

LIBERTY

LIBERTY'S WRITTEN SUBMISSION TO A PRO- INNOVATION APPROACH TO AI REGULATION CONSULTATION

JUNE 2023

ABOUT LIBERTY

Liberty is an independent membership organisation. We challenge injustice, defend freedom and campaign to make sure everyone in the UK is treated fairly. We are campaigners, lawyers and policy experts who work together to protect rights and hold the powerful to account.

Liberty provides policy responses to Government consultations on all issues which have implications for human rights and civil liberties. We also submit evidence to Select Committees, inquiries and other policy fora, and undertake independent, funded research.

Liberty's policy papers are available at libertyhumanrights.org.uk/policy.

CONTACT

EMMANUELLE ANDREWS

Policy and Campaigns Manager

emmanuellea@libertyhumanrights.org.uk

CONTENTS

INTRODUCTION	1-2
THE REVISED CROSS-SECTORAL PRINCIPLES	2-17
A STATUTORY DUTY TO REGARD	17-20
MONITORING AND EVALUATION OF THE FRAMEWORK	20-23
LEGAL ACCOUNTABILITY FOR AI	23-26
CONCLUSION	26-27

INTRODUCTION

1. We are witnessing the rise of artificial intelligence at an unprecedented rate: from bank services detecting fraudulent activity, to decisions made in the name of national security. The direction of travel in the public sector – at both a national and local level – is towards greater digitisation and automation. Current legal frameworks governing Artificial Intelligence are not fit for purpose, and are failing to keep pace with the rise in use across different sectors and contexts. Amidst the growing use of artificial intelligence in the UK, as well as public debates about its potential and harms, the Government’s White Paper on AI regulation is long overdue. Liberty welcomes the opportunity to respond to the call for inputs from the Office of AI in the Department for Science, Innovation & Technology into the Government’s approach to regulation of artificial intelligence (AI).¹
2. In our response to this Consultation – which we limit to questions 1-8, 15, L.1 and L.2 – we make the following arguments:
 - a. The Government’s central aim, which shapes the content of its regulatory approach, is for the UK to be world-leading on AI. But rather than becoming world-leading in terms of setting best practice, and protecting the public from the harms of AI, the Government takes the facilitation of innovation as its foundation. We believe this is misplaced: human rights, democratic principles and the rule of law should be the starting point when assessing intrusive technology which fundamentally changes public decision-making and implicates the rights of millions.
 - b. Consequently, the White Paper falls short of implementing the necessary steps to safeguard against the range of existing and potential human rights harms. Indeed, the phrase ‘human rights’ can be counted a mere handful of times. As Liberty and other civil society groups have argued elsewhere, the Government “misses a vital opportunity to ensure that fundamental rights and democratic values are protected.”²

¹ Call for Inputs available at: <https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach>

² Public Law Project et al, Key Principles for an alternative AI white paper, (June 2023). <https://publiclawproject.org.uk/content/uploads/2023/06/AI-alternative-white-paper-in-template.pdf>

- c. The proposals set out in this consultation are too vague to provide much-needed clarity and guidance on AI regulation. The principles are not mandatory, and despite the declaration to consider legislation “when parliamentary time allows,” there does not seem to be a commitment to do so (and indeed, the Government state they will only do so if the current non-legislative approach does not achieve the principal objective of encouraging innovation).³
- d. The White Paper gives regulators immense responsibility. Yet, without commitment from Government to expand their remit, or provide them with the resources, they will not have enough capacity and expertise to play a sufficient role.
- e. Meanwhile, the Government is weakening existing standards and stripping back the role of regulators elsewhere: from the Data Protection and Digital Information (No.2) Bill, to threats to leave the European Convention on Human Rights, and legislation which disapplies part of the Human Rights Act for certain groups of people.
- f. Uses of AI that threaten fundamental rights should be prohibited. Yet the Government forecloses the possibility of banning harmful AI through its plans to “regulate the use – not the technology” and its explicit refusal in the White Paper to ban particular forms of AI such as facial recognition technology. We do not believe that an open, flexible regime, with robust statutory principles that cover all forms of AI need be at odds with strong legal frameworks prohibiting rights-abusing forms of AI outright.

THE REVISED CROSS-SECTORAL AI PRINCIPLES

QUESTION 1: DO YOU AGREE THAT REQUIRING ORGANISATIONS TO MAKE IT CLEAR WHEN THEY ARE USING AI WOULD ADEQUATELY ENSURE TRANSPARENCY?

³ A Pro-Innovation Approach to AI, p.6.

QUESTION 2: WHAT OTHER TRANSPARENCY MEASURES WOULD BE APPROPRIATE, IF ANY?

3. In the AI White Paper, the Government considers “appropriate transparency and explainability” one of the five principles underpinning the regulatory framework, alongside “safety, security and robustness; fairness; accountability and governance; and contestability and redress.”⁴
4. We wholeheartedly agree that transparency – including requiring organisations to make it clear when they are using AI – is a vital step in AI Governance. Without knowledge that AI is being used, the public cannot meaningfully consent to its use, and it prevents access to meaningful recourse should a person wish to challenge the outcomes of an AI system, particularly in contexts of automated decision making (ADM). Transparency is thus an essential prerequisite for accountability, as well as the enforcement of a plethora of other legal rights by those affected.
5. Yet, we are concerned by the Government’s framing of transparency with the caveat that it is limited to what is “appropriate”, and the inherent suggestion that there can be a surplus. To give effect to the principle of transparency, especially when used by public bodies, there need to be clear rules, supported in legislation, that mandate the publication of information specifying not just when AI is being used, but also that such notice is prominent, clear, and includes information regarding avenues for complaints or appeals regarding the decisions. Transparency does not necessarily mean that every detail of an AI system is presented, and indeed, what, and how information is presented is an important tool to aid the public’s understanding of an AI system in practice. Transparency and explainability must work in tandem, and this is achieved by ensuring that transparent information is accessible, not that access to information is limited. There are numerous examples of good practice that the Government could refer to in order to make the transparency principle more meaningful. The Public Law Project’s (PLP) Tracking Automated Government (TAG) Register – a register on public bodies’ use of AI – for example, details a range of important information including the tool, purpose, policy area, public body, developer and use period of the AI system, details how the algorithm functions, whether the system makes decisions about individuals or groups, or

⁴ A Pro-Innovation Approach to AI, p.27.

makes decisions that affect people’s legal rights, as well as other important things.⁵ It is also a user friendly, and accessible tool.

