BIG BROTHER WATCH

Written Evidence to the Science and Technology Committee's Inquiry: Governance of artificial intelligence (AI)

November 2022

About Big Brother Watch

Big Brother Watch is a civil liberties and privacy campaigning organisation, fighting for a free future. We're determined to reclaim our privacy and defend freedoms at this time of enormous technological change.

We're a fiercely independent, non-partisan and non-profit group who work to roll back the surveillance state and protect rights in parliament, the media or the courts if we have to. We publish unique investigations and pursue powerful public campaigns. We work relentlessly to inform, amplify and empower the public voice so we can collectively reclaim our privacy, defend our civil liberties and protect freedoms for the future.

Contact

Silkie Carlo
Director
Direct line: 020 8075 8478
Email: silkie.carlo@bigbrotherwatch.org.uk

Madeleine Stone
Legal & Policy Officer
Direct line: 07864733785
Email: madeleine.stone@bigbrotherwatch.org.uk

We welcome the opportunity to provide evidence to the Science and Technology Committee's inquiry into the governance of artificial intelligence (AI).

Big Brother Watch works to defend civil liberties in the context of new and emerging technologies. We research and publish ground-breaking reports on the use of AI and automation across society, including on the use of automation in the welfare state,[1] police use of facial recognition[2] and 'smart' surveillance.[3] As such, our response will focus on AI as it impacts individuals and their data and human rights.

To reflect the ways in which this terminology is commonly used, we have followed a wide interpretation of AI, including machine learning, which concerns the imitation of human intelligence in an artificial manner, by computer programs, systems or algorithms. This technology can be used to analyse data and make decisions.

1. How effective is current governance of AI in the UK?

What are the current strengths and weaknesses of current arrangements, including for research?

The UK currently has weak governance relating to AI, and the critical legal frameworks that provide essential protections are under threat.

There is currently no legislation that specifically oversees the public or private sector's use of AI. From a human rights perspective, the legal frameworks most relevant to the operation of AI systems include the Human Rights Act 1998, Data Protection Act 2018 and the Equality Act 2010 - the first two of which this Government has stated an intention to repeal. Currently, any AI systems which impact individuals must comply with these laws. However, throughout our research and campaigning, we have often found systems in both the public and private sector which do not adequately respect the rights of individuals as set out by these pieces of legislation – for example, police forces' use of live facial recognition surveillance. More must be done to ensure that public and private organisations using AI are aware of these legal obligations, and regulators, such as the Information Commissioner's Office, should be well-resourced to ensure these obligations are enforced. Furthermore, those legal frameworks must be protected.

1 Poverty Panopticon – Big Brother Watch, July 2021: https://bigbrotherwatch.org.uk/wp-content/uploads/2021/07/Poverty-Panopticon.pdf
2 Face Off: The lawless growth of facial recognition in UK policing – Big Brother Watch, May 2018: https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf
3 The Streets Are Watching – Big Brother Watch, October 2022: https://bigbrotherwatch.org.uk/wp-content/uploads/2022/10/The-Streets-Are-Watching-You.pdf

In some cases, proposed uses of AI give rise to a complex set of concerns for human rights, equality and civil liberties, and/or reflect wider systemic changes, where applying a patchwork of existing laws may not adequately address potential impacts. In these cases, specific scrutiny and action from parliament is merited. Some of these technological developments have the potential to significantly change the society we live in, the opportunities people have, and the risks people face. For example, widespread and systemic uses of AI in the welfare system, health system, policing and criminal justice system, state surveillance and the military all give rise to serious, diverse and complex issues and require strong governance in addition to the protections required by the foundational frameworks of the Data Protection Act, Equality Act and Human Rights Act. To date, whilst parliamentary committees have provided close scrutiny in some areas and made important recommendations – such as the Science and Technology Committee's 2019 recommendation that "the Government [should] issue a moratorium on the current use of facial recognition technology and no further trials should take place until a legislative framework has been introduced"[4] - recommendations have not been taken forward. On the contrary, facial recognition and other AI technologies have been procured with public money and operationally deployed at pace in the "regulatory lacuna" this Committee warned of in 2019, resulting in legal challenges.[5]

