LIBERTY

LIBERTY'S RESPONSE TO THE DEPARTMENT OF DIGITAL, CULTURE, MEDIA AND SPORT'S CONSULTATION *DATA: A NEW DIRECTION*

NOVEMBER 2021

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 https://www.libertyhumanrights.org.uk/policy.

CONTACT

SAM GRANT
Head of Policy and Campaigns
samg@libertyhumanrights.org.uk

JUN PANG
Policy and Campaigns Officer
junp@libertyhumanrights.org.uk

KATY WATTS
Lawyer
katyw@libertyhumanrights.org.uk

EMMANUELLE ANDREWS
Policy and Campaigns Officer
emmanuellea@libertyhumanrights.org.uk

MEGAN GOULDING
Lawyer
megang@libertyhumanrights.org.uk

CONTENTS

INTRODUCTION

Liberty welcomes the opportunity to respond to the Department for Digital, Culture, Media, and Sport's (DCMS) consultation into *Data: A new direction,* which follows on from its National Data Strategy. We confine our comments to questions under Chapters 1, 2, 4, and 5.

We are highly concerned by the Government's agenda to weaken data protection and privacy rights. Not only are these fundamental rights protected by Article 8 of the European Convention on Human Rights (ECHR) (incorporated in the UK by the Human Rights Act (HRA)), they are also deeply interconnected with, and essential tools for enforcing, a host of other rights, not least our rights to freedom of expression and freedom of assembly and association. Crucially, data protection and privacy rights can be one of the most important – and in some cases, the only – way that people can stand up to untransparent and unfair decision-making by public and private bodies, because they are sometimes the only way to find out if one has even been subjected to such a decision. Data protection and privacy rights have enabled individuals to challenge the unfair withholding of benefits,[1] discriminatory policing and targeting,[2] expansive and intrusive surveillance,[3] racist immigration visa-streaming algorithms,[4] and wage theft in the context of precarious 'gig' economy employment[5] - and much, much more. Given the increasing use of technology in the application of the law,[6] our 'Big Data' society, and the increasing prevalence of algorithmic decision-making (ADM) (especially during the coronavirus pandemic)[7] these rights will only become more important – which makes the Government's attempts to erode them all the more staggering.

Within the wider context, Liberty views these proposals as part of a wider scheme of Government measures to erode accountability and transparency mechanisms and institutions, from the Elections Bill (which threatens to lock many communities out of the ballot box), to the Judicial Review and Courts Bill (which will close off avenues for challenging unfair decision-making), to the Police, Crime, Sentencing and Courts Bill (which will erode

[1] Human Rights Watch, *Automated hardship: How the Tech-Driven Overhaul of the UK's Social Security System Worsens Poverty,* 29 September 2020, available at: https://www.hrw.org/report/2020/09/29/automated-hardship/how-tech-driven-overhaul-uks-social-security-system-worsens
[2] Information Commissioner's Office, *ICO finds Metropolitan Police Service's Gangs Matrix breached data protection laws,* 16 November 2018, available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/ico-finds-metropolitan-police-service-s-gangs-matrix-breached-data-protection-laws/
[3] Liberty, *Legal challenge: Ed Bridges v South Wales Police,* available at: https://www.libertyhumanrights.org.uk/issue/legal-challenge-ed-bridges-v-south-wales-police/
[4] Foxglove, *Home Office says it will abandon its racist visa algorithm – after we sued them,* 4 August 2020, available at: https://www.foxglove.org.uk/2020/08/04/home-office-says-it-will-abandon-its-racist-visa-algorithm-after-we-sued-them/
[5] The App Drivers and Couriers Union, *Gig economy workers score historic digital rights victory against Uber and Ola Cabs*, available at: https://www.adcu.org.uk/news-posts/gig-economy-workers-score-historic-digital-rights-victory-against-uber-and-ola-cabs
[6] The Justice and Home Affairs Committee has recently launched an inquiry into the use of new technologies in law enforcement. See: https://committees.parliament.uk/work/1272/new-technologies-and-the-application-of-the-law/
[7] Algorithm Watch, *ADM Systems in the COVID-19 Pandemic: A European Perspective*, October 2020, available at: https://algorithmwatch.org/en/automating-society-2020-covid19/

our right to protest and other human rights), to the Nationality and Borders Bill (which will fundamentally alter the institution of asylum and greatly restrict migrants' rights). In our view, the Government's plans in *Data: A new direction* should be understood as another way it is trying to stop people from standing up to power, namely to untransparent and unfair decision-making on the part of State bodies and private organisations.

We note that the highly technical and impenetrable nature of the consultation document may have prevented many stakeholders from effectively participating, which is particularly concerning given the significant implications and equalities impacts that these proposals are likely to have. The leading nature and framing of some of the questions and proposals further suggests that at least some of the results of the consultation may be predetermined, which is contrary to the purpose of such an exercise.

CHAPTER 1: REDUCING BARRIERS TO RESPONSIBLE INNOVATION

Building trustworthy AI systems

Q.1.5.10

To what extent do you agree with the proposal to make it explicit that the processing of personal data for the purpose of bias monitoring, detection and correction in relation to AI systems should be part of a limited, exhaustive list of legitimate interests that organisations can use personal data for without applying the balancing test? Please explain your answer, and provide supporting evidence where possible, including on: The key benefits or risks you envisage; What you envisage the parameters of the processing activity should be.

1. **Liberty strongly disagrees with this proposal**. We are concerned that the creation of situations in which a data controller's legitimate interests, in this case for the purpose of bias monitoring, detection and correction in relation to AI systems, will always automatically prevail may expose data subjects to violations of their rights. While we have not answered these questions directly, our response is also relevant to questions Q.1.4.1 to Q.1.4.4.

2. Currently, under Article 6(1)(f) of the EU General Data Protection Regulation 2016, which is retained in domestic law as the UK GDPR, processing shall be lawful if it is "necessary for the purposes of the legitimate interests pursued by the controller or by a third party, *except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child* (emphasis added)." When relying on legitimate interests as a lawful ground, the UK GDPR requires organisations to show that the processing is necessary and to document how their interests outweigh the rights of data subjects. This is the balancing test. In terms of the rationale for this proposal, the consultation document states, "[a]ssessing whether the organisation's interests outweigh the rights of individuals *appears to cause the most uncertainty* for data controllers."[8] DCMS' solution to this problem is to establish a list of legitimate interests that organisations can use personal data for without applying the balancing test.

3. We believe that it is important to retain the balancing test in Article 6(1)(f) GDPR for the processing of personal data for bias monitoring, detection, and correction. Even if activities of bias monitoring, detection and correction appear to be in the public interest, they may still interfere with the rights of the data subject. Retaining the balancing test enables for these issues to be considered in the round so as to mitigate any harmful effects. We note that this proposal may effectively enable data controllers (such as private businesses) to justify a widened range of processing

[8] Pg. 22, *Data: A new direction.*

under the banner of 'bias monitoring, detection and correction' – in service of other objectives (such as profit-making), removing the important safeguard of the need to consider individuals' data rights. Even if the objective of such data controllers is genuinely to mitigate bias, our view (as explained below) is that it is likely not possible to wholly mitigate bias in a given system, and more importantly, attempts to address bias are not necessarily adequate or sufficient in cases where technologies are inherently rights-violative. On this basis, creating an exemption for the balancing test for organisations in order to address bias may compound these underlying issues.

4. The fact there may be uncertainty for data controllers when conducting the balancing test does not legitimate removing that test (clearer guidance on conducting that test would be the better solution), being as it is a vitally important stop on violation of individuals' rights. If there is an urgent need to process data for bias monitoring, detection and correction that overrides any intrusion on the rights of individuals, this is something that will become clear when conducting the balancing test; it is not a reason not to conduct the test in the first place.

5. Further, the consultation document envisages a "limited, exhaustive list of legitimate interests" when the balancing test would not apply; however, even for this one suggested legitimate interest (bias monitoring, detection, correction), the types of processing that could be said to fall within this interest could be vast, as could therefore the amount of data processed without conducting a balancing test. This is even more the case when one considers that it will be organisations who will determine whether certain processing is classified as for bias monitoring, detection, correction.

6. We are also concerned that removing the balancing test will impact on the right to object to data processing contained in Article 21 GDPR – an issue which is not covered by the consultation document at all, but which is central to the legitimate interests test. Article 21 GDPR allows data subjects to inform the data controller of their particular situation and to object to data processing concerning them which is based on Article 6(1)(f) GDPR. Subsequently, the controller will need to repeat the balancing test for that specific data subject when they are given this new information, and if the revised balance is in favour of the data subject, then the processing ceases for that specific data subject. Removing the balancing test in Article 6(1)(f) for a specified list of legitimate interests may negate the Article 21 right to object, with negative impacts for people's ability to challenge decisions that have an impact on their rights and the fairness of such decisions overall.[9]

[9] Amberhawk, *Government propose to tip the scales in the controller's legitimate interests,* 14 October 2021, available at: https://amberhawk.typepad.com/amberhawk/2021/10/government-propose-to-tip-the-scales-in-the-controllers-legitimate-interests.html

Q.1.5.11

To what extent do you agree that further legal clarity is needed on how sensitive personal data can be lawfully processed for the purpose of ensuring bias monitoring, detection and correction in relation to AI systems? Please explain your answer, and provide supporting evidence where possible.

7. **Liberty neither agrees nor disagrees with this proposal.** We disagree in principle with the idea of extending situations where sensitive personal data can be processed, even in pursuit of positive-sounding measures such as bias monitoring, detection, and correction, if that would ride roughshod over established protections. Any form of clarification that will expand these situations without a rigorous assessment of the implications for people's data rights is highly concerning. See our answer to Q.1.5.12 below.

Q1.5.12.

To what extent do you agree with the proposal to create a new condition within Schedule 1 to the Data Protection Act 2018 to support the processing of sensitive personal data for the purpose of bias monitoring, detection and correction in relation to AI systems? Please explain your answer, and provide supporting evidence where possible.

8. **Liberty neither agrees nor disagrees with this proposal.** We acknowledge that the underlying intention is to ensure that "AI system[s] work appropriately and fairly."[10] We also appreciate that there is a distinct difficulty with trying to define 'fairness' in the context of AI systems (and algorithmic decision-making systems specifically): as noted by the Centre for Data Ethics and Innovation (CDEI) – an independent advisory body to the Government on the use of data and AI – in human decision-making systems, it is possible to leave "a degree of ambiguity about how fairness is defined", whereas "algorithms… are unambiguous: If we want a model to comply with a definition of fairness, we must tell it explicitly what that definition is."[11] However, we are concerned that this proposal (and the consultation document as a whole) appears to treat the question of fairness as primarily about mitigating bias. We are worried that this framing obscures broader questions about the development and context-specific implementation of AI and related technologies and structural inequality and discrimination, and works from a likely baseless assumption that wholly mitigating bias in AI systems is even possible.

9. Our starting point is the sensitive nature of certain categories of data – including data revealing someone's racial or ethnic origin, political opinions, religious or

[10] Pg. 33, *Data: A new direction.*

[11] Pg. 29, Centre for Data Ethics and Innovation, *Review into bias in algorithmic decision-making,* November 2020, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/957259/Review_into_bias_in_algorithmic_decision-making.pdf

philosophical beliefs, trade union membership, genetic data, biometric data, health data, and data concerning a person's sex life and sexual orientation. In the GDPR, this data (which is known as sensitive personal data in the UK) is recognised as requiring greater protection because of the significant risks that processing such data can pose to an individual's rights and freedoms, for example, the freedom of thought, conscience, and religion, freedom of expression, freedom of assembly and association, right to bodily integrity, right to respect for private and family life, and freedom from discrimination.[12] Article 9(1) GDPR prohibits the processing of special categories of data, subject to the exceptions in Article 9(2) GDPR.

10. In the UK, Schedule 1 of the Data Protection Act 2018 establishes the conditions that permit the processing of special categories of personal data and criminal offence data. Processing of the special categories of personal data will meet the requirements in Article 9(2)(b), (h), (i), or (j) if they meet one of the conditions listed in Part 1 of Schedule 1. Processing will meet the requirement in Article 9(2)(g) if it meets one of the conditions in Part 2, Schedule 1.

11. The consultation document correctly states that explicit consent is not the only ground under which sensitive personal data can be processed, and that relying on consent as a ground can result in 'consent-fatigue' as individuals face a large volume of consent requests which they might accept despite not having the time or resources to assess them properly.[13] However, the consultation document subsequently goes on to state that "[i]n some circumstances it may be necessary to obtain explicit consent from an individual to use their sensitive personal data to monitor or mitigate bias. Making explicit that consent is a prerequisite for data access may in itself risk introducing bias into the data used in an AI system, as in practice, *every time an individual refuses to provide consent to processing, a dataset may become unrepresentative*. As a consequence, any output of the AI application may be *biased* towards the demographic of individuals willing to consent to processing."[14] We fundamentally disagree with the way that this statement sets explicit consent in opposition to attempts to make technology more fair. We are concerned that this proposal ignores the legitimate reasons why people may not want to share their sensitive personal data, and what it reveals about the general attitude towards consent as one of the grounds under which sensitive personal data can be processed. Not only are people with protected characteristics, including marginalised communities, being blamed for not consenting to attempts to mitigate bias, one perverse implication of this statement is that *they* should be the ones taking the responsibility for mitigating the bias of which they bear the brunt.

[12] ICO, *Special category data,* November 2019, available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/
[13] Pg. 21, *Data: A new direction.*
[14] Pg. 34, *Data: A new direction.*

12. More broadly, we believe that a focus on 'debiasing' AI is misguided, which renders the proposal to create a carve-out for processing sensitive data on the basis of bias monitoring, detection, and correction problematic. On one level, we are unconvinced of whether AI systems can actually be 'debiased'. As noted by European Digital Rights (EDRi), "the act of defining protected attributes and the values they can take is reductive and harmful",[15] given that protected characteristics have multiple (and intersecting) dimensions, the effects of which cannot be easily separated and disaggregated. Taking the example of race: race is not simply an attribute or a category on a census, but a structural, institutional, and relational phenomenon.[16] It is unclear how attempts to mitigate bias in a particular design and/or use of AI could ever adequately mitigate racial discrimination in its full complexity.