6. Nevertheless, by limiting transparency towards only an ‘appropriate’ level (whatever that should mean), the Government enables the controllers of AI systems to make their own judgements about what information to share, and it is already a challenge to understand when AI systems are being used, without the Government setting limits. A significant barrier to transparency in the context of AI systems, is the extent of the involvement of the private sector in their development, and in some cases, their implementation (in collaboration with the public sector). Private companies are often reluctant to publicise their data and code for proprietary reasons. Crucially, unlike public bodies, the private sector is not bound by the same safeguards – such as the Public Sector Equality Duty within the Equality Act (EA) – and is able to shield itself from criticisms regarding transparency behind the veil of ‘commercial sensitivity.’ A mandatory disclosure of information on procurement when private companies supply public bodies with AI, might support public bodies’ own compliance with transparency standards.
7. Beyond use by private companies, public sector bodies have also been less than forthcoming with their AI use. During their research towards building their TAG Register, PLP found that there was opacity around the details, deployment and even the mere existence of AI systems in the public sector.⁶ Similarly, in the review of Artificial Intelligence and Public Standards by the Committee on Standards in Public Life, the Committee found that “even those working closely with the UK Government on the development of AI policy, including the staff at the Alan Turing Institute and the Centre for Data Ethics and Innovation, expressed frustration at their inability to find out which government departments were using these systems and how.”⁷ Writing their report in 2020, the Committee identified that the Government did not yet publish any centralised audit identifying and making publicly available the extent of AI use across central government or the

⁵ Public Law Project, Tracking Automated Government (TAG) Register. <https://trackautomatedgovernment.shinyapps.io/register/>

⁶ Public Law Project, Written Evidence Submitted to House of Commons Science and Technology Committee’s Inquiry into AI Governance, p.3. <https://publiclawproject.org.uk/resources/governance-of-artificial-intelligence-evidence-submission/>

⁷ Artificial Intelligence and Public Standards: A Review, February 2020, Committee on Standards in Public Life, p.15. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/868284/Web_Version_AI_and_Public_Standards.PDF

wider public sector, and that much of what we know is the result of journalists, civil society and academics, who have to rely on freedom of information requests, parliamentary questions or poorly formatted procurement data.⁸

8. Fast forward three years, and the Government is yet to heed these warnings. Despite calls during the pilot of the Cabinet Office’s Algorithmic Transparency Recording Standard (ATS) – a hub collecting a standardised way of recording and sharing information about how the public sector uses algorithmic tools – to make the ATS compulsory, the ATS remains optional.⁹ Without being compulsory, public bodies may decide whether and when to engage, which is deeply inappropriate given the significance of AI systems for key public decisions and their ability to impact on people’s rights. With the opportunity to strengthen the existing transparency framework, we are concerned to see that the Government has no plans to put this principle, or indeed any of the others, on a statutory footing. In the meantime, the burden currently falls upon small NGOs to undertake research and dedicate small resources to making the use of AI by public bodies visible and accessible to the public, as in PLP’s TAG Register. The Government is therefore already failing at its own stated aims of making AI use transparent – even ‘appropriately’.
9. Moreover, the Government states that “an appropriate degree of transparency and explainability should be proportionate to the risk(s) presented by an AI system.”¹⁰ We would argue that it is often not possible to know if an AI system is risky *without* transparency in the first place. Transparency is essential in order to assess risks on a macro level: with the public determining whether an AI system should be used in society at all, and if so, how; as well as on a micro level: in order for individuals to understand how the state or organisations are making decisions that impact on them, assess how dangerous those decisions are, and decide whether to challenge them. Further, even those that have taken a risk-

⁸ Artificial Intelligence and Public Standards: A Review, February 2020, Committee on Standards in Public Life, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/868284/Web_Version_AI_and_Public_Standards.PDF

⁹ Algorithmic Transparency Recording Standard Hub, <https://www.gov.uk/government/collections/algorithmic-transparency-recording-standard-hub>

¹⁰ A Pro-Innovation approach to AI, p.28

based approach – such as in the EU AI Act – recognise that transparency is an essential component to AI governance, even in so-called low-risk environments.¹¹

10. Regardless of the extent of transparency, it is not a sufficient principle in and of itself. As is well documented by anti-corruption advocates Transparency International, contextual factors and enabling conditions – from media freedom, to education, and from functioning legal systems – are all necessary instruments to make governance processes, of which transparency plays one part, meaningful.¹²
11. In addition to making AI more transparent and explainable to the public, when used by public bodies in particular, we must substantively assess the underlying policy objectives for which AI systems are being deployed, as well as how such systems are being deployed. To understand the purpose of an AI system, and to consider its human rights compatibility, we should follow the human rights principles of necessity and proportionality at every stage of the system’s design and operation, including the decision to collect certain kinds of data, the processes through which this data is collected, processed, and shared, the design of the algorithm, and the effects it has on public decision-making.
12. Similarly, we should consider proportionality by taking into consideration the full AI system. For example, it has been revealed that gig economy companies have previously collected data about workers using disproportionate surveillance tactics, including monitoring when workers have not logged in to make themselves available for work, or flagging workers who fail to accept enough of the work being offered to them on a given platform as fraudulent, thereby effectively coercing them to work longer hours.¹³ Even if this data feeds into an AI system designed for the innocuous purpose of allocating work, the extent and kind of surveillance levied against workers would be enough for us to consider the AI system potentially rights-violative.

¹¹ European Commission, Proposal for a Regulation of the European Parliament and of the Council: Laying Down Harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>

¹² Transparency International, Algorithmic Transparency and Accountability (February 2021). https://knowledgehub.transparency.org/assets/uploads/kproducts/Algorithmic-Transparency_2021.pdf

¹³ Privacy International, Managed by bots: surveillance of gig economy workers, (13 December 2021). <https://privacyinternational.org/long-read/4709/managed-bots-surveillance-gig-economy-workers>

13. Given the many risks inherent in AI (and particularly ADM) systems, it is crucial that - at the very least - they are proven to be effective at their stated purposes on the basis of evidence involving a wide range of stakeholders, objectively researched, and taking into consideration the wider context of systemic oppression that the system is operating in. All too often, new technologies are introduced into a vacuum of evidence. This may happen in the context of an active public relations campaign by a manufacturer that promises to save the police and criminal justice system money in the long-term, as in the case with predictive policing automated decision making programmes;¹⁴ or, as in the case with police use of facial recognition technology (FRT), operational use of new technologies may be simply labelled a "trial", but with little or no oversight – and no consent from those who end up as unwitting participants.¹⁵ By the time there is an evidence base, use has been normalised, and such normalisation forecloses the ability for a wider societal and Parliament-led conversation about whether it is appropriate or desirable to use the AI system in the first place. There may also arise circular logics, whereby public bodies seek to justify the mass collection of personal data on the basis that decision-making systems (including ADM systems) require greater amounts (and better quality) of intelligence; in turn, public bodies may seek to justify the creation of more extensive and unaccountable decision-making systems on the basis that there is simply too much data being collected to be processed without some degree of automation, even when these decisions have effects on our human rights.
14. If an AI system is not effective, then it is unlikely to be necessary or proportionate, but crucially, we also note that effectiveness is not the best or full measure. A fundamentally rights-violative decision-making system - for example, one that is based on fundamentally rights-violative policy - can never be deemed acceptable on the basis of efficiency or effectiveness.
15. An analogous example of this can be found in debates over facial recognition, a technology that is inherently rights-violative (being a technology that will always involve the mass processing of thousands' biometric data and fundamentally changes the nature of public space), and for which transparency and

¹⁴ For example, companies like Experian, Axon, Accenture and BAESystems pitch their technologies to law enforcement.