In some cases where AI uses give rise to a complex set of novel concerns, the technological development may be relatively subtle and as such evade consideration of whether additional governance is necessary. For example, the UK's exceptionally broad surveillance camera coverage is undergoing serious change as AI software updates are being used with existing hardware. However, there is no default transparency mechanism to raise people's attention to this and no specific legal framework to apply. The Home Office's combining of the roles of Surveillance Camera Commissioner and Biometrics Commissioner is an acknowledgement of the fact that surveillance cameras are no longer only passively recording the public but actively assessing us, processing our body data and in some cases identifying us – but there is no specific governance in place to appropriately deal with AI surveillance. The Biometric and Surveillance Camera Commissioner's (BSCC) role, insofar as surveillance cameras are concerned, is to promote compliance with the Surveillance Camera Code of Practice. The Code is a set of guiding principles for public authorities to have regard to in the course of their use of surveillance cameras – it is not legally binding. Furthermore, whilst the purpose of the Code rightly states that:

4 The work fo the Biometrics Commissioner and the Forensic Science Regulator – Science and Technology Committee, House of Commons, 18 July 2019, Recommendation 8: https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/1970/197002.htm

5 For example, see *Bridges v South Wales Police*

> "Modern and ever-advancing surveillance camera technology provides increasing potential for the gathering and use of images and associated information. These advances vastly increase the ability and capacity to capture, store, share and analyse images, information and data. Advancements in sensor technology and artificial intelligence are developing at an ever increasing pace, as is the ability to integrate these technologies with surveillance cameras"[6]

the actual Code Principles do not contain the words "artificial intelligence" at all. Nor do the words "artificial intelligence" appear in the Commissioner's most recent annual report, despite his acknowledgement that thousands of cameras in the UK are now using AI for purposes varying from behavioural analysis, anomaly detection and identification. This does not reflect any shortcoming of the Commissioner, but rather of the remit and tools he is equipped with, which are insufficient for the new landscape of AI surveillance. Whilst the foundational rights frameworks outlined apply, and the non-binding Code of Practice provides public authorities with general guidance, there is a serious transparency and governance vacuum that means both the prevalence and impact of AI surveillance is hidden from democratic scrutiny.

RECOMMENDATION 1: In light of the ongoing rapid expansion of AI surveillance, the Government should commission an independent national review of the scale, capabilities, ethics and rights impact of modern surveillance cameras in the UK.

The Government has outlined its intention to repeal and replace both the Data Protection Act and Human Rights Act. We, along with many civil society groups, are extremely concerned about these proposals and the impact they will have on indviduals' rights in the context of AI and automated decision making. Initial analysis of both the Data Protection and Digital Information Bill and the Bill of Rights, which are expected to return to Parliament shortly, suggests that these Bills would seriously weaken data protection and significantly limit individuals' ability to challenge violations of their rights.

RECOMMENDATION 2: The Human Rights Act 1998 and Data Protection Act 2018 provide essential protections for fundamental rights in the context of emerging technologies and must be protected.

6 Surveillance Camera Code of Practice, November 2021: https://www.gov.uk/government/publications/update-to-surveillance-camera-code/amended-surveillance-camera-code-of-practice-accessible-version

Governance is particularly important with regards to AI and research given the breadth of potential impacts, and these impacts can be acute where uses of mass personal data are involved. In a health scenario, the impact can be particularly severe and result in distrust of vital institutions. In 2015, the (then) startup DeepMind received 1.6 million identifiable patient records from the NHS unlawfully, without patients' knowledge or consent. Whilst ostensibly the data sharing was for AI research, the outcome appeared to in fact be a healthcare app 'Streams', modelled using analysis of the structure of the hundreds of thousands of NHS records it had received. The company was acquired by Google for approximately £400m. Many affected patients who did not want Google to process or hold their personal medical data then lost trust in their hospital, and a legal challenge was subsequently initiated. These risks emphasise the need for far greater transparency mechanisms such as a public register of significant AI uses, including the personal data used; and the vital importance of preserving our data protection and privacy standards in the Data Protection Act 2018 and Human Rights Act 1998.

