BIG BROTHER WATCH

Big Brother Watch's response to the Government's consultation the 'A pro-innovation approach to AI regulation' White Paper

June 2023

CONTENTS

INTRODUCTION

Big Brother Watch welcomes the opportunity to respond to the Government's White Paper on AI governance: 'A pro-innovation approach to AI regulation'.

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, and in particular, automated decision-making.**

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.

We have responded to this consultation by addressing questions thematically, to avoid duplication of answers.

TRANSPARENCY

1. Do you agree that requiring organisations to make it clear when they are using AI would improve transparency?

2. Are there other measures we could require of organisations to improve AI transparency?

Transparency is essential for the public and regulators to understand how and where AI is being used. We are concerned about a lack of transparency as to the data used in building AI systems, AI use in the public sector, and AI use in decision-making. This is particularly crucial when AI is used to make automated decisions about individuals or communities. However, we are concerned that transparency requirements on all of these fronts are being reduced by the Data Protection and Digital Information No.2 Bill (DPDI2 Bill), which significantly weakens the definition of personal data, replaces the requirement for Data Protection Impact Assessments, and weakens transparency and other protections with regards to automated decision-making. Even so, while transparency is a vital tool for the regulation of AI, it is important to note that transparency alone cannot and will not mitigate the harms that some AI systems perpetuate. Transparency must be the *minimum* requirement throughout the

1 Poverty Panopticon – Big Brother Watch, July 2021: https://bigbrotherwatch.org.uk/wpcontent/uploads/2021/07/Poverty-Panopticon.pdf
2 Biometric Britain: The Expansion of Facial Recognition Surveillance, May 2023: https://bigbrotherwatch.org.uk/wp-content/uploads/2023/05/Biometric-Britain.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

development and use of AI, but it should not be framed as the primary approach to preventing harm. The first and foundational approach to developing and using AI systems should be to evaluate its efficacy, necessity and proportionality, in line with human rights and data protection law.

As it stands, there is currently a serious lack of transparency around public authorities' and private companies' uses of AI in decision-making. As such, it is difficult for the public and civil society to know how AI is being used, and therefore to understand, challenge its use and seek redress from any harms that may arise.

Automated decision-making is increasingly being used in important contexts such as welfare, immigration, and the criminal justice system. It provokes a range of concerns including encoded bias and discriminatory outcomes, data rights and privacy issues, transparency, accountability and redress, amongst other issues. 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. Individuals should also be informed when their personal data is used to train or develop AI systems.

However, the DPDI2 Bill dilutes existing rights in this regard. Under Article 22 of the UK GDPR, data subjects currently have the right not to be subject to a decision with legal effect (e.g. denying a social benefit granted by law) or similarly significant effect (e.g. access to education, employment or health services) based solely on automated processing or profiling, unless there is a legal basis to do so (e.g. explicit prior consent, a contract between the data subject and the controller, or where such activity is required or authorised by law).[4]

Big Brother Watch welcomes the clarification in the DPDI2 Bill, which we have long called for, defining a decision based on solely automated processing as one that involves "no meaningful human involvement". However, we have grave concerns about the broader reversal of the Article 22 right not to be subjected to solely automated decisions.

The DPDI2 Bill replaces Article 22 with Article 22A-D, which redefines automated decisions and would enable solely automated decision-making in far wider circumstances. Where automated decision-making (ADM) is currently broadly prohibited with specific exceptions, the Bill would broadly permit ADM and only restrict

4 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 17/EN/WP/251 rev. 01, WP29 (2018): https://ec.europa.eu/newsroom/article29/items/612053 21-22; UK data protection reform and the future of the European data protection framework - Jim Killock, Ana Stepanova, Han-Wei Low and Mariano delli Santi, 26th October 2022: https://eu.boell.org/en/uk-data-protection-reform