¹⁵ Liberty (January 2019), *Policing by Machine*. Available at: <https://www.libertyhumanrights.org.uk/issue/policing-by-machine/>

explainability is an inadequate solution. Currently, police must put up signs warning the public of their use of facial recognition. However, this is not a sufficient marker of transparency, and there is significant risk of people being detained by police for trying to exercise their right to divert themselves away from the cameras. Moreover, it should not be left to the individual to notice (small) signs and take steps to avoid and protect themselves from oppressive state surveillance as they go about their everyday lives; this itself is a further violation of the right to free expression. The tech just should not be used.

16. Other important principles, notably absent from the Government's regulatory regime, include whether the laws and policies underlying an AI system are adequately prescribed by law, necessary, and a proportionate means of achieving a legitimate aim. A further primary consideration must be whether the use, collection or retention of data, or wider policy context behind the use of AI (for example, how and on whom the police decide to deploy technology), will result in unlawful discrimination, as well as exacerbate and entrench systemic oppression.
17. In summary, meaningful transparency and explainability would enable individuals to understand when decisions are made against them so that they can enforce their rights. Indeed, when it comes to public decision-making, the public has a legal right in most circumstances to understanding the reasons for a decision made by a public body implicating them and their rights, and to be able to advocate on that decision. Without true and full transparency and explainability this legal right (which facilitates the enforcement of further legal rights) would be made redundant. There is no reason why public decision-making through AI should or can be exempt from these ordinary legal principles.
18. It would be entirely possible for the Government to implement transparency and explainability, but this must be done in conjunction with a range of other, stringent requirements. There are numerous examples in other jurisdictions of more robust regulatory proposals, from those contained within Canada's Directive on ADM,¹⁶ France's Loi Pour Une République numérique,¹⁷ and the AI

¹⁶ Government of Canada, Directive on Automated Decision-Making, <https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592>

¹⁷ Government of the French Republic, Loi Pour Une République numérique, <https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000031589829/>

Regulatory Framework in the US.¹⁸ Similarly, the Council of Europe’s Draft Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law lists a range of fundamental principles of design, development and application of AI systems, including principles of equality and anti-discrimination, privacy and personal data protection, accountability, responsibility and legal liability, transparency and oversight, safety, safe innovation and public consultation. There are also specific measures and safeguards to ensure accountability and redress.¹⁹ Far from being a world-leading regime, the UK Government falls behind the proposals of its competitors. Making transparency compulsory would be one important and vital step in a longer journey towards strengthening the AI Governance system.

QUESTION 3: DO YOU AGREE THAT CURRENT ROUTES TO CONTESTABILITY OR REDRESS FOR AI-RELATED HARMS ARE ADEQUATE?

QUESTION 4: HOW COULD ROUTES TO CONTESTABILITY OR REDRESS FOR AI-RELATED HARMS BE IMPROVED, IF AT ALL?

19. Liberty is alert to this Government's attempts to stop people from holding power - in this case, opaque and unfair decision-making on the part of State bodies and private organisations - to account, alongside a wider agenda of making itself untouchable: from recently ditched proposals to scrap the Human Rights Act, to the introduction of undemocratic and unconstitutional protest restrictions rejected by Parliament.²⁰ It is within this environment of reduced rights that we must understand the proposed AI regulatory regime. As such, not only are current options for challenging the use of AI not adequate, they are also at risk of being undermined further, including by the Data Protection and Reform Bill.

20. Currently, ADM systems are subject to some specific regulation via the Data Protection Act 2018 (DPA) and UK GDPR. The DPA – though imperfect – provides

¹⁸ Federal Government of the United States, Blueprint for an AI Bill of Rights, <https://www.whitehouse.gov/ostp/ai-bill-of-rights/>

¹⁹ Council of Europe, Committee on Artificial Intelligence, Revised Zero Draft [framework] Convention on AI, Human Rights, Democracy and the Rule of Law, (6 January 2023). <https://rm.coe.int/cai-2023-01-revised-zero-draft-framework-convention-public/1680aa193f>

²⁰ The Guardian, *Suella Braverman faces legal action after forcing through anti-protest powers*, (14 June 2023). <https://www.theguardian.com/politics/2023/jun/14/home-secretary-suella-braverman-faces-legal-action-anti-protest-police-powers-liberty>

for a right not to be subject to solely ADM that produces an "adverse legal effect" on, or "significantly affects", the data subject - unless that decision is "required or authorised by law" (or other limited exceptions).²¹ Any such significant decision authorised by law must be "subject to safeguards for the data subject's rights, freedoms and legitimate interests", including: the right to be informed by the data controller that such a decision was made and the right, within one month, to request a reconsideration or a retaking of the decision "that is not based solely on automated processing". A further month is allotted for reconsideration or retaking and for the data subject to be informed of the outcome.²² The vast majority of the exemptions contained in the DPA, allowing data processors to set aside a person's data protection rights for broadly-defined purposes such as public protection and crime, do not apply to ADM.²³

21. The DPA thus allows for significant decisions to be made by sole ADM so long as authorised by law or accompanied by safeguards (in other words, sole ADM is permissible under wide-ranging conditions). During scrutiny of the DPA, Liberty recommended that Parliamentarians support an amendment that would have protected individuals from solely ADM engaging their rights under the Human Rights Act 1998. This would have been a significant, if bare minimum, safeguard; however, the amendment did not succeed.
22. Further, the DPA allows for significant decisions to be made by ADM without being authorised by law or accompanied by safeguards, so long as a human is in the loop (in other words, partial ADM is always permissible (subject to other provisions in the DPA and other laws)). Liberty has advocated for the protections under Article 22 UK GDPR to be extended more widely in order to refute the presumption that partial ADM poses less risks than sole automation by virtue of its human involvement. On the contrary, we believe similar risks arise from all forms of ADM and caution against putting too high a premium on human oversight as a robust safeguard. This is because of the risk of 'automation bias', whereby individuals are for various reasons liable to simply giving a 'rubber stamp' of approval to automated decisions, rather than considering the automated decision as one factor.

²¹ Data Protection Act 2018, Section 49, <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>

²² *Ibid.*, Section 14(5).