13. Fundamentally, we are concerned that a focus on bias mitigation and correction – that is, a 'technocentric' approach that focuses on technical debiasing[17] – ignores wider questions about how AI systems themselves may entrench structural inequality. We are perturbed by DCMS' justification of the potential disproportionate impact that this proposal may have on individuals with protected characteristics, given that many types of sensitive personal data do touch on these characteristics: "The more an individual's personal data is processed, the greater the likelihood of intrusion into their private and family life, and the greater the risk of a breach involving their personal data. Generally, a provision that will result in more processing could be characterised as adverse for affected individuals. However, the purpose of this proposal is to support organisations to monitor harmful bias and eliminate discrimination, so *any detrimental impact is considered objectively justifiable*."[18] This is a sweeping statement that effectively opens the door to the processing of people's sensitive personal data for the 'greater good' of bias mitigation – while preventing any critical scrutiny of whether this is actually a 'good' in the context of certain inherently rights-violative technologies, or indeed whether it is even possible. This is particularly concerning when considering the proposal within the consultation to remove the obligation on organisations to undertake Data Protection Impact Assessments (DPIA),[19] which are a crucial way that organisations can evaluate and mitigate risks arising from different decision-making systems (including algorithmic bias).[20]

---

[15] Pg. 60, EDRi, *Beyond debiasing: Regulating AI and its inequalities,* 2021, available at: https://edri.org/wp-content/uploads/2021/09/EDRi_Beyond-Debiasing-Report_Online.pdf
[16] Hanna, A., Denton, E., Smart, A., and Smith-Loud, J., *Towards a Critical Race Methodology in Algorithmic Fairness,* 2020, available at: https://arxiv.org/pdf/1912.03593.pdf
[17] Pg. 8, EDRi, *Beyond debiasing: Regulating AI and its inequalities,* 2021, available at: https://edri.org/wp-content/uploads/2021/09/EDRi_Beyond-Debiasing-Report_Online.pdf
[18] Pg. 35, *Data: A new direction.*
[19] Pg. 58, *Data: A new Direction.*
[20] Pg.10, Centre for Data Ethics and Innovation, Review into bias in algorithmic decision-making, November 2020, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/957259/Review_into_bias_in_algorithmic_decision-making.pdf

14. We believe the root of the problem is a narrow understanding of bias, which lacks an analysis of structural inequality. We note DCMS' definition of bias as "an unfair skew based on characteristics, arbitrary factors, or an otherwise inappropriate basis".[21] The assumption behind the proposal appears to be that mitigating 'unfair skews' – in other words, ensuring that the AI system treats everyone the same regardless of their characteristics or other factors – will be sufficient to ensure fairness in AI systems. However, this fails to adequately consider the ways AI systems reinforce and/or compound structural oppression.[22] A recently published joint legal opinion on the consultation has further noted that the consultation document as a whole appears to conflate 'outcome fairness' with the principle of non-discrimination, even though the concepts are distinct.[23] The effect of this assumption will be to "mean that organisations will unwittingly discriminate here in the UK."[24] We agree with the opinion, which further states that: "new legislation should recognise that fairness is conceptually different to the principle of non-discrimination and that no data processing can be lawful where it discriminates as understood within the EA 2010."[25]

15. The effect of this proposal will be to allow organisations – including private companies – to justify a wide range of processing on the basis that it is necessary for the purpose of "bias mitigation". Not only is this problematic in the sense of allowing organisations to potentially sweep up many types of processing under a vaguely-defined ground, it also acts to obscure wider issues: in developing 'debiasing' techniques – which themselves can be based on unhelpful and potentially harmful classifications of data – the questions of "[w]ho is doing the classifying? For what purpose are they classifying and to what end?"[26] become easily side-lined. But these are precisely the questions that we need to be asking when it comes to the development of AI and similar technologies. Expanding the pool of data that can be used to support the mitigation of bias for technologies that are inherently oppressive would be a Pyrrhic victory that fails to adequately address structural injustice in the round.

---

[21] Pg. 25, *Data: A new direction.*
[22] Singh, R., and Jackson, S., *Seeing like an infrastructure: Low-resolution citizens and the Aadhaar identification project*, Proceedings of the ACM on Human-Computer Interaction, Vol. 5, CSCW2, Article 315, October 2021, available at: https://dl.acm.org/doi/pdf/10.1145/3476056
[23] Allen, R., and Masters, D., Joint second opinion on the matter of the impact of the proposals within 'Data: A new direction' on discrimination under the Equality Act 2010, The Legal Education Foundation, available at: https://research.thelegaleducationfoundation.org/wp-content/uploads/2021/11/TLEF-Second-Opinion-5-November-2021.pdf
[24] Allen, R., and Masters, D., Joint second opinion on the matter of the impact of the proposals within 'Data: A new direction' on discrimination under the Equality Act 2010, The Legal Education Foundation, available at: https://research.thelegaleducationfoundation.org/wp-content/uploads/2021/11/TLEF-Second-Opinion-5-November-2021.pdf
[25] Allen, R., and Masters, D., Joint second opinion on the matter of the impact of the proposals within 'Data: A new direction' on discrimination under the Equality Act 2010, The Legal Education Foundation, available at: https://research.thelegaleducationfoundation.org/wp-content/uploads/2021/11/TLEF-Second-Opinion-5-November-2021.pdf
[26] Hanna, A., Denton, E., Smart, A., and Smith-Loud, J., *Towards a Critical Race Methodology in Algorithmic Fairness,* 2020, available at: https://arxiv.org/pdf/1912.03593.pdf

16. An analogous example of this can be found in debates over facial recognition technology (FRT). FRT is a demonstrative example of a technology that is inherently rights-violative, and for which bias mitigation is an inadequate solution. Liberty is aware of the deployment of Live Automated Facial Recognition technology (LFR) by police, as well as use of LFR by private companies, often in conjunction with police. Liberty is not aware of any deployments of LFR since the Court of Appeal's judgment in *R (Bridges) v South Wales Police* [2020] EWCA Civ 1058 ('Bridges') which ruled that South Wales Police's use of LFR was unlawful.

17. Liberty supports an outright ban on FRT, rather than simply trying to mitigate its potential biases, because we believe FRT can never be operated in a way that is compliant with human rights and will always compound existing systems of discrimination and oppression. Of course, it merits noting the real issues with bias in FRT, namely, those of misidentification and inaccuracy. In respect of misidentification, a range of studies have shown facial recognition technology disproportionately misidentifies women and BAME people[27][28] – meaning that people from these groups are more likely to be wrongly stopped and questioned (and potentially arrested) by police, and to have their images retained as the result of a false match. Similarly, the Court of Appeal in *Bridges* noted that there is scientific evidence that facial recognition can be biased and create a greater risk of false identifications in the case of women and BAME people. Research has demonstrated how trans and non-binary people are regularly misidentified by the tech, leading these communities vulnerable to situations of embarrassment, and contributing to stigmatisation (as well as the other rights intrusions outlined above in relation to women and BAME people).[29] Studies have also highlighted the disproportionate misidentification of disabled people by facial recognition technology, and AI more broadly.[30] There are also well-documented problems with the accuracy of FRT.[31]

18. Just as important as FRT's problems of misidentification and bias, however, is the way it fundamentally changes the relationship between the individual and the State and our right to remain anonymous more broadly. Being able to choose when and how to disclose one's identity, and to whom, is at the heart of a person's dignity and

[27] Buolamwini et al (2018), *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research, 2018 Conference on Fairness, Accountability, and Transparency
[28] Klare et al (2012), *Face Recognition Performance: Role of Demographic Information*, IEEE Transactions on Information Forensics and Security, available at: https://ieeexplore.ieee.org/document/6327355
[29] Privacy International (2021), *Threats in the usage of facial recognition technologies for authenticating transgender identities.* Available at: https://privacyinternational.org/news-analysis/4474/threats-usage-facial-recognition-technologies-authenticating-transgender
[30] Sheri Byrne-Haber (2019), *Disability and AI Bias. Available at: https://sheribyrnehaber.medium.com/disability-and-ai-bias-cced271bd533*
[31] Pg.11, Fussey, P., and Murray, D., *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, The Human Rights, Big Data and Technology Project, July 2019, available at: https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf

autonomy. In some cases, identification determines how the State interacts with people and whether they are afforded access to their rights. Knowing when and whether we are being tracked and monitored is an important way for us to hold the State to account and to challenge private companies' incursions on our rights – the reverse, *not* knowing, can have deleterious consequences. The human rights impact of the indiscriminate and non-consensual nature of FRT – including on freedom of expression and association - means that it should have no place on our streets.[32]

19. FRT – which in our view is inherently rights-violative, does not operate in a vacuum. In recent years, we have seen growing attempts on the part of the State to justify policy interventions and legislation prioritising surveillance, criminalisation, control, and punishment – with highly racially disproportionate effects – under the banner of protecting public safety. For example, the Government's approach to the coronavirus pandemic has prioritised criminal justice over a true public health approach, with disproportionate effects for marginalised communities.[33] Further, in the aftermath of the killing of Sarah Everard, the police have announced new plans to increase the presence of officers in public spaces – a move which has been described by the End Violence Against Women coalition as a "PR exercise" that fundamentally fails to address the root problems of institutional racism and sexism within the police force, while increasing the over-policing and criminalisation of Black and minoritised communities.[34] In the year ending March 2020, Black people were nine times more likely to be stopped and searched under s.1 PACE powers (and 18 times more likely to be stopped and searched when the requirement for reasonable suspicion was removed) than their white counterparts, with deleterious consequences for those who suffer the brunt of such powers;[35] and minoritised and migrant communities – including survivors of violence against women and girls (VAWG) – continue to face systemic problems accessing safety and justice.[36] We believe that any use of FRT – with its expansion of surveillance and criminalisation of individuals – will entrench existing systemic inequality and oppression, while also serving as a smokescreen for

[32] The use of FRT can be highly intimidating. For example, if we know our faces are being scanned by police and that we are being monitored when using public spaces, we are more likely to change our behaviour. Forty per cent of people aged 16-24 said they simply would not attend an event where facial recognition was being deployed. See: London Policing Ethics Panel, *Final report on Live Facial Recognition*, May 2019, available at: http://www.policingethicspanel.london/reports.html

[33] Busby, M. and Gidda, M., *BAME people fined more than white population under coronavirus laws,* The Guardian, 26 May 2020, available at: https://www.theguardian.com/world/2020/may/26/bame-people-fined-more-than-white-population-under-coronavirus-laws; and Harris, S., Joseph-Salisbury, R., Williams, P. and White, L., *A threat to public safety: policing, racism and the Covid-19 pandemic,* Institute of Race Relations, September 2021, available at: https://irr.org.uk/wp-content/uploads/2021/09/A-threat-to-public-safety-v3.pdf

[34] End Violence Against Women coalition, *Met Police action plan a PR exercise that will cause harm*, 10 November 2021, available at: https://www.endviolenceagainstwomen.org.uk/met-police-action-plan-a-pr-exercise-that-will-cause-harm/

[35] Ali A. and Champion, N. for the Criminal Justice Alliance, More harm than good - A super-complaint on the harms caused by 'suspicion-less' stop and searches and inadequate scrutiny of stop and search powers, May 2021, available at: https://www.criminaljusticealliance.org/wp-content/uploads/CJA-super-complaint-into-section-60-and-scrutiny-of-stop-and-search_FINAL.pdf

[36] HMICFRS, IOPC & College of Policing (2020). Safe to share? Report on Liberty and Southall Black Sisters' super-complaint on policing and immigration status. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/945314/safe-to-share-libertysouthall-black-sisters-super-complaint-policing-immigration-status.pdf

wider Government failures to address the root causes of social issues. In short, FRT will not make us more safe. Attempting to mitigate for bias in FRT puts the cart before the horse and ignores the wider question of whether such technology has any place in public spaces more generally.

20. By analogy with the FRT example above, we believe DCMS' proposal to enable processing of personal sensitive data – such as information about people's racial and ethnic identity – for bias mitigation purposes, appears to be at the very least a distraction from broader questions about whether AI systems – in their wide variety of usages and applications – are necessary, and the ways that they may entrench structural inequalities in the context of wider decision-making processes. We recall the CDEI's reminder that there are "circumstances where using algorithms to make life-affecting decisions can be seen as unfair *by failing to consider an individual's circumstances, or depriving them of personal agency*... It is crucial to take a broad view of the whole decision-making process when considering the different ways bias can enter a system and how this might impact on fairness. The issue is not simply whether an algorithm is biased, but whether the overall decision-making processes are biased. *Looking at algorithms in isolation cannot fully address this*."[37]

Q1.5.13.

What additional safeguards do you think would need to be put in place?

18. We believe a meaningful approach to tackling discrimination in AI cannot be a technocentric one. We echo the sentiment voiced by EDRi that a "sincere response from policymakers should require experts from other disciplines to account for the complexity of discrimination, centre-affected parties and should go beyond algorithms to consider a more holistic evaluation of AI systems".[38] In certain cases, a holistic evaluation of the impact of AI systems may result in the conclusion that the only safeguard against discrimination is an outright ban or prohibition on the use of specific technologies.

Automated decision-making and data rights

Q.1.5.14

To what extent do you agree with what the Government is considering in relation to clarifying the limits and scope of what constitutes 'a decision based solely on automated processing' and 'produc[ing] legal effects concerning [a person] or similarly significant effects? Please explain your answer, and provide supporting evidence where possible, including on: The

[37] Pg.6, Centre for Data Ethics and Innovation, Review into bias in algorithmic decision-making, November 2020, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/957259/Review_into_bias_in_algorithmic_decision-making.pdf

[38] Pg. 117, EDRi, *Beyond debiasing: Regulating AI and its inequalities,* 2021, available at: https://edri.org/wp-content/uploads/2021/09/EDRi_Beyond-Debiasing-Report_Online.pdf

benefits and risks of clarifying the limits and scope of 'solely automated processing'; The benefits and risks of clarifying the limits and scope of 'similarly significant effects'.