2. What measures could make the use of AI more transparent and explainable to the public?

There is a serious lack of transparency around public authorities' and private companies' uses of algorithms and new technologies in decision-making, and even less explainability. As such, it is difficult for the public and civil society to know where and how AI is being used. When AI is informing significant decision-making, it can be difficult to know about, let alone investigate or challenge.

Individuals should know where and when AI is being used in decision-making; be informed when AI impacts a significant decision made about them; have access to information and control about how much of their personal data is used in the course of AI processing; and have a right to request a human review of any significant decision made where this is no meaningful human input.

In November 2021, the Central Digital and Data Office launched the Algorithmic Transparency Standard, which is currently being piloted with several public bodies.[7] The Algorithmic Transparency Standard is for public bodies to publish information about algorithmic tools, including AI, being used in a "complete, open, understandable, easily-accessible, and free format." This is a welcome development, but is currently an optional tool. The Government should take steps to make this a mandatory tool.

7 Algorithmic Transparency Standard – GOV.UK, 29th November 2021, accessed 17th November 2022: https://www.gov.uk/government/collections/algorithmic-transparency-standard

Case study: automation and AI in welfare systems

In July 2021, Big Brother Watch published a report into the use of AI and automation in the welfare state. Our report, *Poverty Panopticon: the hidden algorithms shaping Britain's welfare state,* found that councils across the UK are conducting mass profiling of welfare and social care recipients and "citizen scoring" applicants to predict fraud, rent non-payments and major life events.

Investigating the impact of AI and algorithmic decision-making in the welfare system was challenging, owing to low transparency in the welfare system, proprietary systems and the influence of private technology firms. This means that risks to people's data rights may still be going undocumented and unchallenged. Despite uncovering numerous automated systems, we are still unaware of a single case where an individual has been informed that they have been subjected to a purely automated decision, as per their legal rights under Article 22 of the GDPR.

Thousands of Freedom of Information (FOI) requests formed the basis of the report. At times, it took repeated requests and appeals to access often incomplete information. The influence of private suppliers in the transparency process was also evident. Different local authorities responded with identical responses on the same issues, suggesting coordination from a third party supplier. The fusion of the public sector with private companies on AI systems that impact the public makes it increasingly difficult to obtain information, as companies cite commercial confidentiality in order to avoid disclosure.

Some public authorities have refused to disclose important documents, such as Data Protection Impact Assessments (DPIAs). As part of the Housing Benefit Award Accuracy Initiative (HBAA), the Department for Work and Pensions has created a predictive model for fraud and error which identifies claimants who are most likely to have had a change in their circumstances affecting their benefit payments, leading to burdensome full case reviews. The department refused to disclose its DPIA when asked, claiming it contained details of the model and was therefore exempt from disclosure. This conflicts with the Information Commissioner's advice that DPIAs should usually be published, with redactions if necessary.

Given the serious discrimination and privacy risks, Equality Impact Assessments and Data Protection Impact Assessments should be required for any public sector algorithm that informs decision making about individuals or households, and made publicly available.

RECOMMENDATION 3: We agree with recommendation 19 (paragraph 112) made by the House of Lords' Justice and Home Affairs Committee in their March 2022 inquiry report, Technology Rules? The advent of new technologies in the justice system:

> "Full participation in the Algorithmic Transparency Standard collection should become mandatory, and its scope extended to become inclusive of all advanced algorithms used in the application of the law that have direct or indirect

implications for individuals. This would have the effect of turning the collection into a register."[8]

3. How should decisions involving AI be reviewed and scrutinised in both public and private sectors?

Are current options for challenging the use of AI adequate and, if not, how can they be improved?

There should be a general presumption against subjecting individuals to significant decisions made solely by algorithms, as per GDPR, and where automated decisions are made, strict safeguards are required – including the availability of a human review.