it in very limited circumstances. Whereas the law currently prescribes a number of transparency and redress safeguards with regards to automated decisions authorised by law – namely, that the controller must notify the data subject and that the data subject has the right to request a new decision (including one that is not automated) – Article 22C only requires that the controller ensures safeguards are in place (A22C(1)) and that they include measures which "provide the data subject with information" about the automated decision and enable them to make representations, contest and obtain human intervention with regard to the decision. The proposed requirement to "provide information" is a departure from the current legal requirement to "notify" an individual that they have been subjected to an automated decision – for example, this could be interpreted as a reactive responsibility if information is requested, rather than a proactive duty, or it could even be interpreted as a general responsibility that could be addressed with generic references to ADM in privacy policies. The explanatory notes to the Bill clarify that newly permitted automated decisions will not require the existing legal safeguard of notification, stating that only "*where appropriate*, this *may* include notifying data subjects after such a decision has been taken"[5] (emphases added). This is an unacceptable dilution of a critical safeguard that will not only create uncertainty for organisations seeking to comply, but could lead to vastly expanded ADM operating with unprecedented opacity. If AI decisions take place effectively in secret, data subjects may not even know they are being subjected to ADM and cannot exercise their legal rights in practice. Therefore, we would question what exactly the government means by "transparency" in this regard, as the current legislative direction is to weaken transparency requirements.

Case study: DeepMind

In a health scenario, the impact of a lack of transparency 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 the company had been given access to unlawfully. 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. In the ICO's finding that the NHS Royal Free Trust unlawfully shared patient data with DeepMind, "the Commissioner has concluded that the data controller did not provide an appropriate level of transparency

5 Data Protection And Digital Information (No. 2) Bill - Explanatory Notes, p 35, para 177, 8th March 2023: https://publications.parliament.uk/pa/bills/cbill/58-03/0265/en/220265env2.pdf

to patients about the use of their personal data" and transparency requirements were a key consequence of the scandal.[6]

These risks emphasise the need for far more effective transparency mechanisms such as a mandatory public register of significant AI uses, including the personal data used to initiate and build AI systems; and the vital importance of preserving our data protection and privacy standards in the Data Protection Act 2018 and Human Rights Act 1998.

Commercial confidentiality is a significant barrier to transparency. Often, developers of AI systems use commercial concerns as a shield to prevent public understanding of where and how AI is used, even in the public sector. The Ada Lovelace Institute noted in its evidence to the Science, Innovation and Technology Committee's inquiry into AI governance:

> "*(...)the inspection of systems becomes much more difficult when those systems are provided by third parties, as much of information required for inspection is proprietary, and AI developers and tech companies are often unwilling to share information that they see as integral to their business model.*
>
> *"Indeed, many prominent developers of AI systems have cited intellectual property and trade secrets as reasons to actively disrupt or prevent attempts to audit or assess their systems. With this in mind it will be paramount to ensure that access to third party systems and information is included in any statutory regulation."*[7]

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 system. Our report, *Poverty Panopticon: the hidden algorithms shaping Britain's welfare state,*[8] 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 this regard 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

6 Data Protection Act 1998 Undertaking: Royal Free London NHS Foundation Trust - The Information Commissioner's Office: https://ico.org.uk/media/action-weve-taken/undertakings/2014352/royal-free-undertaking-03072017.pdf

7 Written evidence submitted by Ada Lovelace Institute - Science, Innovation and Technology Committee inquiry on Governance of Artificial Intelligence, November 2022, GAI0086: https://committees.parliament.uk/writtenevidence/113850/pdf/

8 Poverty Panopticon: the hidden algorithms shaping Britain's welfare state – Big Brother Watch, 20th July 2021: https://bigbrotherwatch.org.uk/wp-content/uploads/2021/07/Poverty-Panopticon.pdf

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. As discussed, this highly limited transparency requirement is set only to weaken as the legal definition of personal data and the right not to be subject to a solely automated decision are both set to be diluted in the DPDI2 Bill.

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. 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. As discussed, DPIAs will no longer be required under the DPDI2 Bill.

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.

In November 2021, the Central Digital and Data Office launched the Algorithmic Transparency Standard, which is currently being piloted with several public bodies.[9] 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.