19. **Liberty neither agrees nor disagrees with this proposal.** If by 'clarify' the Government means 'narrow' the definitions of these terms, we **strongly disagree with this proposal.**

20. Before elaborating on our answer, we first set out our key terms and understanding of automated decision-making (ADM). Simply put, algorithms are sets of programmed rules that operate on data, usually large quantities of it. From this data, they produce an output desired by their developers; they "make sense of" large datasets and, for that reason, are integral to the architecture of our contemporary "Big Data" society. An algorithm's output can be a unit of actionable intelligence – a value or classification that is used to inform a decision made by a human decision-maker or, in solely automated systems, forms the sole basis of a decision itself. The algorithms that are of concern to us are those which operate on "a corpus of data composed of traces of our activities, preferences and expressions"; that is, when human beings are the data subjects. These "*public relevance algorithms*"[39] can be used to make significant decisions that engage people's human rights. For example, to draw on Liberty's work on police use of ADM, algorithms have been used to process historical crime data to determine where and when future police patrols should take place (as we note below, algorithms rely on data that already exists about past policing practices, meaning that they do not necessarily correlate with incidence of crime – instead, their use is likely to give rise to feedback loops and the chronic policing of certain areas and communities).[40]

21. Many algorithms are not strictly speaking decision-making algorithms. Instead, they supplement, rather than supplant, the professional judgement of human decision-makers. They are often framed as discretionary "tools"; this ensures that, in the last instance, responsibility for a decision still lies with a human decision-maker. In these contexts, decision-making is sometimes called "semi-automated". In other contexts, decision-making is said to be "solely automated"; that is, an algorithm's output automatically effects a decision or is merely witnessed by a human whose presence is a formality. However, the distinction between semi-ADM and solely ADM is not always so clear because: "automation bias, whereby human users who are provided with advice by machines will often become increasingly reliant on and uncritical of this advice with time, means a decision-assisting tool can easily become a decision-making tool in practice."[41] Issues also arise where people are not equipped with the

[39] Tarleton Gillespie, "The relevance of algorithms" (2014), 168, https://www.microsoft.com/en-us/research/wp-content/uploads/2014/01/Gillespie_2014_The-Relevance-of-Algorithms.pdf.
[40] Liberty (Hannah Couchman), *Policing by Machine*, 1 February 2019, available at: https://www.libertyhumanrights.org.uk/issue/policing-by-machine/
[41] CDEI, Landscape *Summary*, 18-19.

knowledge to question decisions made by complex algorithms or where people will not want to supplant an algorithm's decision, particularly in high-pressure situations. This is exacerbated by the general lack of transparency around how algorithms work.

22. Article 22 of the UK GDPR provides 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".[42] This also applies to ADM that involves "profiling", which is defined as: "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."[43] 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.[44]

23. The reason that solely ADM attracts such scrutiny is because such decisions are recognised to engage people's human rights in significant ways. Indeed, academics have highlighted the exceptional nature of the general prohibition under Article 22 GDPR when compared to other forms of data protection law. While the *travaux préparatoires* to the EU GDPR provide little explanation of the rationale for these provisions, we may refer to the concerns that gave rise to the predecessor to Article 22, Article 15 of the Data Protection Directive (Directive 95/46/EC, or 'DPD').[45] During discussions around the forerunner to what would became Article 15(1) of the DPD, the European Commission stated, "This provision is designed to protect the interest of the data subject in participating in the making of decisions which are of importance to him. The use of extensive data profiles of individuals by powerful public and private institutions *deprives the individual of the capacity to influence decision-making processes within those institutions*, should decisions be taken on the sole basis of his 'data shadow'."[46] As noted by some academics, apart from emphasising the importance of people being able to understand and challenge decisions that have an

[42] Data Protection Act 2018, Section 49, http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf.
[43] *ibid.*, Section 33(4).
[44] *ibid.*, Section 14(5).
[45] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
[46] Pg. 29, Commission of the European Communities, *Proposal for a Council directive concerning the protection of individuals in relation to the processing of personal data: Draft resolution of the representatives of the governments of the Member States of the European Communities meeting within the Council, COM(90) 314 final – SYN 287 and 288,* 13 September 1990, available at: http://aei.pitt.edu/3768/1/3768.pdf

impact on their lives, Article 22 (and its predecessors) appear to be rooted in a concern for the concept of personal integrity and human dignity.[47]

24. Liberty is concerned by the potential consequences of DCMS' proposal, which may include narrowing the scope of what constitutes a "decision based solely on automated processing" (an inference supported by DCMS' later proposal to do away with Article 22 altogether). We are concerned that narrowing the definition of what constitutes solely ADM and "similarly significant effects" may give rise to violations of human rights. We note that in spite of the technological optimism that appears to be driving DCMS's proposals, there remains a limited evidence base regarding the claimed benefits, scientific validity, or cost effectiveness of the use of algorithms in certain sectors (such as policing),[48] not to mention highly controversial past precedents that have resulted in violations of human rights.[49] We are concerned that one of the key motivating factors behind the expanded use of algorithms is austerity and the chronic underfunding of the public sector, meaning that there are not enough resources to fund fair and effective decision-making;[50] however, in the words of CDEI: "[data-driven] tools should not be considered a silver bullet for funding challenges".[51]

25. Current working definitions of solely ADM, legal effects, and "similarly significant effects" are left deliberately broad. Article 29 Working Party – an advisory body set up to address issues of protection of privacy and personal data in the EU – confirmed that the scope of Article 22 should be interpreted expansively, such that a data controller cannot avoid the Article 22 provisions by "fabricating human involvement".[52] Any oversight of a decision must be "meaningful, rather than just a token gesture."[53] This is an inclusive, rather than an exhaustive, definition.

---

[47] Mendoza, I. and Bygrave, L.A., *The right not to be subject to automated decisions based on profiling,* University of Oslo, 9 March 2018, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2964855; "Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals." Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=EN

[48] Pg. 64, Centre for Data Ethics and Innovation, *Review into bias in algorithmic decision-making,* November 2020, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/957259/Review_into_bias_in_algorithmic_decision-making.pdf

[49] Lyall, S., *The dangerous rise of policing by algorithm*, Prospect Magazine, 19 March 2021, available at: https://www.prospectmagazine.co.uk/science-and-technology/the-dangerous-rise-of-policing-by-algorithm

[50] Pilkington, E., *Digital dystopia: how algorithms punish the poor*, The Guardian, 14 October 2019, available at: https://www.theguardian.com/technology/2019/oct/14/automating-poverty-algorithms-punish-poor

[51] Pg. 8, Centre for Data Ethics and Innovation, *Review into bias in algorithmic decision-making,* November 2020, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/957259/Review_into_bias_in_algorithmic_decision-making.pdf

[52] Pg. 21, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, available at: https://ec.europa.eu/newsroom/article29/items/612053/en

[53] Pg. 21, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, available at: https://ec.europa.eu/newsroom/article29/items/612053/en

26. Indeed, we have concerns about how existing definitions of solely ADM are interpreted and applied. In 2018, Liberty observed a police deployment of LFR in Stratford. Despite assurances that human intervention was key and that a police officer would always check images to confirm a match, we observed one situation in which, when a match alert came up on the computer – a young black man bearing little resemblance to the probe image from the watch list – officers were immediately radioed with a description. We watched as the man was stopped and searched and his ID checked. The ordeal went on for some time while the police officers radioed back and forth and eventually concluded that the man was not known to the police. Afterwards, he expressed his frustration as he had done nothing wrong and his time had been wasted. Officers admitted that the person apprehended was clearly not the man in the probe image – it was not, as one officer noted, "a fool-proof system". In this example, the fact that police appeared to act immediately upon being notified of a match alert should at the very least raise the question of whether this qualified as a solely ADM decision, with implications for the responsibilities of police officers in using this technology and importantly, the rights of the individual being stopped. This is particularly important given what we know about the flaws (including issues to do with discrimination and bias) in LFR and algorithmic technology, and the fact individuals from racialised and minoritised communities will be disproportionately stopped.[54]

27. What constitutes "legal effects" for the purposes of Article 22 is also defined broadly as something affecting an individual's legal rights, whether that is their freedom to associate with others, vote in an election, or to take legal action.[55] In acknowledgement of the many ways that public decision-making can affect people's lives beyond their legal rights, the term "similarly significant effects" is included in the provision to encapsulate situations where "even where there is no change in their legal rights or obligations, the data subject could still be impacted sufficiently to require the protections under [Article 22]". In such cases, "the threshold for *significance* must be similar to that of a decision producing a legal effect." [56] The Article 29 Working Party includes decisions affecting people's financial circumstances (such as their eligibility to credit) and their access to education (such as university admissions) within this definition.

28. Certain other countries' domestic GDPR laws (such as those of France and Hungary) take an even broader view of what falls under the scope of the Article 22 protection. In these countries, the right extends to "all automated decisions prejudicial to the

[54] Couchman, H., *"'Not a fool-proof system': Facial recognition in action,* Liberty, 29 June 2018, available at: https://www.libertyhumanrights.org.uk/issue/not-a-fool-proof-system-facial-recognition-in-action/
[55] Pg. 21, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, available at: https://ec.europa.eu/newsroom/article29/items/612053/en
[56] Pg. 21, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, available at: https://ec.europa.eu/newsroom/article29/items/612053/en

person or which have a significant impact on the person concerned", rather than simply "legal" effects or "similarly significant effects" to legal effects.[57]

29. We urge DCMS to consider what it could do to enhance, rather than erode, people's rights not to be subject to potentially detrimental forms of ADM, including by widening the definitions of what constitutes solely ADM and what constitutes "similarly significant effects".

Q.1.5.15

Are there any alternatives you would consider to address the problem? Please explain your answer, and provide supporting evidence where possible.

30. **Liberty does not know whether there are any alternatives we would consider to address the problem.** This is because we are simply unsure about what problem DCMS is trying to solve by trying to clarify what constitutes solely ADM and "similarly significant effects". On one hand, DCMS says that there is a lack of certainty on how and when current safeguards are intended to apply – which implies a desire to retain the integrity of these safeguards due to their importance – and at the same time, DCMS says that the safeguards provided by Article 22 could be considered "too restrictive to ensure that the UK GDPR remains principle-based and future-proofed in light of evolving machine learning and AI technologies". Fundamentally, we question what DCMS means by 'future-proofing' and remain concerned that the direction of travel is towards weakened, rather than more robust, protections for people's rights.

31. We believe that one of the key problems with ADM is the lack of effective scrutiny of how ADM systems currently function.[58] In part, this may be due to an *overly* restrictive view of what constitutes solely ADM. For example, academics have noted that even in situations where there are multiple stages of decision-making and it is assumed there is meaningful human involvement, such as where ADM is used to provide information to a decision-maker, determine which cases get to a human decision-maker or passed to another automated process, or consolidate decisions from one or more human decision-makers, these may arguably actually be solely ADM decisions falling within Article 22. Indeed, "if humans are effectively rubber-stamping the computer outputs, rarely or never overturning them or lack the authority or competence to overturn them, it might be argued that *the decisions remain 'based*

[57] Malgieri, G., *Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations,* Computer Law & Security Review 35(5), Octobre 2019, available at: https://www.sciencedirect.com/science/article/pii/S0267364918303753

[58] In August 2020, JCWI and Foxglove successfully launched the first successful court challenge to an algorithmic decision-system in response to the Home Office's visa streaming algorithm. See: https://www.jcwi.org.uk/news/we-won-home-office-to-stop-using-racist-visa-algorithm and https://www.foxglove.org.uk/2020/08/04/home-office-says-it-will-abandon-its-racist-visa-algorithm-after-we-sued-them/

solely' on automated processing."[59] The solution to this is not to remove Article 22, but to ensure that its central aim – to protect people from harmful forms of decision-making – is achieved by rigorously scrutinising the substance of how decisions are actually made.

32. We also believe there should be greater scrutiny of the extent to which the protections in Article 22 should apply to the following situations, some of which may arguably fall under the prohibition on solely ADM for the reasons outlined above but which may not currently be considered as such:
    - **High-risk environments**, where decision-makers may feel reluctant to question a risk-scoring algorithm in case the danger it predicts materialises. One example of this can be found in Data Justice Lab's (DJL) 2018 report which considered Avon and Somerset Police's use of predictive policing technology.[60] One police inspector told DJL: "there are still some people in the organisation who believe [the technology] is the be-all-and-end-all and professional judgement isn't quite as important. *So there will be people who say…that is what we must do*".[61] They went on to say that "[If] we do something with person B and we don't do something with person A and then person A the goes on to kill someone or seriously injure them, *where is the defenceability [sic] around that?* So I can understand people's thinking in that sense, I really can".[62] The CDEI noted that in these environments, a decision-maker can over-rely on the automated output without applying their professional judgement.[63]

    - **High-pressure environments** where decision-makers may defer to the algorithm to work more swiftly through their caseloads and meet productivity targets (including where this occurs at one or more stages of the decision-making process); or for other reasons abdicate responsibility – either consciously or unconsciously – for significant decisions to the algorithm.[64] This

[59] Binns, R., and Veale, M., *Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR*, International Data Privacy, 00(0), 2021, available at: https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipab020/6403925
[60] See "Avon and Somerset" section in "Current Use in the UK"
[61] Dencik et al, 2018, *Data Scores as Governance: Investigating uses of citizen scoring in public services,* Available at: https://datajustice.files.wordpress.com/2018/12/data-scores-as-governance-project-report.pdf [Accessed December 2018]
[62] Ibid
[63] Pg. 68, Centre for Data Ethics and Innovation, *Review into bias in algorithmic decision-making,* November 2020, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/957259/Review_into_bias_in_algorithmic_decision-making.pdf
[64] "The danger of the misuse of data processing in decision-making may become a major problem in future: the result produced by the machine, using more and more sophisticated software, and even expert systems, has an apparently objective and incontrovertible character to which a human decision-maker may attach too much weight, thus abdicating his own responsibilities." See Pg. 26, Commission of the European Communities, Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM(92) 422 final – SYN 287, 15 October 1992, https://aei.pitt.edu/10375/1/10375.pdf

can leave people at the mercy of complex decision-making systems that they cannot effectively challenge, but that have a significant impact on their lives. Philip Alston, the United Nations Special Rapporteur[65] on extreme poverty and human rights, has said of the Department of Work and Pensions (DWP): *"Because the default position of DWP is to give the automated system the benefit of the doubt, claimants often have to wait for weeks to get paid the proper amount, even when they have written proof that the system was wrong. An old-fashioned pay slip is deemed irrelevant when the information on the computer is different".*[66]