Article 22(1) of the GDPR provides that:

> "Automated individual decision-making, including profiling"
>
> 1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her".

Article 22(2)(b) of the GDPR allows Member States to create certain exemptions from this right, as long as "the data subject's rights, freedoms and legitimate interests" are safeguarded. The UK's Data Protection Act 2018 requires someone to be notified about 'solely' automated decisions that have legal or similar significant effects on them, and to request a human review.[9] However, what constitutes a 'solely' automated decision is a point of contention and Big Brother Watch has long lobbied for greater clarity and guidance and enforcement around the definition to ensure it is a meaningful, functioning safeguard.[10] We are not aware of a single case where an individual has been notified that they have been subjected to a purely automated decision by a public authority.

Recital 71 of the GDPR is relevant, stating that automated decisions are those "without any human intervention" - but it does not clarify that such interventions must be meaningful. Therefore, public authorities may believe that even the most minimal

8 Technology Rules? The advent of new technologies in the justice system - ustice and Home Affairs Committee, 1st Report of Session 2021-22 - 30 March 2022 - HL Paper 180: https://publications.parliament.uk/pa/ld5802/ldselect/ldjusthom/180/18002.htm

9 ICO Guidance on GDPR – Automated Decision Making and Profiling, retrieved 23rd June 2021 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-does-the-uk-gdpr-say-about-automated-decision-making-and-profiling/#id2

10 For example, see Big Brother Watch's Briefing on the Data Protection Bill for Report Stage in the House of Commons, May 2018: https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Big-Brother-Watch%E2%80%99s-Briefing-on-the-Data-Protection-Bill-for-Report-Stage-in-the-House-of-Commons.pdf

human input or token gesture lacking any influence over the decision could authorise an automated decision that has a significant legal effect. We believe that such administrative input currently circumvents the vital safeguards regulating solely automated decisions.

Our concern was echoed by the Deputy Counsel to the Joint Committee on Human Rights during the passage of the Data Protection Act through parliament, who warned that "there may be decisions taken with minimal human input that remain de facto determined by an automated process."[11]

Guidance from the Information Commissioner requires a "meaningful human intervention" in an algorithmic decision to stop it being solely automated – but this is only guidance and is not regularly enforced. According to the ICO, the human has to be able to fully review the information and alter the decision.

An ICO example is: "An employee is issued with a warning about late attendance at work. The warning was issued because the employer's automated clocking-in system flagged the fact that the employee had been late on a defined number of occasions. However, although the warning was issued on the basis of the data collected by the automated system, the decision to issue it was taken by the employer's HR manager following a review of that data."[12]

A legally significant or similar effect is either an impact that directly affects someone's legal rights, such as entitlement to something in law, while a similarly significant effect will have an equivalent impact on their behaviour, choices or personal circumstances. Examples include automatic decisions on eligibility for loans, e-recruitment with no human intervention or the welfare payments someone is entitled to.

In our aforementioned research on AI and algorithms in the welfare system, we found human intervention in algorithmic processes to be limited. Benefits officers who request fraud risk scores, for instance, are permitted in limited circumstances to upgrade a risk score, for example from low to medium, but are forbidden by the DWP from lowering a risk score.[13] Whether this could be considered meaningful human intervention is highly questionable. The benefits officer cannot use their judgement or discretion to lower the score of someone they think poses minimal risk – instead, they can rubber stamp the computer's decision or raise it higher in limited circumstances. Furthermore, they cannot fully review the information that has been processed in

11 Note from Deputy Counsel, 'The Human Rights Implications of the Data Protection Bill', 6 December 2017 (https://www.parliament.uk/documents/joint-committees/human-rights/correspondence/2017-19/Note_Deputy_Counsel_DPBill.pdf)

12 ICO Guidance on GDPR – Automated Decision Making and Profiling, retrieved 23rd June 20212

13 Housing Benefit and Council Tax Benefit Circular - HB/CTB S11/2011

producing the decision, due to aforementioned commercial opacity. This lack of freedom to fully review a decision undermines the claim that the allocation of a risk score is not a solely automated decision.