We agree with Recommendation 19 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*:

9 Algorithmic Transparency Recording Standard Hub – GOV.UK, 5th January 2023, accessed 9th June 2023: https://www.gov.uk/government/collections/algorithmic-transparency-recording-standard-hub

> "*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.*"[10]

REDRESS FOR AI-RELATED HARMS

3. Do you agree that current routes to contest or get redress for AI-related harms are adequate?

4. How could current routes to contest or seek redress for AI-related harms be improved, if at all?

Currently, one of the largest barriers to contesting or seeking redress for AI-related harms is the lack of transparency around when AI has been used to make a decision, as addressed above.

From a rights-based approach, the legal frameworks most relevant to contesting or seeking redress from AI-related harms 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, South Wales Police's use of live facial recognition surveillance, which was found to be unlawful in the *Bridges* case. More must be done to ensure that public and private organisations using AI are aware of their 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.

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 does not adequately provide remedy.

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,

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

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.

Case study: Durham Police's HART tool

In 2018, Big Brother Watch found that Durham Police paid global data broker Experian for UK postcode stereotypes built on 850 million pieces of information to feed into an AI tool used in custody decisions. The tool processed Experian's 'Mosaic' data and other personal information to predict whether a suspect might be at low, medium or high risk of reoffending.

Durham Police fed the 'Mosaic' data, which profiles all 50 million adults in the UK to classify UK postcodes, households and even individuals into stereotypes, into its AI 'Harm Assessment Risk Tool' (HART). The 66 'Mosaic' categories included 'Disconnected Youth', 'Asian Heritage' and 'Dependent Greys'.

Mosaic codes included the 'demographic characteristics' of each stereotype – characterising 'Asian Heritage' as 'extended families' living in 'inexpensive, close-packed Victorian terraces', adding that 'when people do have jobs, they are generally in low paid routine occupations in transport or food service'. 'Disconnected Youth' were characterised as 'avid texters' whose 'wages are often low'– with first names like 'Liam' and 'Chelsea'.

Experian's 'Mosaic' also linked names to stereotypes: for example, people called 'Stacey' were likely to fall under 'Families with Needs' who receive 'a range of benefits'; 'Abdi' and 'Asha' were 'Crowded Kaleidoscope' described as 'multi-cultural' families likely to live in 'cramped' and 'overcrowded flats'; whilst 'Terrence' and 'Denise' were 'Low Income Workers' who have 'few qualifications' and 'heavy TV viewers'.

Durham Police's AI risk predictions guided decisions as to whether a suspect should be charged or released onto the 'Checkpoint' rehabilitation programme. Moderate risk suspects were informed that if they successfully complete the Checkpoint programme they will not receive a criminal conviction.

Three weeks after Big Brother Watch's expose, Durham Police dropped the use of the tool, and Experian subsequently changed its Mosaic categories.[11]

The government has outlined its intention to overhaul the Data Protection Act 2018 via the DPDI2 Bill. We, along with many civil society groups, are extremely concerned

11 Police drop Experian profiling tool following Big Brother Watch exposé – Big Brother Watch, 14th June 2019: https://bigbrotherwatch.org.uk/2019/06/police-drop-experian-profiling-tool-for-ai-custody-decisions-following-big-brother-watch-expose/

about these proposals and the impact they will have on individuals' rights in the context of AI and automated decision making. Our analysis of the DPDI2 Bill shows that it would seriously weaken the existing accountability framework for personal data use and the approach to automated decision-making will be radically more permissive. The government must commit to maintaining standards at least as high as the Data Protection Act, and remaining party to the European Convention on Human Rights, as a foundation for protection from AI-related harms, as well as introducing further regulation, such as a Digital Rights Bill, to protect the public from the most dangerous uses of AI.

CROSS-SECTOR PRINCIPLES

5. Do you agree that, when implemented effectively, the revised cross-sectoral principles will cover the risks posed by AI technologies?