- **"Low-rights environments"**[67] where decision-makers may simply not feel duty-bound to use their professional judgement because the data subjects are perceived as undeserving, or forms of structural inequality and oppression mean that certain people's rights are not given effective and meaningful protection. One example can be found in Big Brother Watch's (BBW) 2021 report into algorithms in the social welfare system, specifically, its findings on RentSense.[68] RentSense, developed by Mobysoft, is the dominant system used to analyse rent payment patterns in the social housing sector. Mobysoft says RentSense has 150 customers, making up one third of local authorities and two thirds of housing associations, and that it analyses data on 1.6 million tenants (which is 31% of all social tenants).[69] Despite asking dozens of social landlords for their Equality Impact Assessments ahead of implementing RentSense, only one responded to BBW with their document, which did not mention RentSense at all (despite the EIA covering housing policy until 2024). As noted by BBW, "the fact that the potential for algorithms to entrench discrimination was not considered is concerning," with some local authorities dismissing any risk of harm to protected groups as a result of algorithmic bias altogether.[70] For example, in Gosport Borough Council Housing Board's request for board approval for procurement of RentSense, it stated: "The service is inclusive for all GBC social housing tenants and is an operational enhancement to existing housing management processes. *There is no impact on groups with protected characteristics.*"[71]

[65] Special Rapporteurs are independent experts appointed by the UN Human Rights Council with the mandate to monitor, advise and publicly report on human rights situations, either in specific countries or worldwide.
[66] Alston, 2018, *Statement on Visit to the United Kingdom*, *United Nations Special Rapporteur on extreme poverty and human rights,* Available at] https://www.ohchr.org/Documents/Issues/Poverty/EOM_GB_16Nov2018.pdf [Accessed November 2018]
[67] See Virginia Eubanks. *Automating Inequality: How High-Tech Tools Profile, Punish and Police the Poor* (2018), 12: "...'low rights environments' where there are few expectations of political accountability and transparency..."
[68] Big Brother Watch, *Poverty Panopticon: The hidden algorithms shaping Britain's welfare state*, 20 July 2021, available at: https://bigbrotherwatch.org.uk/wp-content/uploads/2021/07/Poverty-Panopticon.pdf
[69] RentSense Brochure, https://cdn2.hubspot.net/hubfs/2639450/RentSense%20Brochure.pdf
[70] Big Brother Watch, *Poverty Panopticon: The hidden algorithms shaping Britain's welfare state*, 20 July 2021, available at: https://bigbrotherwatch.org.uk/wp-content/uploads/2021/07/Poverty-Panopticon.pdf
[71] Gosport Report on Procuring Rentsense, 20th January 2021, https://democracy.gosport.gov.uk/documents/s2662/8.Procurement%20of%20Rentsense.pdf

33. In lieu of reducing people's rights in this area, Liberty recommends that there be an expanded exploration and understanding of what constitutes solely ADM. We also agree with the Information Commissioner (IC) who has recommended that Article 22 be extended to cover partly, as well as wholly, automated decision-making.[72]

34. In general, we believe that there must be greater transparency and accountability over ADM systems. More consideration also needs to be given to the impact of ADM on marginalised groups. Data protection law and the GDPR in general tends to focus on individual data subject rights, rather than group-based rights.[73] However, as has been well-documented, ADM (including solely ADM) can have impacts on groups of people, including groups of people with protected characteristics.

35. Finally, the question of whether certain forms of ADM can ever be human rights-compliant – and the risks of the normalisation such forms of decision-making – remains a live and important one. We believe that proper public and Parliamentary scrutiny over the role of ADM in our society is long overdue.

Q.1.5.16

To what extent do you agree with the following statement: 'In the expectation of more widespread adoption of automated decision-making, Article 22 is (i) sufficiently future-proofed, so as to be practical and proportionate, whilst (ii) retaining meaningful safeguards'? Please explain your answer, and provide supporting evidence where possible, on both elements of this question, providing suggestions for change where relevant.

36. **We somewhat agree with this statement**. We believe strongly in the importance of Article 22 and believe that it can be strengthened through implementing more robust safeguards, including for example extending protection to partly ADM (as per the IC's recommendation) and expanding the definition of what constitutes "solely ADM" and "similarly significant effects". The aim of these proposals is to ensure fair, transparent and accountable decision-making. See our answer to Q.1.5.15 above.

Q.1.5.17

To what extent do you agree with the Taskforce on Innovation, Growth and Regulatory Reform's recommendation that Article 22 of UK GDPR should be removed and solely automated decision making permitted where it meets a lawful ground in Article 6(1) (and Article 9-10 (as supplemented by Schedule 1 to the Data Protection Act 2018) where relevant) and subject to compliance with the rest of the data protection legislation?

[72] Pg. 14, ICO, *Response to DCMS consultation "Data: A new direction",* 6 October 2021, available at: https://ico.org.uk/media/about-the-ico/consultation-responses/4018588/dcms-consultation-response-20211006.pdf
[73] Edwards, L. and Veale, M., *Slave to the algorithm? Why a 'right to an explanation' is probably not the remdy you are looking for,* Duke Law and Technology Review, 2017, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855

37. **Liberty strongly disagrees with this proposal.** In our view, it completely ignores the very important reasons why there is a prohibition on solely ADM in the GDPR (see above), not least that ADM can have irrevocable consequences on people's lives. For example, in 2020, after the coronavirus pandemic caused examinations to be cancelled, the Office of Qualifications and Examinations Regulation (Ofqual) decided to use an algorithm to determine pupils' A-level grades. The algorithm - which was found to be inaccurate, biased, and to replicate existing patterns of inequality – led almost 40% of students to receive grades lower than they had anticipated,[74] prompting significant outcry and legal action. Ofqual was eventually forced to make a u-turn, scrapping the grades in favour of teachers' predicted results.[75] The A-levels fiasco resurfaced the importance of democratic oversight and governance of ADM. We agree with the IC that the right to human review of decisions that can fundamentally affect our lives is (and has always been) a fundamental cornerstone of data protection law in the UK.[76]

Q.1.5.20

Please share your views on whether data protection is the right legislative framework to evaluate collective data-driven harms for a specific AI use case, including detail on which tools and/or provisions could be bolstered in the data protection framework, or which other legislative frameworks are more appropriate.

38. **Specific AI use cases must be evaluated using a rights-based approach.** Just as laws and policies engaging human rights must be adequately prescribed by law, necessary, and a proportionate way of achieving a legitimate aim, the design and implementation of AI technologies and ADM must be subject to similarly robust scrutiny. Additionally, the use of AI technologies must be robustly evaluated in relation to (at least) data protection principles, the Human Rights Act 1998, and the Equality Act 2010. Any such application must be adequately communicated to all stakeholders, including those who may encounter particular difficulties accessing this technology, such as people who are digitally excluded and people with protected characteristics.

Further questions

Q.1.8.1.

In your view, which, if any, of the proposals in 'Reducing barriers to responsible innovation' would impact on people who identify with the protected characteristics under the Equality

[74] Bedingfield, W., *Everything that went wrong with the botched A-Levels algorithm*, Wired, 19 August 2020, available at: https://www.wired.co.uk/article/alevel-exam-algorithm

[75] Kolkman, D., *"F**k the algorithm"?: What the world can learn from the UK's A-level grading fiasco*, LSE, 26 August 2020, available at: https://blogs.lse.ac.uk/impactofsocialsciences/2020/08/26/fk-the-algorithm-what-the-world-can-learn-from-the-uks-a-level-grading-fiasco/

[76] Pg. 35, ICO, *Response to DCMS consultation "Data: A new direction",* 6 October 2021, available at: https://ico.org.uk/media/about-the-ico/consultation-responses/4018588/dcms-consultation-response-20211006.pdf

Act 2010 (i.e. age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation)?

39. We are highly concerned that any attempts to erode protections against ADM, including the proposal to remove Article 22, will have a disproportionate impact on people with protected characteristics. Notably, Article 22 specifically applies to ADM that involves "profiling", which is defined as: "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."[77] While not all profiling will take place in relation to protected characteristics, there is significant overlap and crossover (either directly or indirectly via proxy indicators) between the factors used to profile people and those characteristics. Given the existing lack of transparency regarding ADM and the ways that current systems may already impact on people with protected characteristics – indeed, the ignorance on the part of many public bodies that such effects may even be a concern – we are disturbed by DCMS's proposals in this Chapter, which will only further entrench and give rise to potential violations of people's rights.

40. This is not an abstract concern. In April 2018, it was revealed that police data fed into the HART system was supplemented using an Experian[78] dataset called "Mosaic", produced through profiling each of the 50 million adults in the UK.[79] Mosaic profiles and classifies people into spurious groups – for example, a *"crowded kaleidoscope"* is a low-income*, "multi-cultural"* family working *"jobs with high turnover"* and living in *"cramped houses"* and *"overcrowded flats"*.[80] Mosaic even links names to stereotypes: for example, people called Stacey are likely to fall under *"Families with Needs"* who receive "a range of benefits". Terrence and Denise are *"Low Income Workers"* who have *"few qualifications"* and are *"heavy TV viewers"*.[81] Running this data through individual risk assessment programs inevitably encourages a discriminatory and offensive association between factors such as family circumstances, income, and propensity to commit crime. At the time of Liberty's 2018 report *Policing by Machine*, this individual risk assessment program was being used to assess whether a person is eligible to be diverted to a rehabilitation program and

[77] *ibid.*, Section 33(4).
[78] Experian is a consumer reporting agency. Consumer reporting agencies are companies that collect and sell personal information on consumers that is used to decide whether to provide consumers credit, insurance, medical care, housing, banking services, utilities, and employment.
[79] Big Brother Watch, *Police use Experian Marketing Data for AI Custody Decisions* [Press release], 6 April 2018, available at: https://bigbrotherwatch.org.uk/all-media/police-use-experian-marketing-data-for-ai-custody-decisions
[80] Ibid.
[81] Ibid.

avoid the formal court process.[82] This alone is a significant decision, and there is potential for these programs to be used in a much wider range of circumstances within the criminal justice sector.

41. Another example is the National Data Analytics Solution (NDAS), which features in a 2021 report by the organisation Fair Trials.[83] West Midlands Police state that NDAS uses "advanced analytics and statistical techniques"[84] in order to "create meaningful insight and identify value driving patterns which should ultimately lead to crime prediction and prevention", enabling police "to action the insights generated", "make early interventions" and "evidence-based local interventions", in order to "prevent criminality… by proactively addressing threats".[85] NDAS uses police intelligence reports on individuals and 'events', stop and search data, drug use data and custody information, as well as social media data and commercial marketing data from Experian,[86] to inform its operations.[87] West Midlands Police has said that it intends future partners providing data for the NDAS to include the National Health Service, the Department for Education, the Department for Work and Pensions, and the Department for Communities and Local Government,[88] giving it the ability to: "pull in data from other local public service providers (such as social care services, local authorities, education providers and other emergency services), private sector organisations, or open source data to deepen understanding of local services and the social context."[89] Notably, West Midlands Police acknowledges that it uses personal data and special category personal data and conducts 'sensitive processing' under the Data Protection Act 2018 as part of the NDAS.[90] It also acknowledges that there is an "absence of a framework regulating analytics in law enforcement" and has said that it is "developing a proposed framework" itself.[91]

---

[82] People who are scored as "medium risk" are eligible to participate in the program, called "Checkpoint". See Liberty (Hannah Couchman), *Policing by Machine*, 1 February 2019, available at: https://www.libertyhumanrights.org.uk/issue/policing-by-machine/

[83] Fair Trials, *Automating Injustice: The use of artificial intelligence and automated decision-making systems in criminal justice in Europe,* 9 September 2021, available at: https://www.fairtrials.org/publication/automating-injustice

[84] West Midlands Police, National Data Analytics Solution Privacy Notice. https://west-midlands.police.uk/aboutus/privacy-notice/national-data-analytics-solution#

[85] Intelligence Management System (IMS) – police intelligence reports about events, locations and offenders; ICIS – custody information data; Corvus – an intelligence, briefing and tasking system; Police National Computer (PNC) – major police database containing information on individuals, crimes, vehicles and property; Drug Intervention Programme (DiP) data; OASIS – event logging system; among others. See: Police Transformation Fund, National Analytics Solution, Final Business Case v6.0, 29 March 2017 (http://foi.west-midlands.police.uk/wp-content/uploads/2019/01/report1_.pdf

[86] Police Transformation Fund, National Analytics Solution, Final Business Case v6.0, 29 March 2017 (http://foi.west-midlands.police.uk/wp-content/uploads/2019/01/report1_.pdf)

[87] Police Transformation Fund, National Analytics Solution, Final Business Case v6.0, 29 March 2017 (http://foi.west-midlands.police.uk/wp-content/uploads/2019/01/report1_.pdf)

[88] Police Transformation Fund, National Analytics Solution, Final Business Case v6.0, 29 March 2017 (http://foi.west-midlands.police.uk/wp-content/uploads/2019/01/report1_.pdf)

[89] West Midlands police, National Data Analytics Solution Privacy Notice. https://west-midlands.police.uk/aboutus/privacy-notice/national-data-analytics-solution#

[90] West Midlands police, National Data Analytics Solution Privacy Notice. https://west-midlands.police.uk/aboutus/privacy-notice/national-data-analytics-solution#

[91] West Midlands police, 'NDAS Submission to the WMP Ethics Committee', September 2020. https:// www.westmidlands-pcc.gov.uk/wp-content/uploads/2020/11/25092020-EC-Agenda-Item-5-NDASUpdate.pdf?x16458

