcement context unless the decision is required or authorised by law. Clause 80 of the DUA Bill would reverse this safeguard, permitting solely automated decision-making ("ADM") in all scenarios unless the data processing involves special category data. In practice, this means that automated decisions about people could be made in the law enforcement context on the basis of their socioeconomic status, regional or postcode data, inferred emotions, or even regional accents. This greatly expands the possibilities for bias, discrimination, and lack of transparency.

Additionally, there are many contexts in which non-special category personal data acts as a proxy for protected characteristics when used in ADM. For example, data about a person's name or occupation can act as a proxy for their sex, or postcodes may act as a proxy for race[1] when processed in an algorithm. Indeed, in the Impact Assessment of the DUA Bill, the Government acknowledged that, "those with protected characteristics

1 ICO, 'How do we ensure fairness in AI?' Accessed 11 March 2025, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-fairness-in-ai/what-about-fairness-bias-and-discrimination/

such as race, gender, and age are more likely to face discrimination from ADM due to historical biases in datasets."[2] In allowing the police to make solely automated-decisions in these contexts, the DUA Bill therefore puts marginalised groups at risk of opaque, unfair and harmful automated decisions.

Under the DUA Bill, even the prohibitions on ADM where special category data is processed are not absolute. This means that where "authorised by law," police officers will be able to make automated decisions that have significant adverse effects on individuals by processing data which reveal their racial or ethnic origin, sexual orientation and health status, as well as genetic or biometric data. We expect that police in England and Wales may rely on a very broad interpretation of ADM "authorised by law" based on common law and a patchwork of laws pre-dating the technological revolution, to exploit this loophole – for example, as seven police forces have done in the context of live facial recognition software, which processes biometric data. As such, police will be able to conduct ADM without limitation and to conduct ADM involving sensitive data with very few limitations.

We are also alarmed about the diluted safeguards for solely automated decisions in the law enforcement context proposed under the DUA Bill. Currently, individuals who are subjected to ADM must be informed about the decision and have the right to obtain human intervention to contest it. Under the proposed clause 80, these safeguards are completely disregarded if the controller deems that solely ADM may, inter alia, protect public security or safeguard national security. Given the already minimal transparency and difficulty in obtaining redress from ADM, affected individuals in the law enforcement context would have no or highly limited routes to redress.

Concerns about ADM are especially pronounced in the criminal justice context. Collectively, we have scrutinised big data uses by police in the UK – such as the AI recidivism tool HART, which predicted reoffending risks partly based on an individual's postcode in order to inform charging decisions; PredPol, which was used to allocate policing resources based on postcodes; facial recognition, which has well-documented demographic bias issues disproportionately impacting people of colour; and the Gangs Matrix, which harvests "intelligence" disproportionately affecting innocent young black men. Under the proposed changes, similar discriminatory tools could be used on a larger and more intrusive scale, with fewer safeguards and potentially even in secrecy. This means affected individuals or groups will have no or highly limited routes to redress and could either be affected by ADM with adverse legal effects in total secrecy, or if they do discover ADM has impacted them, will have to

2 Data (Use and Access Bill), Impact Assessment from DSIT, 23 October 2024: https://bills.parliament.uk/publications/56548/documents/5221 para. 531, p.163

attempt to prove discriminatory impacts or a failure to uphold the Public Sector Equality Duty in order to challenge decisions.

The erosion of safeguards around decisions that will adversely impact individuals' lives under the DUA Bill risks making the British criminal justice system less accountable and transparent, and more likely to discriminate against protected groups unfairly.

Given DUA's progress through the House of Commons, we hope that you will swiftly urge your colleagues to address the flaws that remain in the Bill.

Yours Sincerely,

Rebecca Vincent, Interim Director, Big Brother Watch

Indy Cross, Chief Executive, Agenda Alliance

Jess Mullen, Chief Executive, Alliance for Youth Justice

Ilyas Nagdee, Racial Justice Programme Director, Amnesty International

Rhona Friedman, Director, Commons Law CIC

Paige Collins, Senior Speech and Privacy Activist, Electronic Frontier Foundation

Deborah Coles, Executive Director, INQUEST

Liz Fekete, Director, Institute of Race Relations

Akiko Hart, Director, Liberty

Anna Peiris, Executive Director, MedAct

Northern Police Monitoring Group

Sara Chitesko, Programme Manager (Pre-crime), Open Rights Group

Lubia Begum-Rob, Director, Prisoners' Advice Service

Caroline Wilson Palow, Legal Director and General Counsel, Privacy International

Shameem Ahmad, Chief Executive Officer, Public Law Project

Aliya Mohammed, Chief Executive Officer, Race Equality First

Niamh Eastwood, Executive Director, Release

Chris Jones, Director, Statewatch

Habib Kadiri, Executive Director, Stop Watch

Sian Williams, Chief Executive Officer, Switch Back

Yvonne MacNamara, Chief Executive Officer, The Traveller Movement

Katrina Ffrench, Executive Director, UNJUST

Paula Harriot, Chief Executive Officer, Unlock

Sara Dowling, Chief Executive Officer, Why Me?

Natasha Finlayson, Chief Executive, Working Chance

Khatuna Tsintsadze, Co-director, Zahid Mubarek Trust

Professor Brent Mittelstadt, Professor of Data Ethics and Policy, Director of Research, Oxford Internet Institute

Professor Chris Russell, Dieter Schwarz Associate Professor, AI, Government and Policy, Oxford Internet Institute

Professor Sandra Wachter, Professor of Technology and Regulation, Oxford Internet Institute

Professor Netta Weinstein, Research Associate, Oxford Internet Institute

Dr Toyin Agbetu, Lecturer in Social Anthropology, University College London