6. What, if anything, is missing from the revised principles?

The White Paper acknowledges that "Government intervention is needed to improve the regulatory landscape."[12] However, it does not propose any new legislation to oversee the development and use of AI systems. Instead, the White Paper sets out "a principles-based framework for regulators to interpret and apply to AI within their remits",[13] with five "values-focused cross-sectoral principles".[14] 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."[15] Far from a "pro-innovation" approach, this will create an uncertain environment that is out of step with the clearer legislative approach being taken in the rest of Europe.

The only proposed legislative change would be to require regulators to "have due regard" to the five principles. This would not come into force until after an (undefined) "period of non-statutory implementation" and "when parliamentary time allows".[16] It is not clear whether or how this duty would be enforced. Although the introduction of a statutory duty is preferable to a total absence of statutory obligations, the use of

12 A pro-innovation approach to AI regulation – Department for Science, Innovation and Technology, GOV.UK, 29th March 2023, para 30: https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper

13 A pro-innovation approach to AI regulation – Department for Science, Innovation and Technology, GOV.UK, 29th March 2023, para 36: https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper

14 A pro-innovation approach to AI regulation – Department for Science, Innovation and Technology, GOV.UK, 29th March 2023, para 48: https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper

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

16 A pro-innovation approach to AI regulation – Department for Science, Innovation and Technology, GOV.UK, 29th March 2023, para 57: https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper

cross-sector principles to regulate the development and use of AI will not provide the robust safeguards so urgently needed. Indeed, the White Paper does not even commit to introducing this thin statutory duty, stating if monitoring "suggests that a statutory duty is unnecessary, [the government] would not introduce it."[17]

The cross-sectoral principles will not cover the risks posed by AI technologies. While they broadly set out commendable concepts such as fairness, explainability, safety, accountability and contestability, without a statutory basis and regulation that sets out how they will be enforced, they will serve little purpose. The DPDI2 Bill already radically reduces safety, accountability and contestability with regards to automated decision-making, meaning the regulator will be working with a weak framework insofar as it applies to AI.

The principles are overly vague and flexible, allowing each regulator to define and apply them differently. For example, the suggestion that "AI systems should be *appropriately* transparent and explainable" and references to an "*appropriate* level" of transparency when defining these principles means that regulators have huge discretion in interpreting what is 'appropriate' in their sector, within the confines of weak, inadequate legislation.[18] This could not only see significant gaps in protections, but also serious divergence between regulators as to what an 'appropriate' level of transparency is, causing confusion for businesses and an uneven regulatory environment.

Indeed, the White Paper goes on to state that "it may be the case that not every regulator need introduce measures to implement every principle [...] a regulator may exercise their expert judgement and determine that their sector or domain does not require action to be taken."[19] Given the serious risk of significant harm that AI technologies can pose across virtually every area of public life, this approach is not sufficient. It will lead to a deeply confused regulatory environment and leaves the door open to deeply damaging social, economic, political and rights impacts.

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*

17 A pro-innovation approach to AI regulation – Department for Science, Innovation and Technology, GOV.UK, 29th March 2023, para 59: https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper

18 A pro-innovation approach to AI regulation – Department for Science, Innovation and Technology, GOV.UK, 29th March 2023, para 52, emphasis added: https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper

19 A pro-innovation approach to AI regulation – Department for Science, Innovation and Technology, GOV.UK, 29th March 2023, para 58: https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper

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."[20]

Other groups have also been critical. The TUC stated that the "white paper is vague and fails to offer any clear guidance to regulators"[21] while the Ada Lovelace Institute warned of "significant gaps" in the proposals.[22]

The stable, pioneering and world-leading AI governance that the UK aspires to will need to move beyond recommendations, guidance and principles. It is essential that AI systems that pose novel, unique and serious threats to human rights, from intrusive and ineffective new forms of biometric surveillance to unconsented pornographic deepfakes, are met with strong and specific legislation. Some of these risks could be addressed in a Digital Rights Bill. Further, it is vital that standards of legislation that is foundational to AI in the UK such as the Data Protection Act and UK GDPR are maintained rather than weakened, and robustly enforced. This is particularly important for ensuring that AI systems that are used to make decisions about individuals are subject to stringent, legally enforceable, regulations.