42. In recent years, West Midlands Police have developed a model aimed at predicting serious violence. The purpose of this model is "to predict which individual nominals, who are already known to the police, are likely to commit their first most serious violence offence in the next 24 months."[92] Data used to inform this model includes "a summary of an individual's past behaviour derived from appearances within police data. Some examples of these behaviours are the past number of offences committed, the number of times a person has been a victim, or the number of times a person has been mentioned within an intelligence report".[93] As noted by Fair Trials:[94]

> "In its own analysis of NDAS, and specifically the MSV model, West Midlands Police admits that "there is currently no formal system in place" to analyse and demonstrate whether the MSV model will "improve the current system".[95] West Midlands Police states that it uses a "precision score" of only 50 per cent for the outputs of the model, meaning that the prediction must only be around 50 per cent certain to actually occur for it to be used to inform interventions.[96] Initial testing of the MSV model by West Midlands Police resulted in a precision score of just 54 per cent.[97] An independent review of the NDAS by the Alan Turing Institute Data Ethics Group (ATI DEG) and Independent Digital Ethics Panel for Policing (IDEPP) concluded that there were: "serious ethical issues… concerning surveillance and autonomy, as well as the reversal of the presumption of innocence on the basis of statistical prediction".[98]

43. It is worth noting the particular impact that ADM may have on children and young people. The West Midlands Police Ethics Committee has raised concerns that active proposals using crime data to identify young 'violent offenders' in school catchment areas would create "risks of stigmatising and labelling children, areas, schools or neighbourhoods)."[99]

---

[92] Logistic Regression, Gradient Boosting Machines and Random Forest algorithms. The Random Forest algorithm was used as the main classifier. See: West Midlands police, 'WMP Ethics Committee briefing note, NDAS – Most Serious Violence (MSV)', 20 November 2019. https://www.westmidlands-pcc.gov.uk/wp-content/uploads/2019/12/27112019-EC-Item-3-BriefingNote-NDAS-MSV.pdf

[93] West Midlands police, WMP Ethics Committee briefing note, NDAS – Most Serious Violence (MSV), 20 November 2019. https://www.westmidlands-pcc.gov.uk/wp-content/uploads/2019/12/27112019-EC-Item-3- Briefing-Note-NDAS-MSV.pdf

[94] Fair Trials, *Automating Injustice: The use of artificial intelligence and automated decision-making systems in criminal justice in Europe,* 9 September 2021, available at: https://www.fairtrials.org/publication/automating-injustice

[95] West Midlands police, WMP Ethics Committee briefing note, NDAS – Most Serious Violence (MSV), 20 November 2019, available at: https://www.westmidlands-pcc.gov.uk/wp-content/uploads/2019/12/27112019-EC-Item-3-Briefing-Note-NDAS-MSV.pdf

[96] West Midlands police, WMP Ethics Committee briefing note, NDAS – Most Serious Violence (MSV), 20 November 2019, https://www.westmidlands-pcc.gov.uk/wp-content/uploads/2019/12/27112019-EC-Item-3-Briefing-Note-NDAS-MSV.pdf

[97] Ibid.

[98] Alan Turing Institute Data Ethics Group (ATI DEG) and Independent Digital Ethics Panel for Policing (IDEPP), 'Ethics Advisory Report for West Midlands Police', 28 July 2017. https://www.turing.ac.uk/sites/default/files/2018-11/turing_idepp_ethics_advisory_report_to_wmp.pdf

[99] https://www.westmidlands-pcc.gov.uk/archive/ethics-committee-february-2020/ See also: Documents ref 14122020 - EC - Agenda Item 3c - Analysis of school catchment areas and violence – proposal and 14122020 - EC -

44. We are highly concerned that the expansion of the use of ADM, especially in the policing and law enforcement context, will entrench racial disproportionality within the criminal justice system. For example, we know that certain communities are policed disproportionately as compared to other communities. Because there is greater involvement of the police in respect of certain communities, the data that is fed into ADM and predictive policing programmes is more likely to reflect police involvement in a certain community than potential crime. One study suggests that predictive mapping programs merely spark a "feedback loop" that leads to officers being repeatedly sent to certain neighbourhoods – typically ones with a higher percentage of BAME residents – regardless of the true crime rate in that area.[100] The problem stems from the logic that predictive mapping programs are used to decide where officers should be sent. If an officer is sent to a neighbourhood and then makes an arrest, the software takes this as indicating a good chance of more crimes being committed in that area in future.[101]

45. In a similar example, researchers from the Human Rights Data Analysis Group released a landmark study that reconstructed and applied a predictive policing program to Oakland, California in the United States. [102] This study focused on the local police department's record of drug crimes from 2010.[103] They found that the system would have sent police officers "*almost exclusively to lower income, minority neighbourhoods*"[104] even though public health-based estimates suggested that drug use was widespread across the city. If these predictions had been used in active deployment, police would have patrolled areas where they were exacerbating pre-existing policing bias.

46. Importantly, the same report noted that increased scrutiny and surveillance resulting from the disproportionate patrolling of historically over-policed communities had been linked to worsening mental and physical health.[105] There is longstanding scientific and medical evidence pointing to the severe health related consequences of over

Minutes Advice For background see article: https://www.birminghammail.co.uk/news/midlands-news/fears-over-police-plan-identify-20193614

[100] *Ensign et al, 2017, Runaway feedback loops in predictive policing*, available at https://arxiv.org/abs/1706.09847 [Accessed November 2018]

[101] The issue of feedback loops was also raised in JCWI's and Foxglove's successful challenge to the Home Office's visa-streaming algorithm. See: https://www.foxglove.org.uk/2020/08/04/home-office-says-it-will-abandon-its-racist-visa-algorithm-after-we-sued-them/

[102] Lum et al, 2016, *To predict and serve?,* Significance Magazine, Available at: https://rss.onlinelibrary.wiley.com/doi/abs/10.1111/j.1740-9713.2016.00960.x [Accessed November 2018]

[103] Ibid.

[104] Ferguson, 2017, *The Truth About Predictive Policing and Race*, Available at: https://medium.com/in-justice-today/the-truth-about-predictive-policing-and-race-b87cf7c070b1 [Accessed November 2018]

[105] Lum et al, 2016, *To predict and serve?,* Significance Magazine. Available at: https://rss.onlinelibrary.wiley.com/doi/abs/10.1111/j.1740-9713.2016.00960.x [Accessed November 2018]

policing.[106] We are concerned that by entrenching harmful policing practices – and potentially giving them greater legitimacy and a guise of neutrality as a result of being supported by a flawed algorithm – the effect may actually be to exacerbate the root causes of crime.

47. It is worth noting that there is no clear evidence of the benefits of data-sharing in the policing and wider criminal justice contexts. The CDEI notes for example in its AI Barometer Report that its expert panel "noted that there is a lack of evidence that making more data available in judicial proceedings necessarily improves the quality and reliability of justice decisions. Assessing the proportionality of data extraction may therefore be difficult."[107]

48. This is particularly important when considering the Police, Crime, Sentencing and Courts Bill (PCSC Bill) which is currently undergoing its passage through Parliament. Part 2, Chapter 1 of the Bill places a new statutory duty on public bodies such as healthcare authorities, youth services, local authorities and education providers to collaborate with each other to prevent and tackle serious violence. Under the Bill, police will be given the power to demand information disclosure from public bodies (including education authorities, healthcare providers or social workers) and they must acquiesce, regardless of whether they determine sharing the information is in the public interest or breaches any of their other legal duties or professional obligations. This is backed up by the power of the Secretary of State to give directions mandating public bodies' compliance with the duty, including obligations of information disclosure. Not only have these disclosure provisions been drafted in such a way so as to override the professional and legal safeguards around personal data that exist in order to safeguard people's human rights, and potentially even the data protection legislation, the broad drafting of the duty under clause 7 means that any information disclosure - whether that is about individuals' health status, religious beliefs or political opinions and affiliations - could ostensibly be justified under the banner of 'preventing and reducing serious violence'.[108]

49. Instructive examples of the kinds of harms that data-sharing of this kind can give rise to can be seen from the well-documented systemic failings of the London Metropolitan Police Service's (MPS) Gangs Matrix that were identified following investigations by the Information Commissioner's Office (ICO) and the Mayor's Office of Police and

[106] Deivanayagam, T.A., Lasoye, S., Smith J., and Selvarajah, S., *Policing is a threat to public health and human rights*, BMJ Global Health, 2021, available at: https://gh.bmj.com/content/bmjgh/6/2/e004582.full.pdf; American Public Health Association, *Addressing Law Enforcement Violence as a Public Health Issue,* 13 November 2018, available at: https://www.apha.org/policies-and-advocacy/public-health-policy-statements/policy-database/2019/01/29/law-enforcement-violence

[107] Pg. 44, Centre for Data Ethics and Innovation, *AI Barometer Report,* June 2020, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/894170/CDEI_AI_Barometer.pdf

[108] These are subject to a higher degree of protection under both the Data Protection Act 2018 (DPA) and the ECHR.

Crime (MOPAC). One of the key problems identified in the Gangs Matrix by the ICO was that it failed to distinguish between victims of serious violence and perpetrators of serious violence, resulting in chronic and widespread surveillance and criminalisation of individuals, their families and their communities.[109] People were also denied access to vital services such as housing and education as a result of unfettered data-sharing.[110] In one devastating case a 14-year-old was shot and killed in 2017 after his details were mistakenly shared by Newham Council. Newham was subsequently fined £140,000 over this serious data breach.[111] Crucially, the Gangs Matrix was criticised for stark statistics demonstrating that it over-identified people of colour as gang-affiliated – at the time of publication of a report by Amnesty in 2018,72 per cent of individuals on the MPS's Gangs Matrix were black, yet the MPS's own figures showed that just 27 per cent of those responsible for serious youth violence were black.[112][113]

50. It is worth noting that a wide range of professional bodies, organisations, and individuals have spoken out against the data harms that may result from the serious violence duty, not least the National Data Guardian,[114] the General Medical Council and the British Medical Association,[115] the British Association for Counselling and Psychotherapy and the British Psychological Society,[116] more than 665 frontline social,

[109] Information Commissioner's Office, *ICO finds Metropolitan Police Service's Gangs Matrix breached data protection laws,* 16 November 2018, available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/ico-finds-metropolitan-police-service-s-gangs-matrix-breached-data-protection-laws/

[110] Amnesty International, 'Trapped in the Matrix: Secrecy, stigma and bias in the Met's Gangs Database', May 2018, https://www.amnesty.org.uk/files/reports/Trapped%20in%20the%20Matrix%20Amnesty%20report.pdf; Patrick Williams, 'Being Matrixed: The (over)policing of gang suspects in London', August 2018, https://www.stop-watch.org/uploads/documents/Being_Matrixed.pdf

[111] Amnesty International, 'Trapped in the Matrix: Secrecy, stigma and bias in the Met's Gangs Database', May 2018, https://www.amnesty.org.uk/files/reports/Trapped%20in%20the%20Matrix%20Amnesty%20report.pdf

[112] Amnesty International, 'Trapped in the Matrix: Secrecy, stigma and bias in the Met's Gangs Database', May 2018, https://www.amnesty.org.uk/files/reports/Trapped%20in%20the%20Matrix%20Amnesty%20report.pdf.

[113] The West Midlands Police Ethics Committee has raised concerns that active proposals using crime data to identify young 'violent offenders' in school catchment areas would create "risks of stigmatising and labelling children, areas, schools or neighbourhoods)." (published February 2021) https://www.westmidlands-pcc.gov.uk/archive/ethics-committee-february-2020/ See also: Documents ref 14122020 - EC - Agenda Item 3c - Analysis of school catchment areas and violence – proposal and 14122020 - EC - Minutes Advice. For background see article: https://www.birminghammail.co.uk/news/midlands-news/fears-over-police-plan-identify-20193614

[114] National Data Guardian, *Data-driven innovation: why confidentiality and transparency must underpin the nation's bright vision for the future of health and care*, 4 October 2021, available at: https://www.gov.uk/government/news/data-driven-innovation-why-confidentiality-and-transparency-must-underpin-the-nations-bright-vision-for-the-future-of-health-and-care; Diver, T., *Priti Patel's crime Bill will turn us into police informants, complain medics*, The Telegraph, 13 September 2021, available at: https://www.telegraph.co.uk/politics/2021/09/13/priti-patels-crime-bill-will-turn-us-police-informants-complain/

[115] Lintern, S., *Concern police will be able to 'strong-arm' NHS to hand over patient data under new plans,* The Independent, 17 October 2021, available at: https://www.independent.co.uk/news/health/police-nhs-patient-data-bill-b1938998.html

[116] The British Psychological Society, *BPS raises serious concerns about patient confidentiality and trust under new proposed legislation*, 27 October 2021, available at: https://www.bps.org.uk/news-and-policy/bps-raises-serious-concerns-about-patient-confidentiality-and-trust-under-new; BACP, *We join BPS in calling for changes to draft crime Bill*, 20 October 2021, available at: https://www.bacp.co.uk/news/news-from-bacp/2021/20-october-we-join-bps-in-calling-for-changes-to-draft-legislation/

health, education, youth, and community workers,[117] as well as former senior police officers and advisors.[118]

51. The erosion of protections against solely ADM and the expansion of ADM is likely to hasten and extend the potential harms resulting from such sharing (and potentially give rise to more of these practices), with significant negative consequences for people with protected characteristics.

CHAPTER 2: REDUCING BURDENS ON BUSINESSES AND DELIVERING BETTER OUTCOMES FOR PEOPLE

Data protection impact assessments

Q.2.2.7

To what extent do you agree with the following statement: 'Under the current legislation, data protection impact assessment requirements are helpful in the identification and minimisation of data protection risks to a project'? Please explain your answer, and provide supporting evidence where possible; **and**

Q.2.2.8

To what extent do you agree with the proposal to remove the requirement for organisations to undertake data protection impact assessments? Please explain your answer, and provide supporting evidence where possible, and in particular describe what alternative risk assessment tools would achieve the intended outcome of minimising data protection risks.