²³ Information Commissioner's Office, A Guide to the Data Protection Exemptions, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/a-guide-to-the-data-protection-exemptions/>

23. For example, in a situation where an individual police officer is required to make a decision as to whether to arrest a suspect, it is conceivable that they would defer to the ADM system and engage in an arrest for fear of going against what is purportedly 'better' intelligence (even if it may not be). In turn, "human users who are provided with advice by machines will often become increasingly reliant on and uncritical of this advice with time."²⁴ This is a very real threat: limited knowledge regarding AI among end users (in part because private manufacturers restrict information) coupled with time restraints and a lack of empowerment to meaningfully challenge ADM decisions, mean that what is meant to be a decision-assisting tool becomes a decision-making tool in practice. The narrow definition of solely ADM under the DPA also means that many ADM systems, including the facial recognition technology now being rolled out by the Metropolitan police, and to which the Policing Minister has expressed desire to roll out nationally,²⁵ may not be caught by the DPA because they include some human involvement. Liberty would encourage clarification and expansion of the meaning of sole ADM to extend to instances where there is human involvement, and would seek to dismantle the distinction between sole and partial ADM altogether.

24. The UK is undertaking its process of changing its data protection regime post-Brexit via the Data Protection and Digital Information (No.2) Bill (currently making its way through Parliament). This Bill provides another pertinent example of proposals recommended in the name of governance being a euphemism for reducing legal protections for individuals and their data. The Retained EU Law (Revocation and Reform) (REUL) Bill also further risks eroding essential data protection laws in the UK, by giving the Government broad powers to amend laws falling within the category of 'retained EU law' and allow currently unidentified swathes of these laws to disappear at the end of 2023 unless specifically 'saved' by a minister.²⁶ Up until very recently, the Government had plans to repeal and replace the Human Rights Act, which would undermine rights protections including individuals' data and privacy rights as well as their right to freedom of

²⁴ Centre for Data Ethics and Innovation, Landscape Summary: bias in algorithmic decision-making, (19 July 2019), p.18-19.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819055/Landscape_Summary_-_Bias_in_Algorithmic_Decision-Making.pdf

²⁵ Financial Times, *UK Policing Minister pushes for greater use of facial recognition*, (May 16 2023).

<https://www.ft.com/content/b8477e16-349d-442d-8e69-59b328ba9189>

²⁶ Public Law Project, Bill committee Briefing, Retained EU Law Bill, (November 2022).

<https://publiclawproject.org.uk/content/uploads/2022/11/Commons-Committee-stage-briefing-REUL-Bill-V2.0.pdf>

expression - essential safeguards that ensure that AI systems can be held to account and that would need to form the basis of any meaningful discussion on AI governance more broadly.

25. Not only do these changes and threats risk endangering human rights, they also risk threatening the data adequacy agreement that the UK currently maintains with the EU, which would have wide-ranging impacts, including on UK businesses.²⁷ This further calls into question the practical feasibility and effectiveness of the Government's so-called 'pro-innovation' approach.
26. Notwithstanding our concerns about the UK GDPR, legislation around automated decision-making which governs when decisions about people can be made using algorithms and AI, and what rights those people then have to object, ask for human review, or seek redress (Article 22) does provide a stronger floor of protection than the proposals made to change it in the Data Protection and Digital Information Bill. While the Bill hasn't removed controls over automated decision-making altogether, we have significant concerns about the ways in which Article 22 is rewritten to “flip the original regulation in Article 22 on its head: instead of automated decision-making being prohibited except for when it's safe, it's now allowed except for under what are judged to be risky circumstances.”²⁸
27. Numerous human rights groups have sounded the alarm bell for other critical reasons. For example Open Rights Group have argued that the Bill will “introduce new barriers to exercise data protection rights, lower protections around AI and automated decision-making, lessen rights against online manipulation and discrimination, and create new obstacles to lodging a complaint.” They also identify how the Bill will diminish the UK international reputation by lowering safety standards. This, coupled with the lowering of AI standards will make “the UK a safe haven where unethical tech companies and data marketers can avoid legal liability and circumvent regulatory standards. Companies will move to the

²⁷ The Information Commissioner's Response to the Ministry of Justice Consultation on Human Rights Act Reform. <https://ico.org.uk/media/about-the-ico/consultation-responses/4020181/ico-response-to-moj-human-rights-act-reform-consultation.pdf>

²⁸ Connected by Data, What should change in the Data Protection and Digital Information Bill, (Sept 29 2022). <https://connectedbydata.org/events/2022-09-29-data-protection-digital-information-bill-civil-society-event>

UK to move fast and break things, leaving UK residents with the burden of picking up the broken pieces.”²⁹

28. Current routes to contestability or redress for AI-related harms are therefore not adequate, and are at risk of deteriorating further. As a first step, the Government must cease its plans to weaken ADM protections in the Data Protection and Digital Information Bill, and safeguard data protection rights more widely. The Government should also look to implementing robust accountability practices. For example, the Treasury Board of Canada has implemented a mandatory tool that assesses the risk level of an ADM system. The tool assesses the risk level of an ADM system, including consideration of the capabilities of the systems design; transparency of the algorithm; classifications of the automated decision; the impact the automated decision has on freedom, health, economy or environment; and the data source and type. The Canadian Civil Liberties Association has also called for compliance with tests and evaluations, and an enforcement regime that includes consequences for non-compliance.³⁰

29. Other examples of accountability mechanisms include giving people subject to ADM a right to explanation, the right to object to ADM and to be free from such decision-making, and the right to request human intervention.

QUESTION 5: DO YOU AGREE THAT, WHEN IMPLEMENTED EFFECTIVELY, THE REVISED CROSS-SECTORAL PRINCIPLES WILL COVER THE RISKS POSED BY AI TECHNOLOGIES?

QUESTION 6: WHAT, IF ANYTHING, IS MISSING FROM THE REVISED PRINCIPLES?

30. Liberty does not believe that the revised cross-sectoral principles, even when implemented effectively, will cover the risks posed by AI technologies. While a principles-based approach and guidance are preferable to the current situation,

²⁹ Open Rights Group, Written evidence submitted to the Data Protection and Digital Information (No.2) Bill. <https://publications.parliament.uk/pa/cm5803/cmpublic/DataProtectionDigitalInformation/memo/DPDIB06.htm>

³⁰ Canadian Civil Liberties Association, Submission to Ontario’s Trustworthy AI Framework 201.

they are inadequate for the reasons already described and particularly without the force of law behind them.