Legally significant or similar effects likewise need defining more clearly in guidance and enforcement. Denial of a loan, assigning school grades or rejection from a job are considered legally significant but whether an automated risk score triggering a benefits investigation qualifies as 'significant' is unclear. Without clear guidelines, the extent to which decisions involving AI are even known about, let alone reviewed and scrutinised, remains unknown.

A further issue is that many more decisions are more genuinely made in a way that involves AI without the decision being solely an AI or algorithmic decision. For example, police forces' experimental use of live facial recognition and AI recidivism tools are ostensibly used to inform officers' decisions. In such cases, it is important that human decision-making is centred, documented and explained and that the machine is 'in the loop' rather than the human being 'in the loop' of machine-driven decision making, as further safeguards are required in the latter case. Furthermore, there are a number of psychological effects such as confirmation bias, deference resulting from perceptions of superiority, and indeed defiance resulting from perceptions of inferiority, that can influence human-machine dynamics in decision-making that must be assessed.

RECOMMENDATION 4: In the case of human decisions supported by AI, frequent audits should be undertaken to assess and compare AI decision recommendations to the human decisions made, and assess any patterns of discrepancies.

For example, if there were no discrepancies at all between an AI tool's assessment of risk and a human assessment of risk, further inquiries may be required to ascertain whether the decisions being made are in practice purely automated.

Even if an individual were notified that they had been subjected to a purely automated decision, or a decision significantly impacted by AI, they may not be informed of how much of their personal data or what types of their data had been processed in the course of making that decision. For example, Big Brother Watch's investigation of the 'Harm Assessment Risk Tool' (HART), an recidivism risk-scoring tool previously used by Durham Constabulary until our expose, revealed that the AI tool controversially used two postcode variables to determine whether a suspect was likely to re-offend. One of those postcode variables was an Experian Mosaic socio-geodemographic segmentation variable, laden with racist, classist and ageist stereotypes. Experian has

now redesigned the Mosaic segmentation tool, and Durham Constabulary has paused its use of the HART tool. However, no regulatory action or parliamentary action has improved safeguards in this regard. Similarly, we found that the Risk Based Verification (RBV) systems used by dozens of local authorities to assess the fraud risk of housing benefit applicants processed age and gender in the course of risk-scoring, without properly assessing the equalities risk.[14]

Finally, the outcomes as well as the processes of AI decision-making should be open to review and scrutiny. We have observed a lack of monitoring by public authorities with regards to fair outcomes and frequent uses of data variables that reflect, or are proxies for, protected characteristics. In the public bodies we have researched, this appears to be rooted in the erroneous idea that if all data subjects are analysed by the same machine, the processing is fair. Freedom of Information documents we obtained from Haringey Council, one of the few councils to monitor demographic outputs for Risk Based Verification scoring for benefits, found sex and ethnicity disparities in who was flagged as highest risk. RBV is no longer used by Haringey Council following a "standard internal review" and we do not know if this data was probed further. The fact that Haringey Council's monitoring was the exception rather than the norm is a serious problem that must be addressed by better training and guidance.

A mandatory public register of such algorithms, that requires transparency of data fields ingested by such systems, as well as Equality Impact Assessments, would significantly improve opportunities for scrutiny of AI-related decision-making.

4. How should the use of AI be regulated, and which body or bodies should provide regulatory oversight?

In its July 2022 policy paper 'Establishing a pro-innovation approach to regulating AI', the Department for Digital, Culture, Media and Sport (DCMS) outlines that it will "delegate responsibility for designing and implementing proportionate regulatory responses to regulators,"[15] meaning AI governance will be sector specific. Sector specific regulations may help provide specified guidance and oversight, but over-arching structures and oversight is also needed.