CENTRAL GOVERNMENT FUNCTIONS

9. Do you agree that the functions outlined in Box 3.1 would benefit our AI regulation framework if delivered centrally?

10. What, if anything, is missing from the central functions?

The premise underpinning the central government functions, and the White Paper's AI framework as a whole, is that limited, or no, intervention is needed to safeguard rights in the context of AI. The White Paper repeatedly states the government will rely on further monitoring to mitigate harms, assessing the risks of AI as they arise, and essentially taking a 'wait and see' approach to AI-related harms. This is the riskiest possible approach. As demonstrated by the current panic around generative AI, high-risk tools with complex impacts are hard to mitigate once they have been built and released into an under-regulated environment. By the time AI risks arise, it is likely to be too late to take action that protects people from harm.

20 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

21 TUC criticises "flimsy" and "vague" Artificial Intelligence (AI) white paper – politics.co.uk, 30th March 2023: https://www.politics.co.uk/opinion-former/press-release/2023/03/30/tuc-criticises-flimsy-and-vague-artificial-intelligence-ai-white-paper/page/26/

22 UK rules out new AI regulator – BBC News, 29th March 2020: https://www.bbc.co.uk/news/technology-65102210

There is no absence of evidence about current and future risks posed by AI, and as such, no reason to delay and wait for people to be harmed before taking action. The AI Now Institute argues in its recent annual report:

> *"We have abundant research and reporting that clearly documents the problems with AI and the companies behind it. This means that more than ever before, we are prepared to move from identifying and diagnosing harms to taking action to remediate them."*[23]

In the UK alone, harms arising from irresponsible, unethical and unlawful uses of AI are already occurring in education,[24] healthcare,[25] policing,[26]welfare[27] and beyond. While we welcome the government's plan to create a "society-wide AI risk register" and to "identify and prioritise new and emerging risks", the framework set out in the White Paper does little to address current, well-known and well-documented risks.[28] The government should be ahead rather than behind the curve, seeking to take an ambitious regulatory approach that prohibits the most dangerous uses of AI and upholds citizens' rights, as the EU is currently set to do, rather than attempting to roll back current protections (via the DPDI2 Bill) and offering flimsy principles to oversee AI development and use.[29]

REGULATORS

7. Do you agree that introducing a statutory duty on regulators to have due regard to the principles would clarify and strengthen regulators' mandates to implement our principles while retaining a flexible approach to implementation?

8. Is there an alternative statutory intervention that would be more effective?

14. How can we avoid overlapping, duplicative or contradictory guidance on AI issued by different regulators?

L1. What challenges might arise when regulators apply the principles across different AI applications and systems? How could we address these challenges through our proposed AI regulatory framework?

---

23 2023 Landscapre: Confronting Tech Power – Amba Kak and Dr. Sarah Myers West, AI Now Institute, 11th April 2023: https://ainowinstitute.org/wp-content/uploads/2023/04/AI-Now-2023-Landscape-Report-FINAL.pdf

24 Ofqual's A-level algorithm: why did it fail to make the grade? - Alex Hern, the Guardian, 21st August 2020: https://www.theguardian.com/education/2020/aug/21/ofqual-exams-algorithm-why-did-it-fail-make-grade-a-levels

25 DeepMind faces legal action over NHS data use – BBC News, 1st October 2021: https://www.bbc.co.uk/news/technology-58761324

26 Facial recognition use by South Wales Police ruled unlawful – BBC News, 11th August 2020: https://www.bbc.co.uk/news/uk-wales-53734716

27 Calls for legal review of UK welfare screening system which factors in age – Robert Booth, the Guardian, 18th July 2021: https://www.theguardian.com/society/2021/jul/18/calls-for-legal-review-of-uk-welfare-screening-system-that-factors-in-age

28 A pro-innovation approach to AI regulation – Department for Science, Innovation and Technology, GOV.UK, 29th March 2023, box 3.1: https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper

29 EU moves closer to passing one of world's first laws governing AI – Lisa O'Carroll, the Guardian, 14th June 2023: https://www.theguardian.com/technology/2023/jun/14/eu-moves-closer-to-passing-one-of-worlds-first-laws-governing-ai

As addressed in previous sections, Big Brother Watch does not agree that the proposals set out in the White Paper – whereby the use and development of AI are only governed by cross-sector principles, overseen by regulators – are sufficient to safeguard human rights and data protection.