31. Additionally, the consultation does not address the full range of risks posed by AI technologies. The rapid advances in the field of artificial intelligence and machine learning represent a huge shift in the relationship between the individual and the state. For example, the prevalence of data collection that is required to enable ADM systems to work has ushered in widespread surveillance technologies, whose purpose is to lay bare the intimate details of people's everyday lives. Since algorithmic models are based on data, the content of that data - and the way it is collected and processed - is significant.
32. The Government's proposed 'fairness' principle, while important, fails to acknowledge the nuances of the oppression that AI can wield, and the Government also explicitly leaves the question of fairness to regulators to interpret.³¹ As succinctly put by EDRI, "it is possible to have harmful systems that give fair outputs." To illustrate this, EDRI give the example of AI systems that distribute harmful jobs, or allocate subprime credits; two examples of things that primarily target people from financially and otherwise vulnerable populations, mostly people of colour. They state that parity in such systems of exploitation neither makes sense nor is desirable.³²
33. At Liberty, we would advocate for a deep consideration of AI's potential oppressive impact. For instance, AI can have discrimination built into it, with the risk that marginalised communities are subject to discrimination via the dual threat of being both under and overrepresented.
34. As an example of marginalised communities being underrepresented, a range of studies have revealed the biases inherent in facial recognition technology due to the reliance of training data on white, straight, non-disabled, cis- gender men.³³ Less explored, however, are the risks to marginalised communities of being overrepresented in data. Wealth and social privilege shield certain populations, for example, those who opt for private healthcare or who do not access benefits,

³¹ A Pro-Innovation Approach to AI, p.29.

³² European Digital Rights, Beyond Debiasing, P.127. https://edri.org/wp-content/uploads/2021/09/EDRI_Beyond-Debiasing-Report_Online.pdf

³³ Buolamwini et al, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, (2018).

from tools of societal control and surveillance. As Virginia Eubanks details when speaking of the "invisible spider web" of ADM, "many of us in the professional middle class only brush against it briefly, up where the holes in the web are wider and fewer of the strands are activated. We may have to pause a moment to extricate ourselves from its gummy grasp, but its impacts don't linger."³⁴ In contrast, poverty and race, through proxy indicators such as access to public services and residential postcodes (or in some cases, even names),³⁵ attract over-policing and hyper-surveillance, which then proceeds to feed the data mined by the algorithm to produce the desired outputs. For example, an ADM system used to flag a child in need of protective services in the US, was based on data gathered from public service providers (such as public drug support services), rather than private data (such as private rehabilitation centres).³⁶

35. Just this month, the Guardian reported that several food banks in London have been asking users to submit face scans to allow them to choose food from shops via a new app-based voucher system. The system also has the potential to track purchases. In order to opt out, food bank users would have to choose to take a convention food bank parcel instead.³⁷ In other words, the more you interact with the State, the more data points are likely to exist about you that are accessible by public bodies, and the greater the State's ability becomes to track you across society and use your data to build punitive AI systems which in turn re-target you and your communities.

36. Another important set of considerations are the structurally oppressive impacts of AI, the entrenchment and mechanisation of oppression, and the application of AI in oppressive ways. For example the police's deployment of new technologies that seek to analyse and predict crime outcomes and identify and profile people has a seismic impact on the way laws are being and will continue to be enforced, and policing powers are exercised, magnifying existing inequalities and oppression. A prime example is the Gangs Matrix, a Metropolitan Police Service database containing personal information of people perceived to be in a gang or likely to commit violence. In 2018 the Information Commissioner published an

³⁴ Virginia Eubanks, *Automated Inequality: how high-tech tools profile, punish and police the poor* (2018).

³⁵ Big Brother Watch, *Police use Experian Marketing Data for AI Custody Decisions*, (6 April 2018).
<https://bigbrotherwatch.org.uk/2018/04/police-use-experian-marketing-data-for-ai-custody-decisions/>

³⁶ Eubanks, *Automated Inequality*.

³⁷ The Guardian, *Campaigners urge London food banks to end use of face scans*, (13 June 2023).
<https://www.theguardian.com/society/2023/jun/13/campaigners-urge-london-food-banks-to-end-use-of-face-scans>

enforcement notice which ruled that it had been consistently breaching data protection laws since its creation.³⁸ Research found that 15% of people on the Matrix were children (some as young as 12) and 78% were Black males.³⁹ Reasons for being placed on the Matrix were opaque and could result in criminalisation and difficulties accessing public services - children and young people on the Matrix faced the risk of over-policing, school exclusion, eviction, and in some cases being stripped of welfare benefits, being taken into care, or even deportation. Following a legal challenge focusing on the racial disproportionality of the database, the MPS was forced to concede that their operation of the Matrix was unlawful. It has now finally agreed to radically overhaul the database and to remove more than a thousand names from it.⁴⁰

37. In addition to the implications that come from privacy, data protection and human rights perspectives, there arises the larger issue surrounding the lack of democratic engagement with whether we should, as a society, have these technologies in the first place. In turn, the question must be asked of whether the public can have such a discussion, if they are not well-informed, and the Government is not proactively engaging them in this debate. By questioning whether technologies can be used correctly and reliably within a regime of regulation and oversight, we have already foreclosed – without democratic input – the wider question of whether these technologies should be used at all. The EU, in its recently passed AI Act, has demonstrated that it is possible to draw boundaries around legitimate and non-legitimate uses of AI, and mandate strict safeguards for permissible AI, through democratic participation. The UK Government has failed to explain why it has rejected this approach. It appears the Government's attempts to erode accountability mechanisms in public life extends to avoiding democratic debate in favour of business and tech solutionism.

38. While there should be bare minimum and stringent safeguards to ensure accountability and transparency, there will also be various cases where AI should

³⁸ ICO Enforcement Notice, <https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/about-us/gangs-violence-matrix/ico-enforcement-notice.pdf>

³⁹ Amnesty International, Trapped in the Matrix: secrecy, stigma, and bias in the Met's Gang's Database (2018). <https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/about-us/gangs-violence-matrix/ico-enforcement-notice.pdf>

⁴⁰ Liberty, 'Met to overhaul 'racist' gangs matrix after landmark legal challenge (11 November 2022). <https://www.libertyhumanrights.org.uk/issue/met-to-overhaul-racist-gangs-matrix-after-landmark-legal-challenge/>

be banned entirely. Areas of high concern include any AI system that engages the freedoms and protections in the Human Right Act, ADM systems which involve the use of data which flow from oppressive practices in the first place (such as racist policing), and AI use by public bodies, especially in the context of welfare, and the criminal justice system, such as facial recognition technology and predictive policing. The EU AI Act has proposed a full ban on real-time remote biometric identification in public spaces and most uses of post or retroactive biometric identification, and a ban on emotion recognition in law enforcement, border management, workplaces, and education. The Act would also ban or set significant restrictions on discriminatory biometric categorisation, predictive policing, social scoring, risk assessments in certain contexts, and the mass scraping of biometric data to create surveillance databases.

39. In summary, Liberty does not believe that regulation can fix the harms of some AI systems, and the Government must commit to banning certain forms of AI. Without doing so, the UK will be on a collision course with the EU, who commentators have claimed is “fast becoming the de facto global leader on tech regulation.”⁴¹ It is also important to recognise the particular social, political and historical context that AI systems operate in; it is in these contexts in which potential human rights violations occur.