52. **Liberty firmly rejects the government proposal to further attenuate the already weak regulatory framework around Data Protection Impact Assessments (DPIAs)**, and instead suggests changes that would make DPIAs far more effective at protecting both data controllers and data subjects.

53. Question 2.2.7 appears to invite an assessment of the utility of DPIAs as simply a risk management tool for data controllers. Used correctly, they can indeed *"help you systematically analyse, identify and minimise the data protection risks of a project or*

[117] Lasoye, S., *Prevention, not punishment: why health workers must resist the policing bill,* Medact, 18 October 2021, available at: https://www.medact.org/2021/blogs/prevention-not-punishment/the; Liberty, *Frontline workers warn Policing Bill puts young people at risk,* 13 September 2021, available at: https://www.libertyhumanrights.org.uk/issue/frontline-workers-warn-policing-bill-puts-young-people-at-risk/; Modin, A., and Topping A., *Policing bill will deepen racial and gender disparities, say experts*, The Guardian, 13 September 2021, available at: https://www.theguardian.com/uk-news/2021/sep/13/policing-bill-will-deepen-racial-and-gender-disparities-say-experts; Sharman, J., *Policing bill 'will put young people at risk', hundreds of experts warn,* The Independent, 13 September 2021, available at: https://www.independent.co.uk/news/uk/politics/policing-bill-2021-data-surveillance-b1918664.html

[118] PA, *Policing bill 'disproportionately impacts black men' and 'exacerbates violence', ex-chiefs warn*, ITV, 25 October 2021, available at: https://www.itv.com/news/2021-10-25/policing-bill-could-undermine-trust-and-exacerbate-violence-ex-chiefs-warn

plan", but, for data processors, DPIAs are also *"an essential part of your accountability obligations"*, and should be evaluated as such.[119] Section 64(1) of the Data Protection Act 2018 (DPA 2018) contains the obligation for a data controller to conduct a DPIA, "*[w]here a type of processing is likely to result in a high risk to the rights and freedoms of individuals.*" The trigger is already a high bar, allowing organisations to process significant amounts of personal data without completing a DPIA. Crucially, it depends directly on the risk posed to individuals by the proposed processing. DPIAs are also "*an essential part of your accountability obligations*".[120] DPIAs are not a suggestion, but an obligation; a bulwark (albeit a limited one) against data processors who might exploit the personal data of individuals with no regard for the impact on their rights and freedoms.

54. In a properly executed DPIA, there is no conflict between these two elements; all organisations have a strong intrinsic financial and reputational interest in ensuring that they are in compliance with the law and respect the data protection and other rights of those whose data they process. DPIAs can enable data processing organisations to avoid ploughing money, time and expertise into developing systems which breach data protection law, or violate other rights, and may subsequently be under legal challenges or investigations, which are often accompanied by steep fines and huge national and international reputational damage.

55. The government's proposal to allow organisations to "*adopt different approaches*" to data protection risks which "*better reflect their circumstances*" appears to link the level of scrutiny applied to a proposed project to the nature of the data processor,[121] rather than the threat they pose to the rights and freedoms of individuals. This is not just an erosion of the principles underpinning DPIAs, but a radical inversion of them.

56. The entire purpose of a single regulatory standard is to create a single baseline of protection for individuals' rights and freedoms. It is self-evident that the level of protection due to an individual should follow from the risk they face, not the "*circumstances*" of the entity threatening them. It is, in fact, extremely concerning that the government is considering making *greater* allowances for entities with *less* capacity to assess the impact of their own actions. If an entity does not have capacity to assess the impact of its processing on the rights/freedoms of individuals, when that processing is likely to pose a high risk to those rights/freedoms, then the conclusion should be that the entity should not carry out that processing; not that it does not need to assess its impact.

[119] ICO: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/what-is-a-dpia/
[120] ICO: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/what-is-a-dpia/
[121] Pg. 58, *Data: A new direction.*

57. Further, having a single regulatory standard to assess risk from data processing in the form of a DPIA is imperative to allow the public to know what to ask data processors for (including, in respect of public bodies, through freedom of information requests) when seeking to examine the processors' risk assessment; and for that assessment to be contained in one place, which can be readily analysed by the recipient. DPIAs are also an important and straightforward means by which data processors can demonstrate to courts, and courts can assess, the compliance (or otherwise) of those processors with relevant data protection and other laws in their processing.

58. DPIAs also have advantages for organisations carrying them out. The negative implications of tearing out one of the few protections that do exist around the exploitation of personal data on individuals are obvious but, given the framing of this question, it is also worth considering the negative impact on data processors. As discussed above, it is in data processors' own interests to *at least consider* the impact of their activities on individuals' rights and freedoms. This is true of huge multinational organisations, but may be even more important for smaller organisations, which are generally far less capable of bearing the cost of failing to comply with the law.

59. One of the ironies of this government proposal is that, though large data processors would likely be able to design bespoke 'compliance' processes which would allow them to undertake higher and higher risk activities with less and less oversight, smaller organisations without significant internal compliance departments may well end up sticking with the existing DPIA templates. The likelihood of this scenario is compounded by the relative lack of organisational knowledge in smaller data processors about how to comply with the data protection principles and their broader obligations, which can currently be demonstrated through DPIAs.[122] Equally, if data processors are left to design their own divergent compliance systems, this would effectively hamstring the ICO's ability to provide comprehensive, specific and practical guidance on how to conduct effective DPIAs (for which Liberty argues below). This would, again, likely have a disproportionately negative impact on smaller, less well-resourced organisations. Ultimately, this proposal risks creating a two-tier system of compliance which primarily advantages precisely the large, wealthy organisations which pose the greatest structural threat to the rights and freedoms of individuals. This proposal would not just let them mark their own homework, but set the questions too.

[122] ICO: DPIAs "can be an effective way to assess and demonstrate your compliance with all data protection principles and obligations." - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/what-is-a-dpia/

60. It is also easy for data processing organisations, legislators and data subjects alike to undervalue DPIAs because so much of their impact is not quantitively measurable. Data processors, in particular, may isolate and decry the upfront administrative cost of conducting DPIAs in absolute terms rather than, correctly, viewing that cost as relative to the potentially vast counter-factual cost of building a system, or even a whole business around a process which poses an unacceptable risk to the rights and freedoms of individuals and may be subject to legal challenge.

61. DPIAs create an indispensable baseline of protection for data processors and subjects alike: at the very least, they force the data protection and other rights impacts of internal decisions onto the data processors' agendas. Like so many regulations protecting individual rights, DPIAs are most important when they are least convenient.

62. DPIAs are, however, by no means perfect. Even before the passage of the GDPR, commentators were arguing that a DPIA could only be as useful as its implementation. In 2012, data protection lawyers warned that DPIAs: "*will only be effective if organisations carry out reasonable risk analysis assessments to ensure 'privacy by design' and where meaningful reports are produced, as opposed to organisations simply completing a bureaucratic box ticking exercise (or sub-contracting this work to data processors without proper consideration)*."[123] Experience has shown that, all too often, the DPIAs that are produced do not reach even this minimal threshold. This is for a range of interrelated reasons:

    - **DPIAs are internal assessments.** They are initiated, conducted and largely overseen by those who typically have the greatest investment in driving forwards the project that is being assessed. This sort of conflict of interests can lead to a DPIA being reduced to a bureaucratic box ticking exercise. Assessors may be exposed to internal pressure to deliver a favourable DPIA at high speed and low cost, but even in the absence of such pressure, the accuracy and utility of DPIAs are entirely contingent on the skills, time, resources, and organisational co-operation available to the internal assessor. Small organisations in particular may lack these elements, while their processing poses no less significant a risk to individuals' rights/freedoms.

    - **DPIA triggers are not clear enough.** The problems associated with the execution of DPIAs also apply to the decision to conduct them at all. A data processor must conduct one if the processing is "*likely to result in a high risk"* to the rights and freedoms of individuals, but even this phrase includes three significant value

[123] Stephanie Pritchett, 'Data protection impact assessments: look before you leap'(2012) - Data protection impact assessments: look before you leap | Westlaw UK

judgments which are to be made by the data processor themselves about the threat they pose. The paucity of clear guidance around the obligation means that DPIAs may not even be conducted, save for in the three specific circumstances specified in the legislation itself.

- **DPIAs may be pitched extremely narrowly.** The above issues can also result in DPIAs being conducted in relation to the rights/freedoms of only a sub-set of those individuals potentially affected by a process. For example, South Wales Police carried out a DPIA in relation to their deployment of LFR, but made the incorrect assumption that this practice only presented a risk to the privacy rights to those individuals on their 'watchlist', and not the thousands of other members of the general public whose faces were scanned.[124] As a result, the DPIA did not assess the risk it posed to this (much larger) group, or present effective mitigation for those risks, resulting in the Court of Appeal finding that it was unlawful. This issue is, of course, particularly acute in the context of DPIAs conducted by public authorities, many of which hold the most sensitive of personal data.

- **DPIAs are extremely flexible.** DPIAs are already a flexible set of principles-based requirements, which can be adapted for a wide range of circumstances. The required elements of a DPIA that are set out in section 64(3) of the DPA 2018 comprise a very loose skeleton which can already be adapted by organisations conducting them. At their essence, these elements require that a data processor give a "*general description*" of the envisaged processing, assess the risks associated with it, indicate what they will do to mitigate those risks, and note which safeguards they will include to protect personal data. It is hard to see which of these already over-broad elements could be removed without rendering the entire exercise redundant.

- **DPIAs fundamentally lack transparency.** This is true both in principle and in practice, in relation to DPIAs. Limited external oversight of their accuracy or comprehensiveness means that we currently rely on the principle of organisational self-interest to enforce a proper analysis of the data protection risks associated with a project. We hope that this is enough to ensure every DPIA is carried out with proper skill, care, time, and attention, but experience suggests this has not been the case. The lack of transparency compounds the issues identified above as it severely limits the ability of data subjects to interrogate the effectiveness and adequacy of either the DPIA or the safeguards it should include. This is particularly problematic in relation to DPIAs conducted by private organisations; as they cannot be obtained through Freedom of Information Act

[124] See paragraph 153 of *Bridges*.

requests, the very existence, let alone the substance, of such DPIAs is often impossible to confirm for concerned data subjects. Leading data and digital rights academic Swee Leng Harris has suggested that mandating that DPIAs conducted by the Government must be published "*would help to address the current lack of transparency on government data processing systems*",[125] but this could also serve the additional objective of opening up a broader conversation about best practice between public and private entities. The current system siloes both best and worst practice in the internal systems of individual organisations.

- **DPIAS are forward-looking.** As leading technology and fundamental rights academic Heleen Janssen has pointed out, a "*DPIA is an ex ante form of risk assessment*".[126] There is a significant risk, which is enhanced with particularly novel processing systems, that data protection risks would only be discovered once a system is in operation. Under Article 35(11) GDPR, another DPIA should be undertaken when a change of risk occurs and is identified, but isolating either of these points can be an extremely subjective exercise.

- **DPIAs are often focused on risks to the right to privacy alone.** Section 64(1) of the DPA 2018 links the DPIA obligation to the "*rights and freedoms of individuals*". As Swee Leng Harris has argued, to discharge this requirement, "*DPIAs need to look at all human rights, not just privacy*".[127] Harris gives the example of a DPIA in relation to the Government's "settled status" scheme for EU citizens in the UK and identifies that this processing "*could affect applicants' rights to family life, to housing, to work, and to access healthcare because of the immigration law restrictions on the right to work, right to rent, and access to health services in the context of UK immigration policy*".[128] A properly compliant DPIA should consider the risks posed by processing to a much broader swathe of rights and freedoms as the ICO states, "*DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm – to individuals or to society at large, whether it is physical, material or non-material.*"[129].

[125] Swee Leng Harris, 'Data Protection Impact Assessments as rule of law governance mechanisms' (30 March 2020), Cambridge University Press. Data Protection Impact Assessments as rule of law governance mechanisms | Data & Policy | Cambridge Core
[126] Heleen Janssen, 'Detecting New Approaches for a Fundamental Rights Impact Assessment to Automated Decision-Making' (17 February 2021), International Data Privacy Law -Detecting New Approaches for a Fundamental Rights Impact Assessment to Automated Decision-Making by Heleen Janssen :: SSRN
[127] Swee Leng Harris, 'Data Protection Impact Assessments as rule of law governance mechanisms' (30 March 2020), Cambridge University Press. Data Protection Impact Assessments as rule of law governance mechanisms | Data & Policy | Cambridge Core
[128] Op cit.
[129] ICO: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

63. The shortcomings in the current DPIA regime are real, but the solution is to build on, not undermine, the levels of protection that individuals have in the face of opaque and possibly abusive data processing practices. We need proper guidance around when and how DPIAs should be conducted, an energised and vigilant regulator and a re-orientation of our cultural relationship to vast data-mining and data-marketing organisations. The government's proposals would exacerbate, rather than mitigate, the current issues with DPIAs. Liberty believes that the way forward is to strengthen the DPIA regime, not weaken it, or even throw it out altogether. It is self-evident that regulation is always inconvenient for those who would otherwise breach it. To fairly assess the value of DPIAs, we need to look instead at what they do for individuals and society, and to consider not just if data processors can afford or be motivated to do them, but think seriously about whether we can afford to do without them.

Subject Access Requests

Q.2.3.1

Please share your views on the extent to which organisations find subject access requests time-consuming or costly to process. Please provide supporting evidence where possible, including: What characteristics of the subject access requests might generate or elevate costs; Whether vexatious subject access requests and/or repeat subject access requests from the same requester play a role; Whether it is clear what kind of information does and does not fall within scope when responding to a subject access request.

64. As the consultation document states, the ability of individuals to access their own data is a fundamental right, ensuring that organisations are accountable for how they use personal data and also that individuals have a right to privacy and self-determination. Without access to their own data, individuals cannot check or correct its accuracy, know who it has been shared with, or how it is used to make decisions which affect them. The proposals to introduce a cost ceiling and to amend the threshold for a response mistakenly conflates the right to access our own data with the rights contained in the Freedom of Information Act 2000 to access information about public bodies. The right of access to one's own data is qualitatively different from the right of access to information about public decision-making. Individuals have a clear and legitimate interest in both types of information, but access to our personal data and the way in which it is used directly impacts our ability to enforce our rights. The procedure and threshold for accessing personal data must reflect that distinction.