RECOMMENDATION 5: A strengthened and mandatory Algorithmic Transparency Standard, as well as well-resourced regulators such as the Information Commissioner, Equality and Human Rights Commission, and oversight provided by the Biometrics and

14 Poverty Panopticon: the hidden algorithms shaping Britain's welfare state – Big Brother Watch, July 2021, e.g. p.29: https://bigbrotherwatch.org.uk/wp-content/uploads/2021/07/Poverty-Panopticon.pdf

15 Establishing a pro-innovation approach to regulating AI An overview of the UK's emerging approach - Department for Digital, Culture, Media and Sport, 18th July 2022, p. 2:https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1092630/_CP_728__-_Establishing_a_pro-innovation_approach_to_regulating_AI.pdf

Surveillance Camera Commissioner, are vital to ensure that the regulatory mechanisms that exist can be fully operationalised.

Furthermore, the Algorithmic Transparency Standard could require more transparency of the actual algorithmic functioning including via algorithmic audits examining risks prior to their operational use.

The DCMS paper also proposed to introduce a set of cross-sectoral principles, designed to be "interpreted and implemented in practice by our existing regulators."[16] This principle-based regulation is part of the government's 'pro-innovation' approach to AI, which seeks to diminish legal obligations and instead asks regulators to "consider lighter touch options, such as guidance or voluntary measures."[17] Additionally, the government intends to "ask that regulators focus on high risk concerns rather than hypothetical or low risks associated with AI."[18] The principles proposed by DCMS are vague and flexible, with the suggestion that concepts like 'fairness' can be defined differently by each regulator. This approach is likely to lead to inconsistency and a lack of clarity.

It is concerning that the government's AI governance approach appears to conflate a reduction in safeguards with innovation and growth. On the contrary, regulation gives public bodies and private companies clear guidelines within which to operate, enabling developers to feel confident that they are operating in accordance with the law when developing new technologies. Robust regulation also fosters public trust. Individuals should feel confident that their data is not being misused, and that decisions made about them are transparent, fair and open to challenge. The inverse will lead to backlash and an unwillingness to adopt or trust new AI-powered technologies.

The Oxford Internet Institute's Governance of Emerging Technologies program has also criticised this principles-led approach to governance as overly vague and flexible:

> "Failing to define the principles more concretely will allow companies to satisfy regulation according to weak definitions, or to effectively 'shop' between different fairness definitions or metrics for the one that presents their system or

16 Establishing a pro-innovation approach to regulating AI An overview of the UK's emerging approach - Department for Digital, Culture, Media and Sport, 18th July 2022, p. 12: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1092630/_CP_728__-_Establishing_a_pro-innovation_approach_to_regulating_AI.pdf

17 Establishing a pro-innovation approach to regulating AI An overview of the UK's emerging approach - Department for Digital, Culture, Media and Sport, 18th July 2022, p. 2: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1092630/_CP_728__-_Establishing_a_pro-innovation_approach_to_regulating_AI.pdf

18 Establishing a pro-innovation approach to regulating AI An overview of the UK's emerging approach - Department of Digital, Culture, Media and Sport, 18th July 2022, p. 2: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1092630/_CP_728__-_Establishing_a_pro-innovation_approach_to_regulating_AI.pdf

business practice in the best possible light. This will not require them to make meaningful changes to make their products safer, and therefore defeats the point of having principles in the first place."[19]

5. To what extent is the legal framework for the use of AI, especially in making decisions, fit for purpose?

Is more legislation or better guidance required?

Our response to question 3 is also relevant to this question.

As we warned when the legislation was going through Parliament,[20] the Data Protection Act fails to provide sufficient clarity as to what constitutes a solely automated decision making and as such provides insufficient protection where human input is so minimal as to be meaningless, such as a merely administrative authorisation of an automated decision by a human controller. Whilst the Government has stated that such administrative human intervention would not be sufficient,[21] there is no wording in the Act at all that defines what constitutes an automated decision.

RECOMMENDATION 6: Further clarity is required on both what constitutes a "solely automated" decision, and what constitutes a significant decision that meets the threshold to trigger the legal safeguards provided by Article 22 of the GDPR.

In order to safeguard rights, we recommend new, detailed guidance on solely automated decision-making, which clarifies minimum standards of human involvement in significant decisions made by AI and algorithms.