A STATUTORY DUTY TO REGARD

QUESTION 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?

QUESTION 8: IS THERE ANY ALTERNATIVE STATUTORY INTERVENTION THAT WOULD BE MORE EFFECTIVE?

⁴¹ The Washington Post, *Europe moves ahead on AI regulation, challenging tech giants’ power*, (June 14 2023). <https://www.washingtonpost.com/technology/2023/06/14/eu-parliament-approves-ai-act/>

40. It is Liberty's view that strengthening the weight of the Government's proposed regulatory regime is necessary and any such proposals must be carefully considered and widely consulted on with a range of stakeholders, especially with regulators themselves, as well as civil society who regularly act in the interests of the public to hold public bodies to account. Introducing a statutory duty on regulators to have due regard to the principle is a possible way to clarify and strengthen regulators' mandates to implement the principles, but this should still be seen as a bare minimum safeguard, for the reasons already identified.
41. As an organisation that regularly utilises another type of statutory duty (the Public Sector Equality Duty, (PSED)) to initiate legal challenges, we support its use as a tool to identify and challenge oppressive policies and practices – and in theory at least, for public bodies to consider discrimination and thus the appropriateness of policies and practices at an early stage. However, we caution seeing statutory due regard duties as a magic bullet. For starters, if the duty will be for regulators to have due regard to the AI governance principles, it relies on the principles themselves being robust. As we have outlined above, the content of the Government's proposed principles contain significant gaps, and lack the right mechanisms to make them meaningful in practice.
42. Furthermore, the Criminal Justice Alliance has undertaken extensive research into the strength of the PSED within the Equality Act. Their research identifies that the Home Office, the Ministry of Justice and other public bodies (such as individual police forces, HM Prison and Probation Service (HMPPS) and Police and Crime Commissioners) are "often failing to adhere to fully to the PSED." This is despite the fact that the due regard duties in the Equality Act already have a low threshold. For example, Equality Impact Assessments (EIAs) (which are not a legal requirement) are one simple way for public bodies to show how they have met their legal duties under the PSED. And yet, "EIAs are often produced internally without involving external stakeholders and those directly impacted by the proposed policies; can lack evidence and effective analysis of the data available; and fail to consider intersectionality where any adverse impacts can be compounded due to a person's race, age, gender, religion or belief, or other multiple protected characteristics." Furthermore, they argue that "too often EIAs do not set out well-developed mitigation to effectively counteract any indirect discrimination that has been identified. EIAs also tend to be published after policy decisions have been made, if published at all. This results in organisations

needing to request EIAs through submitting Freedom of Information (Fol) requests or by beginning legal action.”⁴²

43. It is also revealing that the Government is proposing regulators carry the weight of the AI governance regime, while there is no promise of them receiving additional resources. As the Government itself recognises, current regulators may lack appropriate expertise in AI and thus may not effectively provide the necessary checks in order to uphold the regulatory regime effectively.⁴³
44. Regulators are already overstretched. For example, we often experience delays with investigations led by the Information Commissioner Office long, and in our experience these timeframes are only getting longer. As one of the oldest human rights and civil liberties organisations in the country, with paid staff and resources to carry out this type of work, we are concerned what the everyday person – particularly victims of AI harms – without such support would not have the capacity, resilience or experience to withstand such challenges; nor should they have to.
45. Meanwhile, the Government has plans to reduce the specialism within one of the main regulators we foresee shouldering much of the weight of regulating AI (the ICO). Regulator specialism is not something to be taken for granted, and the success of a regulatory regime rests upon the fact that they a regulator such as the ICO can focus on the important issue of data protection sufficiently. But this does not mean that they will be able to apply other substantial principles well; indeed, lots of different regulators (from the Food Standards Agency, to the General Dentist Council) applying optional principles to different extents will cause difficulties with establishing clear, coherent standards and best practice. This in and of itself would undermine the Government’s own agenda of providing clarity for business.
46. Meanwhile, proposals in the Data Protection and Digital Information Bill would merge the Biometrics and Surveillance Camera (BSC) Commissioner with the ICO. It is worth remembering that this role was already borne from two separate roles (the Biometrics Commissioner, and Surveillance Camera Commissioner

⁴² The Criminal Justice Alliance, The Tackling Racial Inequality Project. Empowering Civil Society: using the Public Sector Equality Duty to tackle race disparity in the criminal justice system.

https://www.criminaljusticealliance.org/wp-content/uploads/Tackling-Racial-Inequality_Introduction.pdf

⁴³ A Pro-Innovation Approach to AI, p.62.

respectively). Speaking out against this proposal in his submission to the Bill Committee, the BSC Commissioner wrote that,

The Bill proposes the erasure of many such functions and, by extension, their associated value to society. As one expert interviewee for the report expressed, having been based on a consultation about ‘absorption’ of the functions by the Information Commissioner “the Bill makes no provision for absorption whatsoever. It just deals with extinction”⁴⁴

47. Other concerning proposals include empowering the Secretary of State (SoS) to introduce a Statement of Strategic Priorities to which the Commissioner must have regard, and require the regulator to respond in writing as to how it will address them. It would also require the ICO to submit Codes of Practice to the prior approval of the SoS before they can be laid before Parliament. This in effect would politicise the ICO – allowing the SoS to interfere with how it functions, and give her new powers to provide instructions to the Commissioner – when it is vital that it remains independent from Government.

MONITORING AND EVALUATION OF THE FRAMEWORK

QUESTION 15: DO YOU AGREE WITH OUR OVERALL APPROACH TO MONITORING AND EVALUATION?

48. Liberty does not agree with the Government’s overall approach to monitoring and evaluation. This is because of the central focus underpinning the framework, to which the Government will measure and evaluate the success of AI Governance. They state, “Government has a responsibility to make sure the regulatory framework *operates proportionately and supports innovation*” (emphasis added).⁴⁵ In other words, the basis for which success will be measured is whether and how far the regime boosts the economy, and how far and whether regulatory burdens are proportionate to that wider aim.

⁴⁴ Biometrics and Surveillance Camera Commissioner Submission and Interim Report by Professor Pete Fussey and Professor William Webster. <https://bills.parliament.uk/publications/51173/documents/3425>

⁴⁵ A Pro-Innovation Approach to AI, p.42.