65. Given the Government's acknowledgement of the importance of the right of access to personal data, the framing of the first question is surprising. The time or cost to an organisation of complying with a request by an individual carries little weight against the "fundamental right" of access to personal data. A more appropriate framing would be to investigate the extent to which individuals find it easy to request and access their own data from organisations. We note that the GDPR provides not only

that individuals have a right of access to their own data, but also a right to exercise the right of access "easily and at reasonable intervals".[130]

66. Ease of access to one's own data is a vital safeguard against unlawful data processing. For example, the claimant in *Catt v UK*[131] was only able to discover the unlawful retention of data about his attendance at protests as a result of subject access requests. Placing any barriers in the way of individuals who are seeking to discover what information is held about them will limit their ability to challenge incorrect records and the unlawful collection and retention of data; and may in turn disincentivise proper data management by data processors.

67. Unlawful data processing can have significant consequences for individuals; for example, in 2018 the ICO found that the Metropolitan Police Service's use of the 'Gangs Matrix' to record intelligence related to alleged gang members had led to serious breaches of data protection laws. The ICO's investigation found that the sharing of individuals' personal data with third parties and the failure to distinguish between those assessed as high and low risk created the potential for disproportionate action against the predominantly young Black men on the database. The only way for individuals to discover whether their data has been recorded on the database is by making a subject access request; anything that limits the ability of individuals to find out what information is held about them will increase the likelihood of discriminatory outcomes resulting from incorrect records, particularly concerning in policing and other contexts where significant decisions affecting individual's rights and freedoms are being made.

68. Subject access requests are also an essential tool for individuals and their lawyers in immigration cases. For example, the ability to access data held by local authorities and the police can play a crucial role in helping individuals to conclusively demonstrate that they are victims of modern slavery, and to enforce the rights that flow from that status. Subject access requests are often the only route through which legal practitioners can obtain access to information on which claims are based, and the only way to piece together complicated immigration histories.[132] In many cases, individuals will have been subject to control by traffickers or abusive partners, and have no access to their own documents. Records of interactions with organisations will be essential to demonstrating their right to remain in the UK and to access vital services. Similarly, individuals who have been unlawfully detained by the State will only be able to challenge their detention if they are able to obtain documents which demonstrate the Home Office's decision-making in the case. As with the Gangs Matrix, any restrictions on the right of access to personal data will have a disproportionate

[130] Recital 63, GDPR
[131] 69 EHHR 7
[132] Joanna Cherry, *Data Protection Bill [Lords]* Second Reading on 5 March 2018 (Volume 637, Columns 105-106).

impact on vulnerable and marginalised groups and make it harder for them to exercise and enforce their rights.

69. Given the overwhelming importance of access to personal data in these contexts, the time it takes for an organisation to comply with a request and the cost of doing so are a necessary obligation in order to ensure that everyone is able to access, correct and rely on their own data.

Q.2.3.2

To what extent do you agree with the following statement: 'The 'manifestly unfounded' threshold to refuse a subject access request is too high'? Please explain your answer, providing supporting evidence where possible, including on what, if any, measures would make it easier to assess an appropriate threshold.

70. **Liberty strongly disagrees with the statement that the "manifestly unfounded" threshold to refuse a subject access request is too high.** Given the nature of the data under concern, it is very difficult to imagine circumstances in which it would not be right to provide an individual with access to their own personal data. The ICO provides some examples of such circumstances in its guidance.[133] The ICO's guidance also provides a clear framework for organisations, setting the threshold for refusing a request appropriately high. The examples provided by the ICO make it clear that only malicious requests and requests by individuals who are not actually seeking to exercise their right of access to their data should be refused.

71. Any attempt to lower this threshold would result in the refusal of legitimate attempts by individuals to access their own data and would undermine the basic principle that individuals have the right to know what data is held about them.

72. The consultation document provides one example in support of lowering the threshold; that subject access requests may be used to circumvent disclosure rules contained in the Civil Procedure Rules. We note that there are clear exemptions in addition to the manifestly unfounded threshold that organisations must apply when considering a request for personal data, which include data that involves information about other individuals. In the case of *Dr DB v The General Medical Council*[134] the Court found that a request for data in the context of litigation ought to have been refused on the basis of the mixed data. The manifestly unfounded threshold also applied on the basis that the request was not made for the purpose of accessing the individual's own data. Rather than providing a basis for change, this case supports the status quo; the system already prevents the scenario presented by the consultation document.

[133] ICO guidance: 'When can we refuse to comply with a request?', cited in the Consultation document at paragraph 186.
[134] *Dr DB v The General Medical Council* [2016] EWHC 2331(QB).

73. The consultation response also proposes amending the threshold to provide that a request may be refused if it is vexatious, in line with the provisions governing freedom of information requests. We note that the Upper Tribunal has found that 'vexatious' in this context means "*manifestly unjustified, inappropriate or improper use of a formal procedure*".[135] It is difficult to see how the first part of that test can be distinguished from 'manifestly unfounded'. In relation to the request being inappropriate or improper, in Liberty's view an inappropriate use is accounted for by the ICO's guidance around requests made for purposes other than exercising a right of access. The Court of Appeal's further reasoning in the same case that "*the starting point is that vexatiousness primarily involves making a request which has no reasonable foundation, that is, no reasonable foundation for thinking that the information sought would be of value to the requester or to the public or any section of the public*"[136] does not assist the case for weakening the threshold for subject access requests. Subject access requests can clearly be distinguished from freedom of information requests on the basis that personal data has an inherent value to the individual which will always amount to a reasonable foundation for the request, save for the scenarios already envisaged by the ICO as malicious or not within the scope of the right.

Q.2.3.3

To what extent do you agree that introducing a cost limit and amending the threshold for response, akin to the Freedom of Information regime (detailed in the section on subject access requests), would help to alleviate potential costs (time and resource) in responding to these requests?

74. **Liberty is strongly opposed to the introduction of a cost ceiling to subject access requests.** As set out above, an individual's right of access to their own data is a fundamentally different right from the right of access to information about Government activity and decision-making. Freedom of information rights are an indispensable tool to ensure transparency and accountability and reliance on cost limit regime to restrict access to information held by public bodies can be of concern, but when applied to the personal data of the individual making the request, a cost limit is clearly inappropriate.

75. In Liberty's view it would be inappropriate to extend the cost limit that already applies to 'unstructured manual data' to filing systems and digital records. A cost limit would enable organisations to hide behind poor filing systems and record-keeping as a reason to charge individuals a fee to obtain information held about them. It would create a barrier preventing individuals from obtaining and challenging personal data

[135] *Information Commissioner vs Devon County Council & Dransfield* [2012] UKUT 440 (AAC), (28 January 2013).
[136] *Dransfield v Information Commissioner and Devon County Council* [2015] EWCA Civ 454 (14 May 2015).

which has been collected and retained and, on the basis of which, decisions are made about them. It also creates a perverse incentive for organisations to store data in an inaccessible way and to make it harder to retrieve records on request.

76. A cost ceiling would mean that whether an individual is able to obtain their personal data would be a lottery, depending on the amount of their data held by an organisation and the way in which it is stored. The proposal to require organisations to assist individuals to make targeted requests within the cost limit creates an additional burden on both organisations and individuals that is simply unnecessary under the existing straightforward regime that organisations must disclose all information held about the individual making the request. A cost limit creates an arbitrary barrier to the right of access to personal data in cases where the limit is exceeded and also adds unnecessary complexity to a procedure which ought to be as accessible to individuals as possible.

77. The consultation document acknowledges that this proposal may impact "persons less able to express themselves due to age or disability"[137] and states that this may be mitigated by the fact that a third party can raise a subject access request on their behalf. The assertion that individuals will easily be able to obtain assistance from a third party is simply not an adequate answer to a regime that will disproportionately prevent individuals who are most at risk from unlawful processing, from freely accessing their own data.

Q.2.3.4

To what extent do you agree with the following statement: 'There is a case for re-introducing a small nominal fee for processing subject access requests (akin to the approach in the Data Protection Act 1998)'? Please explain your answer, and provide supporting evidence where possible, including what a reasonable level of the fee would be, and which safeguards should apply.

78. **Liberty does not support the re-introduction of a "nominal" fee for processing subject access requests.** We note that DCMS' 'Analysis of expected impact' of the consultation only considers the estimated current cost of subject access requests to small and medium-sized enterprises (SMEs) and large businesses),[138] and the cost savings that might result from 'limiting the time and threshold for responding to subject access requests.'[139] A crucial fact that is missed is that the right of access to

[137] Paragraph 188, Data: A new direction.

[138] "Around 9 SARs on average per year at a cost of £75/SAR for SMEs and £375/SAR for large businesses." See paragraph 45, *Analysis of expected impacts*, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1016471/Data_Reform_Impact_Analysis_Paper.pdf

[139] '...Limiting the time and threshold for responding to subject access requests could lead to cost savings for businesses of around £55 million each year.' See paragraph 52, *Analysis of expected impacts*, available at:

personal data is often of the most vital importance to those vulnerable and marginalised individuals who are at the sharp end of decision-making by public bodies. In order to enforce rights ranging from the right to remain in the UK, to the right to access public services, to the right not to be discriminated against on the basis of incorrect or misleading data, it is imperative that individuals can easily make subject access requests about themselves. There does not appear to be any consideration of these impacts in the consultation document.

79. The nominal fee for one individual may amount to a significant barrier to another, particularly in the case of individuals who may have interacted with a number of public bodies and private organisations. We note that the outsourcing of public functions to private bodies increases the number of organisations holding information about individuals who rely on public services or who interact with the state, and that for individuals who are destitute or relying on subsistence benefits, even a nominal fee can create an obstacle preventing access to personal information vital for the enforcement of rights.

Further questions

Q2.6.1.

In your view, which, if any, of the proposals in 'Reducing Burdens on Businesses and Delivering Better Outcomes for People', would impact on people who identify with the protected characteristics under the Equality Act 2010 (i.e. age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation)?

80. We have limited our response to this question to the impact of the proposals we have responded to above, namely the proposals in respect of data protection impact assessments and the proposals in respect of subject access requests. If any of the proposals in this consultation are taken forward, we would expect a robust Equality Impact Assessment to be conducted and published in a timely manner (and in any event before any legislative proposal is made) examining these issues to enable effective scrutiny.

81. In Liberty's view, proposals to remove the requirement to carry out DPIAs would disproportionately impact on individuals with protected characteristics. As we have set out above, the increased use of ADM can lead to learned bias and discriminatory outcomes. The removal of the requirement to carry out a DPIA is therefore likely to lead to increased risks that data will be processed in ways which harm people with protected characteristics.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1016471/Data_Reform_Impact_Analysis_Paper.pdf

82. A properly conducted DPIA should consider the impact of data processing on the rights and freedoms of individuals, "focusing on the potential for harm".[140] This should include a consideration of any aspects of data processing which might disproportionately affect groups with protected characteristics. Public sector organisations are required to carry out equality impact assessments (or otherwise demonstrate their compliance with the Public Sector Equality Duty contained in s149 of the Equality Act 2010) which should complement DPIAs, but there is no equivalent requirement for private organisations. DPIAs then, are the only mechanism by which private organisations are required to consider the risks of discriminatory outcomes arising from data processing. In the public sector, DPIAs should complement equality impact assessments, and ensure that wherever data is collected, used and shared by public bodies, it is done with a view to eliminating discrimination and advancing equality as well as minimising data risks. By removing one element of this process, there is an increased risk of designing services with inbuilt data driven discrimination.

83. The proposals to reduce the threshold for refusing a subject access request, introducing a cost ceiling, and introducing a 'nominal' fee will all impact disproportionately on individuals with protected characteristics. As we have set out above, vulnerable and marginalised individuals (who are often individuals with one or more protected characteristic) are more likely to engage with the state and are therefore more likely to come to harm if the data which is used to make decisions about their lives is inaccurate or if they are unable to obtain it. Individuals who fear discriminatory data collection by the police, or whose access to social security benefits depends on accurate data, or who require access to their data to prove their right to remain in the UK, are the very individuals who will find even a nominal fee a significant barrier to accessing their own data.

84. A cost ceiling above which further fees apply will disproportionately affect individuals who have multiple and repeated interactions with the state. This may include individuals who have protected characteristics and access public services (such as health and social care facilities). Certain public services are also used more frequently by people with certain protected characteristics: for example, Employment and Support Allowance is paid to people who are disabled or sick.[141] The Government itself acknowledges that proposals which require individuals to express their requests in a targeted way to avoid the cost ceiling may disadvantage disabled people;[142] we would add that they will also disadvantage some individuals with the protected characteristic of race who do not speak English as a first language.

[140] ICO: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/
[141] Finnis, A., *What are legacy benefits? DWP court case explained and who could be eligible for £1,500 after missing uplift*, inews, 17 November 2021, available at: https://inews.co.uk/inews-lifestyle/money/legacy-benefits-dwp-court-case-what-explained-eligible-missing-uplift-1305289
[142] Pg. 70, *Data: A new direction*

85. The proposal to lower the threshold for refusing a request is also likely to disproportionately affect marginalised individuals, such as precarious workers (many of whom are migrants and/or people of colour).[143] For example, a driver of Ola – a 'gig' economy company – recently used subject access requests to uncover the company's use of algorithmic decision-making that resulted in deductions to their earnings.[144] Any proposal which makes it easier for public and private bodies to refuse requests will impair the rights of individuals to correct their data or challenge decisions based on it, leading to discriminatory and unlawful outcomes.

CHAPTER 4: DELIVERING BETTER PUBLIC SERVICES

Processing health data in an emergency

Q.4.3.3

To what extent do you agree with the proposal to clarify that public and private bodies may lawfully process health data when necessary for reasons of substantial public interest in relation to public health or other emergencies? Please explain your answer, and provide supporting evidence where possible.