6. What lessons, if any, can the UK learn from other countries on AI governance?

Countries around the world are starting to legislate for the impacts of AI on the public. The European Union is currently in the process of passing the AI Act, and in the US, the White House has published a blueprint for an AI Bill of Rights.[22] The framing of other countries has largely been around protecting citizens from the harms that AI can perpetrate, such as discrimination, bias and violations of privacy. The EU AI Act in particular is likely to influence Western standards for the regulation of AI, and while it is not a perfect response to the risks that AI can pose to individuals, its attempt to

19 Written Evidence on 'Establishing a pro-innovation approach to regulating AI' - Prof. Brent Mittelstadt et al, Oxford Internet Institute, 17th November 2022: https://www.oii.ox.ac.uk/wp-content/uploads/2022/11/GET-Call-for-evidence-response.pdf
20 Ibid.
21 HL Deb (13th November 2017), vol. 785, col. 1869 : https://hansard.parliament. uk/lords/2017-11-13/debates/F52C75EF-3CCC-4AC4-9515-A794F269FDAE/DataProtectionBill
22 Blueprint for an AI Bill of Rights – Office of Science and Technology Policy, The White House, 4th October 2022: https://www.whitehouse.gov/ostp/ai-bill-of-rights/

assess AI systems by the harms they can cause is a positive approach which centres the impact on individuals. The Act acknowledges the importance of prohibiting certain high-risk AI practices, such as social scoring and open-ended remote biometric identification.

RECOMMENDATION 7: The UK should legislate to prohibit the most serious algorithmic and AI harms that are already affecting the public – such as live facial recognition surveillance.

The UK's approach, which appears to erroneously equate 'pro-innovation' with limited regulation and legal safeguards, is likely to place the UK at odds with other jurisdictions. Rather than being 'world-leading', the UK's approach to AI diverges from our closest trading partners and could result in a reputation for poor standards and practices. There are also likely to be issues for UK companies who build or use AI systems attempting to enter foreign markets, if they have developed systems or practices that do not meet more rigorous legal standards.

RECOMMENDATIONS:

RECOMMENDATION 1. In light of the ongoing rapid expansion of AI surveillance, the Government should commission an independent national review of the scale, capabilities, ethics and rights impact of modern surveillance cameras in the UK.

RECOMMENDATION 2. The Human Rights Act 1998 and Data Protection Act 2018 provide essential protections for fundamental rights in the context of emerging technologies and must be protected.

RECOMMENDATION 3. We agree with recommendation 19 (paragraph 112) made by the House of Lords' Justice and Home Affairs Committee in their March 2022 inquiry report, Technology Rules? The advent of new technologies in the justice system:

> **"Full participation in the Algorithmic Transparency Standard collection should become mandatory, and its scope extended to become inclusive of all advanced algorithms used in the application of the law that have direct or indirect implications for individuals. This would have the effect of turning the collection into a register."[23]**

23 Technology Rules? The advent of new technologies in the justice system - ustice and Home Affairs Committee, 1st Report of Session 2021-22 - 30 March 2022 - HL Paper 180: https://publications.parliament.uk/pa/ld5802/ldselect/ldjusthom/180/18002.htm

RECOMMENDATION 4. In the case of human decisions supported by AI, frequent audits should be undertaken to assess and compare AI decision recommendations to the human decisions made, and assess any patterns of discrepancies.

RECOMMENDATION 5. A strengthened and mandatory Algorithmic Transparency Standard, as well as well-resourced regulators such as the Information Commissioner, Equality and Human Rights Commission, and oversight provided by the Biometrics and Surveillance Camera Commissioner, are vital to ensure that the regulatory mechanisms that exist can be fully operationalised.

RECOMMENDATION 6. Further clarity is required on both what constitutes a "solely automated" decision, and what constitutes a significant decision that meets the threshold to trigger the legal safeguards provided by Article 22 of the GDPR.

RECOMMENDATION 7. The UK should legislate to prohibit the most serious algorithmic and AI harms that are already affecting the public – such as live facial recognition surveillance.