49. Regulation should be about mitigating harm, not simply boosting the economy, and evaluating by the principles of pro-innovation miss the crucial impact on human rights. It has been well documented that industry sees innovation as being in conflict with regulation, and they have historically protested legally mandated regulatory standards and enforcement mechanisms for this reason. Indeed, the Government admits that “industry has strongly supported non-statutory measures in the first instance, favouring flexibility and fewer burdens...”⁴⁶

50. As aptly identified by AI governance scholars:

*These protests assume that innovation is an unvarnished and unmitigated good, an unexamined belief that has resulted in technological innovation (particularly in the digital services industry) entrenching itself as the altar upon which cash-strapped contemporary governments worship, naively hoping that digital innovation will create jobs, stimulate economic growth and thereby fill diminishing governmental coffers left bare after propping up the banking sector which teetered on the brink of collapse following the global financial crisis in 2008.*⁴⁷

51. We understand the desire to stimulate the economy, provide people with much-needed jobs, and ensure that public services can run effectively and efficiently, and we do not believe that AI can't play a role in doing so. Indeed, AI has great potential, from organisations using AI to aid the Just Transition and hence securing workers' rights and livelihoods, as well as combatting climate change. Yet we caution the tech industry's support for, and the Government's reliance on vague and elastic principles, “effectively plucked out of the air, without any grounding in a specific vision of the character and kind of political community that is committed to establishing and maintaining, and which those principles are intended to secure and protect.”⁴⁸

52. Noticeably, the White Paper makes some reference to ‘AI ethics’. While we do not have scope to go into detail about the distinctions between ethics and human rights frameworks, it is important to put into context what critics have described

⁴⁶ A Pro-Innovation Approach to AI, p.36.

⁴⁷ Karen Yeung, et al., AI Governance by Human Rights-Centred Design, Deliberation and Oversight: an end to ethics washing, (9 August 2019). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3435011

⁴⁸ Yeung, AI Governance.

as a “move of genius” by the tech industry,⁴⁹ “to focus attention and resources on the ethics of AI to delay the debate and work on the *law* for AI.”⁵⁰ Indeed, amidst increasingly public debates, especially by the tech industry, about the threat of AI – from fears AI will become sentient,⁵¹ to its potential to “wipe out humanity”,⁵² a fear perpetuated by the Prime Minister Rishi Sunak’s own AI advisor Matt Clifford⁵³ – we must take heed of the reality that AI is having harmful impacts already. Far from being a *future* threat, AI’s human rights impacts are felt by communities across the country: from the Home Office’s automated ‘triage’ tool used to decide whether couples planning to get marriage should be subject to a ‘sham marriage’ investigation entrenching racism;⁵⁴ to Councils wrongly targeting welfare claimants on suspicion of committing fraud.⁵⁵

53. Though human rights frameworks provide far more robust alternatives, we have instead noticed a concerted effort by the Government to downgrade human rights from its AI Governance (and, indeed, wider policy) agenda. For example, in the National AI Strategy, published before the AI White Paper, the Government originally stated that their approach would “facilitate innovation” while at the same time ensure the regulatory regime “[protects] people and our fundamental values.”⁵⁶ Liberty and others criticised the coupling of innovation with human rights as well as the Government’s suggestion that human rights, democratic principles, and the rule of law was relevant only to shaping international, and not UK frameworks.⁵⁷ But rather than respond to such feedback by embedding

⁴⁹ Paul Nemitz, Constitutional Democracy and Technology in the Age of Artificial Intelligence (14 August 2018), <https://royalsocietypublishing.org/doi/pdf/10.1098/rsta.2018.0089>

⁵⁰ Yeung, AI Governance.

⁵¹ The Guardian, *‘I am, in fact, a person’: can artificial intelligence ever be sentient?* (14 August 2022). <https://www.theguardian.com/technology/2022/aug/14/can-artificial-intelligence-ever-be-sentient-googles-new-ai-program-is-raising-questions>

⁵² The New York Times, *‘The Godfather of AI’ quits Google and Warns of Danger Ahead*, (4 May 2023). <https://www.nytimes.com/2023/05/01/technology/ai-google-chatbot-engineer-quits-hinton.html>

⁵³ Sky News, *AI could help produce deadly weapons that ‘kill humans’ in two years’ time, Rishi Sunak’s advisor warns*, (6 June 2023). <https://news.sky.com/story/ai-could-help-produce-deadly-weapons-that-kill-humans-in-two-years-time-rishi-sunaks-adviser-warns-12897366>

⁵⁴ Public Law Project, Legal action launched over sham marriage screening algorithm, (17 February 2023), <https://publiclawproject.org.uk/latest/legal-action-launched-over-sham-marriage-screening-algorithm/>

⁵⁵ Rowland Mathorpe, Sky News, Thousands Face Incorrect Benefit Cuts from Automated Fraud Detector (1 March 2019), <https://news.sky.com/story/thousands-face-incorrect-benefit-cuts-from-automated-fraud-detector-11651031>

⁵⁶ National AI Strategy, (September 2021).

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1020402/National_AI_Strategy_-_PDF_version.pdf

⁵⁷ Liberty’s response to the Science and Technology Committee’s call for evidence into governance of artificial intelligence, (September 2022). <https://www.libertyhumanrights.org.uk/wp->

human rights within the framework, the Government explicitly respond by taking human rights out, explaining that human rights are “not explicitly named in the revised principles as we expect regulators to adhere to existing law when implementing [them].”⁵⁸

54. Rather than strengthen the principles further in line with human rights, it is concerning that human rights have been dropped from the regulatory priorities altogether with the AI White Paper instead proposing the most light touch regulatory option. This is despite the Government considering a strengthened regulatory regime in the impact assessment released alongside the AI White Paper.⁵⁹ As such, we are worried about the harm and errors that will continue to occur in the gaps between regulation.

55. Finally, we are not convinced by the Government’s promise that it will put the duty on a statutory basis if the framework is not having its expected aim. Given that innovation is the central measure of success for the regulatory regime, it means that other important pressing reasons, such as the failure for regulators to hold AI systems properly account may not trigger the Government to take further action, even though that clearly would present an urgent reason to do so.

LEGAL RESPONSIBILITY FOR AI

QUESTION L.1: 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?

QUESTION L.2.i: DO YOU AGREE THAT THE IMPLEMENTATION OF OUR PRINCIPLES THROUGH EXISTING LEGAL FRAMEWORKS WILL FULLY AND

[content/uploads/2021/11/Libertys-response-to-the-Science-and-Tech-Committees-Call-for-Evidence-into-Governance-of-Artificial-Intelligence.-November-2022.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/114704/content/uploads/2021/11/Libertys-response-to-the-Science-and-Tech-Committees-Call-for-Evidence-into-Governance-of-Artificial-Intelligence.-November-2022.pdf)

⁵⁸ A Pro-Innovation Approach to AI, p.79.

⁵⁹ UK Artificial Intelligence Regulation Impact Assessment.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/114704/5/uk_ai_regulation_impact_assessment.pdf

EFFECTIVELY ALLOCATE LEGAL RESPONSIBILITY FOR AI ACROSS THE LIFE CYCLE?