Crucially, many sectors of public life are not currently covered by specific regulators, or are covered by a range of regulators. Transport, for example, is regulated by the Civil Aviation Authority, the Driver and Vehicle Standards Agency, the Maritime and Coastguard Agency, the Department for Transport, the Office of Rail and Road and Traffic Commissioners for Great Britain. Areas such as employment and recruitment, although subject to data protection law and equalities law, are not overseen by a specific regulator. The White Paper does not meaningfully engage with these concerns, beyond stating the government will "identify and assess gaps in the regulatory ecosystem".[30]

In the absence of a clear regulatory framework, it is unavoidable that regulators will produce contradictory and uneven guidance. The White Paper states that the government anticipates "that developing joint guidance will be a priority for regulators" and that this joint guidance, in conjunction with central government oversight will ensure coherent implementation of principles across different regulators.[31] In reality, this will result in a vast quantity of different sets of guidance for businesses, as each regulator will produce sector-specific guidance as well as joint guidance produced with a range of other regulators. Given the considerable scope the White Paper sets out for regulators to determine how they will interpret the principles, this could cause difficulty for regulators, uncertainty for organisations and confusion for the public. The White Paper acknowledges "a risk that some regulators could begin to dominate and interpret the scope of their remit or role more broadly than may have been intended in order to fill perceived gaps in a way that increases incoherence and uncertainty."[32] However, the White Paper does not set out any proposal to prevent this taking place. The only solution is for clear, legally enforceable statutory restrictions to be introduced by Parliament and to be interpreted by the courts where warranted.

The decision to leave the enforcement and consequences of contravention so vague is also deeply concerning. The White Paper makes only passing references to enforcement, simply stating "regulators are best placed to conduct [...] enforcement activities within their areas of expertise" and offers no suggestion as to what

30 A pro-innovation approach to AI regulation – Department for Science, Innovation and Technology, GOV.UK, 29th March 2023, para 66: https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper

31 A pro-innovation approach to AI regulation – Department for Science, Innovation and Technology, GOV.UK, 29th March 2023, para 52: https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper

32 A pro-innovation approach to AI regulation – Department for Science, Innovation and Technology, GOV.UK, 29th March 2023, para 29: https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper

enforcement action might be appropriate.[33] Regulators currently have varying levels of enforcement powers. Some are able to issue fines, such as the Information Commissioner's Office, others are able to suspend the actions of businesses, such as the Financial Conduct Authority, others have inspection powers, such as the DVSA and Ofqal, and others have the power to prosecute, such as the Pensions Regulator. Such varying powers, with no clear, binding rules on how regulators should respond to harm arising from the use of AI, enforcement will inevitably vary from sector to sector.

PRO-INNOVATION APPROACH

22. Do you have any other thoughts on our overall approach? Please include any missed opportunities, flaws, and gaps in our framework.

We are deeply concerned that the government's approach to AI governance will do little to safeguard the rights of individuals from the harms raised by the widespread use of AI technologies. Rather than learning the lessons from several decades of technology-enabled rights violations that have occurred both in the UK and globally, the White Paper takes that view that strong, clear protections are not warranted, and that it is "too soon" to make important designations about accountability and legal responsibility.[34] Instead, the White Paper proposes extremely limited inventions, no extension of the remit of regulators tasked with overseeing the development and use of AI, and no new legally regulations outlining safeguards on the development and use of AI technologies. As a result, AI businesses cultivated in the UK may not benefit from the longevity and international appeal that AI companies grown in the EU and other regions with stronger regulations might do.