56. As we have already acknowledged, we anticipate regulators struggling to apply the principles within a context of stripped back resources, capacity and expertise. Indeed, in the AI White Paper, the Government admits regulators have “expressed concerns that they lack the statutory basis to consider the application of the principles.”⁶⁰ As a result, we are concerned that human rights will fall through the gaps.

57. The use of technologies in the justice system provides an illustrative example of the challenges that will arise from the use of different regulators and their application of the principles across different AI applications and systems. While only making up one part of many possible uses of AI (welfare provision and public health are other significant examples), there is no consolidated or clear framework in this area. Governance of technologies in the justice system sits across the Human Rights Act 1998 (HRA), DPA, EA, public administration, police common law powers to ‘prevent and detect crime,’ the Protection of Freedoms Act 2012, law enforcement bodies’ own published policies, a raft of guidance, regulation and other guidelines, and has over 30 public bodies, initiatives, and programmes playing a governance function.⁶¹ There is complexity, lack of cohesion and confusion around who and what play key roles in oversight, responsibility and accountability. The Government’s hands-off approach to AI governance as promulgated in its White Paper only compounds this confusion, and thus the likely harms that will result from intrusive use of AI.

58. When the House of Lords Select Committee on Justice and Home Affairs sought to find a neat and coordinated ‘family tree’ of the organisations involved in the governance of new technologies for the application of the law, Professor Paul Taylor, National Policing Chief Scientific Advisor, told them that “it may be more of a family bush.”⁶² The fact that a high-level policing advisor attests to the level of confusion and disorientation of this field speaks volumes. As explained by one respondent to the Committee’s call for evidence, this is nothing short of a ‘public

⁶⁰ A Pro-Innovation Approach to AI, p.36.

⁶¹ House of Lords Justice and Home Affairs Committee, Technology Rules? The Advent of New Technologies in the Justice System. <https://publications.parliament.uk/pa/ld5802/ldselect/ljjusthom/180/180.pdf>

⁶² Technology Rules? P.21.

failure’ which could “lead to not just operational defects or inefficiencies, but miscarriages of justice,” which, without “accountability for errors and misuse [...] may leave people open to dangers for which no person can be identified as responsible.”⁶³

59. In the policing and criminal justice context, the miscarriages of justice arising from errors are obvious, ranging from wrongful imprisonment to police monitoring, surveillance and harassment. But it is worth noting the life-changing consequences that can also happen in other, seemingly more innocuous circumstances – as in the decision by the Office of Qualifications and Examinations Regulation (Ofqual) to use an algorithm to determine pupils’ final grades, which had severe consequences for pupils across the country, and a disproportionate impact on the most marginalised students.
60. Considering this fragmented framework, and the organisational confusion on the part of public bodies about what framework applies in their use of AI, we are disappointed by the Government’s missed opportunity to utilise the AI White Paper to address governance concerns substantively. When the Home Affairs and Justice Committee previously raised their doubts, the Government suggested that issues could be clarified by the courts, an approach made much harder by the passage of the Judicial Review and Courts Act 2022, and constant Government criticism of the ‘overreach’ of the Courts.⁶⁴
61. There are significant dangers to an approach which relies on the Courts to set governance standards, and we are already starting from the wrong footing if the assumption is that something is lawful, until it is proven otherwise by legal challenge. This is at complete odds with the rule of law: it is the role of Government, with Parliamentary scrutiny, to determine governance, set standards, and empower public bodies to comply with them. While the Courts can hold back the tide on particular instances of use, it is difficult to bring legal challenges, not to mention the difficulties of finding a client, attaining funding in an environment of cuts to legal aid, limitations on what arguments may be run, and wider Government plans to limit Judicial Review.

⁶³ Technology Rules? P.14.

⁶⁴ Prospect, *The Government wanted to reign in the Supreme Court. Now it may not need to*, (October 16 2021). <https://www.prospectmagazine.co.uk/politics/38065/the-government-wanted-to-rein-in-the-supreme-court.-now-it-may-not-need-to>

62. In Liberty’s experience, even after a successful legal challenge (such as after the Court of Appeals *Bridges* judgment which ruled South Wales Police’s use of live facial recognition technology unlawful and breached privacy rights, data protection and equality laws), there is no guarantee that public bodies will change their approach.⁶⁵ Liberty is aware that South Wales Police still use the tech, and there have been other operational deployments by other police forces.⁶⁶ Meanwhile, police have been scoping and have procured other facial recognition technologies, including retrospective, facial recognition watches, and mobile phone/hand-held facial recognition devices.

63. With current laws not sufficient, and the principles within the Government’s proposed regulatory approach not either, we fear that combined they will constitute a recipe for disaster.

CONCLUSION

64. Current legal frameworks governing Artificial Intelligence are not fit for purpose, and are failing to keep pace with the rise in use across different sectors and contexts. Unfortunately, the proposals provided within the Government’s AI White Paper fail to provide even a mere floor of protection and developments in other contexts – such as the UK GDPR, Data Protection Act, and Data Protection and Digital Information Bill – risks sully any potential progress.

65. In order to safeguard against AI harms, human rights and anti-oppression must be embedded throughout an AI governance framework, including being considered at the design, development and implementation of an AI system. It would be possible to do so with high-level, more expansive principles, backed up by context specific legislation which deals with the potential harms of AI, and clear bans on particular uses. Liberty would also consider supporting a legally mandated regulatory regime buttressed by independent and properly resourced regulatory authorities, with appropriate powers of investigation and enforcement.

⁶⁵ Liberty, Legal challenge: *Ed Bridges v South Wales Police*.

<https://www.libertyhumanrights.org.uk/issue/legal-challenge-ed-bridges-v-south-wales-police/>

⁶⁶ Big Brother Watch, Biometric Britain: the expansion of facial recognition surveillance, (May 2023).

<https://bigbrotherwatch.org.uk/wp-content/uploads/2023/05/Biometric-Britain.pdf>

66. We do not believe that a human rights-based approach need stifle innovation – indeed, scholars have provided ample evidence of legal regulation fostering it: from the introduction of mandatory environmental laws imposing limits on emissions was an important catalyst in the emergence and development of a competitive market for emission reduction technologies.⁶⁷

67. While the Prime Minister has shown new interest in AI since the White Paper was published, and expressed intention for Britain to become the “potential home of a global regulator,” it is urgent that the Government rethink its current approach, and develop a proposal that puts human rights at its centre.⁶⁸

⁶⁷ Karen Yeung, et al., AI Governnace by Human Rights-Centred Design, Deliberation and Oversight: an end to ethics washing, (9 August 2019), p.25. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3435011

⁶⁸ Time Magazine, *Sunak wants the UK to be a key player in global AI regulation*, (June 14 2023). <https://time.com/6287253/uk-rishi-sunak-ai-regulation/>