Not only is this approach damaging to rights, but it is undemocratic. The growing use of AI in education, healthcare, policing, national security, employment and beyond is one of the biggest challenges society faces. A survey conducted by the Centre for Data, Ethics and Innovation found that a large proportion of respondents used words such as 'worry', 'scary', 'concern' and 'nervous' to describe their feelings towards AI,[35] while a survey conducted by the Ada Lovelace Institute and The Alan Turing Institute found that 62% of respondents would like to see laws and regulations guiding the use of AI technologies.[36] Despite the Prime Minister's recent pledges to make the UK the

33 A pro-innovation approach to AI regulation – Department for Science, Innovation and Technology, GOV.UK, 29th March 2023, para 47: https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper

34 A pro-innovation approach to AI regulation – Department for Science, Innovation and Technology, GOV.UK, 29th March 2023, para 83: https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper

35 Public Attitudes to Data and AI Tracke Survey – Centre for Data, Ethics and innovation, GOV.UK, December 2021: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1092140/Public_Attitudes_to_Data_and_AI_-_Tracker_Survey.pdf

36 How do people feel about AI? - Ada Lovelace Institute and The Alan Turing Institute, 6th June 2023: https://www.adalovelaceinstitute.org/report/public-attitudes-ai/

"home of global AI safety regulation",[37] the 'pro-innovation' approach set out in the White Paper brushes safety concerns aside and leaves the British public vulnerable to unethical and unlawful uses of AI.

Analysis of the government's White Paper from leading experts in AI policy from the Oxford Internet Institute and Alan Turing Institute found that the:

> *"growing domestic emphasis from the central government on promoting innovation through weakening checks (...) will undermine the effectiveness and ethical permissibility of UK AI governance initiatives"*
>
> *(...)*
>
> *"Accordingly, for the UK to fulfil its ambition of producing "trustworthy", "pro-innovation", and "world leading" AI governance, a change of direction in UK policy is needed that strengthens sectoral regulatory powers, capacities, and coordination, while positioning the UK internationally as an agile and innovative AI regulator."*[38]

It is concerning that the government 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.

Countries around the world are starting to legislate for the impacts of AI on the public, and the White Paper rightly acknowledges the "complex and cross-border nature of AI supply chains" and the fact that "many AI businesses [are] operating across multiple jurisdictions".[39] However, it is difficult to see how the government will be able to "promote interoperability and coherence between different approaches" given the UK's current direction, which diverges significantly from other jurisdictions.[40]

37 AI could be used to boost food supply and healthcare under new UK government plans, announces Rishi Sunak - Eleanor Langford and Chloe Chaplain, iNews, 12th June 2023: https://inews.co.uk/news/politics/ai-boost-food-supply-healthcare-new-uk-government-plans-rishi-sunak-2405038

38 Artificial intelligence regulation in the United Kingdom: a path to good governance and global leadership? - Huw Roberts et al, Internet Policy Review (2023): https://policyreview.info/articles/analysis/artificial-intelligence-regulation-united-kingdom-path-good-governance

39 A pro-innovation approach to AI regulation – Department for Science, Innovation and Technology, GOV.UK, 29th March 2023, para 117: https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper

40 A pro-innovation approach to AI regulation – Department for Science, Innovation and Technology, GOV.UK, 29th March 2023, para 118: https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-

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, while proposals have been made for an Algorithmic Accountability Act. 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 far from perfect, the Act acknowledges the importance of prohibiting certain high-risk AI practices, such as social scoring and open-ended remote biometric identification.

In the US, the White House announced its blueprint for an AI Bill of Rights, stressing that the "important progress [AI can bring] must not come at the price of civil rights or democratic values" and setting out key rights of citizens in relation to AI, such as the right to be protected from ineffective or biased AI systems.[41] An Algorithmic Accountability Act was introduced in February 2022, and similarly to the EU, it takes a risk-based approach. It proposes that organisations deploying AI systems take steps to mitigate harm and bias within AI systems.

This 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.

It is disappointing that as countries are beginning to legislate to lay the foundations for a high-tech future and protect people from AI risks, the UK is seeking to weaken citizens' current rights and protections whilst waiting to for risks to manifest. Far from world-leading, this is a thoroughly retrograde approach that will disadvantage UK businesses and citizens alike.

approach/white-paper

41 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/