86. **We strongly disagree with this proposal.** We note the concerning way that it appears to ignore the outcry that resulted from revelations in 2020 over NHS Digital's plans to share millions of patients' data – including large volumes of data pertaining to individuals such as protected health information, Covid-19 test results, the contents of people's calls to the NHS health advice line 111 and clinical information about those in intensive care[145] – in a database available to academic and commercial third parties for research and planning purposes (the 'General Practice Data for Planning and Research', also known as GPDPR or the NHS Dashboard). In April 2020, a Whitehall source expressed alarm at the amount of sensitive health data to which the companies involved in the database would be granted access, describing it as "unprecedented". At the time, Liberty joined a wider chorus of voices opposing the scheme, including the British Medical Association,[146] medical workers,[147] and privacy

[143] See: https://www.workerinfoexchange.org/ and Focus on Labour Exploitation, Independent Workers Union of Great Britain and United Voices of the World, *No viable alternatives: Social (in)security and risk of labour exploitation during Covid-19,* 2021, available at: https://labourexploitation.org/publications/no-viable-alternatives-social-insecurity-and-risk-labour-exploitation-during-covid-19

[144] The App Drivers and Couriers Union, *Gig economy workers score historic digital rights victory against Uber and Ola Cabs*, available at: https://www.adcu.org.uk/news-posts/gig-economy-workers-score-historic-digital-rights-victory-against-uber-and-ola-cabs

[145] Lewis, P., Conn, D., and Pegg, D., *UK government using confidential patient data in coronavirus response,* The Guardian, 12 April 2020, available at: https://www.theguardian.com/world/2020/apr/12/uk-government-using-confidential-patient-data-in-coronavirus-response

[146] BMA media team, *BMA calls for delay in roll-out of patient data sharing programme*, 4 June 2021, available at: https://www.bma.org.uk/bma-media-centre/bma-calls-for-delay-in-roll-out-of-patient-data-sharing-programme

[147] Bhatti, O., Singer, E., and Applebee, J., *GPDPR – An open letter to GP practices,* 31 May 2021, available at: https://drbhatti.com/2021/05/31/gpdpr-an-open-letter-to-gp-practices/

campaigners;[148] together, these widely-publicised challenges (and legal action) forced the NHS to delay its data grab and enabled more than a million people to opt-out.[149] No doubt NHS' data grab would be said to fall within the substantial public interest scenario being proposed, and thus would be considered lawful on the proposal, despite the number of people affected, volume/sensitivity of data shared and widespread public opposition; that cannot be right.

87. We are highly concerned that the Government is using the pandemic as an excuse to unpick the long-established principle of medical confidentiality, which is recognised at domestic[150] and international law, and which undergirds relationships of trust that enable effective medical treatment and respect for people's rights and dignity.[151] Liberty supports evidence-based, rights-centred, and proportionate responses to public health emergencies. It is for this reason that we do not support this proposal, because we believe that data-sharing with lesser safeguards can have the counterproductive effect of eroding people's right to privacy, which has longer term, negative implications for meaningful access to healthcare.

88. People have a right to know how and why their data is being processed, and to exercise control over that data – this is even more important when it comes to their sensitive health data. It is worth noting that in December 2020, Dame Fiona Caldicott enshrined the fundamental importance of medical confidentiality and transparency in a new Caldicott Principle (the standards that guide the use of patient identifiable information in the NHS): "*Inform patients and service users about how their confidential information is used*".[152]

89. When people do not know the purposes for which their data is being used, or fear that their data will be used for other purposes than medical care, this can result in withdrawal from services. An instructive example can be found in the operation of the hostile environment for migrants. The sharing of personal data between essential public services, central Government departments and the Home Office is a

[148] Marsh, S., *GPs warn over plans to share patient data with third parties in England,* The Guardian,30 May 2021, available at: https://www.theguardian.com/society/2021/may/30/gps-warn-plans-share-patient-data-third-parties-england
[149] Jayanetti, C., *NHS data grab on hold as millions opt out,* The Guardian, 22 August 2021, available at: https://www.theguardian.com/society/2021/aug/22/nhs-data-grab-on-hold-as-millions-opt-out
[150] See: The UK Caldicott Guardian Council, *The common law duty of confidentiality,* 2021, available at: https://www.ukcgc.uk/duty-of-confidentiality and General Medical Council, *Confidentiality: good practice in handling patient information – Legal annex,* 2021, available at: https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality/legal-annex#sources-of-law-on-confidentiality-data-protection-and-privacy
[151] General Medical Council, *Ethical and legal duties of confidentiality,* 2021, available at: https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality/ethical-and-legal-duties-of-confidentiality and National Data Guardian, *Data-driven innovation: why confidentiality and transparency must underpin the nation's bright vision for the future of health and care*, 4 October 2021, available at: https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality/ethical-and-legal-duties-of-confidentiality
[152] National Data Guardian, *Data-driven innovation: why confidentiality and transparency must underpin the nation's bright vision for the future of health and care*, 4 October 2021, available at: https://www.gov.uk/government/news/data-driven-innovation-why-confidentiality-and-transparency-must-underpin-the-nations-bright-vision-for-the-future-of-health-and-care

cornerstone of the hostile environment. Data-sharing currently occurs in respect of health, education, banking, driving, welfare benefits, employment, homelessness, local authority support, and policing. It often occurs without the knowledge or consent of the data subject, and in some cases the trusted public servant (e.g. doctor) who initially collected the data. Secrecy and non-consensual sharing are enabled in part by an exemption to data protection rights set out at Schedule 2, paragraph 4 of the Data Protection Act 2018.

90. Survey data from the Joint Council for the Welfare of Immigrants (JCWI) evidenced the impact of such data-sharing practices, with almost half of all migrants surveyed feeling scared to access healthcare if they got sick during the coronavirus pandemic.[153] Although NHS policy states that "anyone can register with a GP surgery" without "proof of address or immigration status, ID or an NHS number"[154], recent research by the Bureau of Investigative Journalism (TBIJ) shows that less than a quarter of GP surgeries (24%) surveyed across England, Scotland and Wales would register someone without proof of address, proof of ID or legal immigration status.[155] Testimony gathered by TBIJ note feelings of humiliation when turned away by GP surgeries due to a lack of identification.[156] As GP surgeries are the main dispensers of the Covid-19 vaccine, their inaccessibility has a knock-on impact for vaccine take-up amongst migrant communities. Recent evidence shows that migrants are having to travel to pop-up clinics across the country to receive the Covid-19 vaccine.[157] We are concerned that the further expansion of private and public bodies' processing of data, which may give rise to fears of (and actual) onward sharing without adequate safeguards, will deter people from accessing vital support.

91. Also worrying is the potential for proposals akin to the NHS Dashboard to give rise to greater use of unlawful predictive models and crude profiling.[158] In 2020, it was reported that the NHS Dashboard appeared to use a 'pseudo NHS number' to crossmatch large datasets including something referred to as a 'master patient index', an existing NHS resource that uses "social marketing data" to segment the British population into different "types" at household level.[159] As a baseline, we believe

[153] Gardner, Z. *Migrants deterred from healthcare during the COVID-19 pandemic,* JCWI, February 2021, available at: https://www.jcwi.org.uk/Handlers/Download.ashx?IDMF=a135b52c-e9d0-469c-aad8-3dde31aec7a1
[154] NHS, *How to register with a GP surgery,* 15 September 2021, available at: https://www.nhs.uk/nhs-services/gps/how-to-register-with-a-gp-surgery/
[155] Hamada, R et al., *Most GP surgeries refuse to register undocumented migrants despite NHS policy,* The Bureau of Investigative Journalism (TBIJ), 15 July 2021, available at: https://www.thebureauinvestigates.com/stories/2021-07-15/most-gp-surgeries-refuse-to-register-undocumented-migrants
[156] Ibid
[157] Ibid
[158] Lewis, P., Conn, D., and Pegg, D., *UK government using confidential patient data in coronavirus response,* The Guardian, 12 April 2020, available at: https://www.theguardian.com/world/2020/apr/12/uk-government-using-confidential-patient-data-in-coronavirus-response
[159] Lewis, P., Conn, D., and Pegg, D., *UK government using confidential patient data in coronavirus response,* The Guardian, 12 April 2020, available at: https://www.theguardian.com/world/2020/apr/12/uk-government-using-confidential-patient-data-in-coronavirus-response

predictive models may create discriminatory effects and entrench structural inequality. This is particularly worrying given the increasing prevalence of private companies becoming embedded in our public services.[160]

Transparency mechanisms for algorithms

Q4.4.1.

To what extent do you agree that introducing compulsory transparency reporting on the use of algorithms in decision-making for public authorities, government departments and government contractors using public data will improve public trust in government use of data? Please explain your answer, and provide supporting evidence where possible.

92. **Liberty somewhat agrees that introducing compulsory transparency reporting on the use of algorithms in public decision-making will improve public trust in government use of data.** We believe that transparency reporting is an important first step, but is not the only thing that is needed, for building public trust. Another crucial element of the puzzle is the maintenance and strengthening of robust safeguards for people's rights. We also believe that improving public trust in the government use of data should not be the only – nor the primary – consideration when it comes to such uses. Instead, all government usage of data should be compliant with human rights standards and data protection legislation. Depending on what transparency reporting will involve, for example, if it takes place through greater processing of sensitive personal data (even if this is for the purposes of "bias mitigation"), we echo our concerns above that this will in some cases be inadequate and potentially inappropriate to deal with the fundamental issues arising from ADM.

93. We are wary of reinforcing the "transparency fallacy" – that is, the idea that transparency is a sufficient remedy for algorithmic harms.[161] We echo the concern voiced by academics Mike Ananny and Kate Crawford that transparency can place "a tremendous burden on individuals to seek out information about a system, to interpret that information, and determine its significance".[162] We are concerned that one implication of this proposal might be to allow the government to shift responsibility for developing robust and rights-centred approaches to regulating ADM by placing the onus on individuals to challenge such decision-making on the basis of transparency reports. This is particularly concerning due to the asymmetry in power between some data controllers and the systems they design to make decisions which

[160] Williams, O., *Secret data and the future of public health: why the NHS turned to Palantir*, 21 May 2020, available at: https://www.newstatesman.com/science-tech/2020/05/secret-data-and-future-public-health-why-nhs-has-turned-palantir

[161] Pg. 6, Ananny, M. and Crawford, K., *Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability,* New Media and Society, 2016, available at: https://journals.sagepub.com/doi/10.1177/1461444816676645

[162] Pg. 7, Ananny, M. and Crawford, K., *Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability,* New Media and Society, 2016, available at: https://journals.sagepub.com/doi/10.1177/1461444816676645

have material impacts on people's lives; and the people themselves. Ultimately, we believe that there must be meaningful scrutiny of ADM, and not simply "formalistic bureaucratic overkill alongside a lack of substantial change".[163]

Clarifying rules on the collection, use and retention of biometric data by the police

Q.4.4.8

To what extent do you agree with the following statement: 'There is an opportunity to streamline and clarify rules on police collection, use and retention of data for biometrics in order to improve transparency and public safety'? Please explain your answer, providing supporting evidence where possible.

94. Liberty is concerned that the proposal to 'streamline and clarify' framework governing the collection, use and retention of biometric data by the police is a euphemism for reducing legal protections for individuals and their personal data. The primary consideration for the Government must be to ensure that the legal framework governing the use of biometric data is compatible with the rights of individuals; the key questions being whether the laws and policies are adequately prescribed by law, necessary, and a proportionate means of achieving a legitimate aim. A further consideration must be whether the use, collection or retention of biometric data will result in unlawful discrimination. We note that the Information Commissioner's response to this consultation states that it is imperative not to weaken the data protection regimes for policing or intelligence services, and we endorse that position.

95. Further, in respect of the use of facial recognition technology as a tool dependent on the collection of biometric data, our view is that no legal framework could legitimise its use. The Consultation Document states that facial recognition technology is an increasingly important tool in tackling crime. As we have set out in detail above, in Liberty's view, FRT poses significant risks to individuals and society, and can never be lawfully or ethically deployed in public spaces.

96. The use of FRT in public spaces is a significant infringement of privacy for every individual in the vicinity of a camera. The use of this technology exacerbates existing disproportionate policing practices, including the use of stop and search powers on Black people, and the collection, retention and sharing of data through the Gangs Matrix. More widely, the removal of individuals' autonomy over when and how to disclose their identity fundamentally alters the relationship between individuals and the State and normalises authoritarian surveillance. Liberty believes that the use of FRT, whether used by the police or private companies, should be prohibited entirely.

[163] Edwards, L. and Veale, M., *Slave to the algorithm? Why a 'right to an explanation' is probably not the remdy you are looking for,* Duke Law and Technology Review, 2017, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855

97. In respect of other policing tools which rely on the collection, retention and use of biometric data,[164] Liberty notes that just because technology may be deemed to be useful for law enforcement and the detection and prevention of crime, does not provide sufficient justification in and of itself. Indeed, it is often precisely because certain technologies are particularly intrusive and oppressive that they are 'useful' for law enforcement. The 'flexibility' which the Government claims to be desirable must take a backseat to the rights and freedoms of the individuals whose data is being collected. For example, in the case of *S and Marper v UK* it was held that while a national DNA database would be extremely helpful for the police, it was disproportionate and unlawful.

98. Finally, we note with concern the Government's stated ambition to "align more closely the commercial, law enforcement and national security processing frameworks".[165] It is self-evident that the collection and use of biometric data by the State poses different and more harmful implications for individuals. If the Government chooses to pursue this goal, commercial frameworks must be designed to be as rigorous and compliant with human rights standards as law enforcement and national security framework, and must not create a system that weakens protection for all.

Further questions

Q4.6.1

In your view, which, if any, of the proposals in the chapter on 'Delivering better public services' would impact on people who identify with the protected characteristics under the Equality Act 2010 (i.e. age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation)?

99. We believe that each of the proposals that we have responded to above will have impacts on people who identify with the protected characteristics under the Equality Act 2010. As above, we would expect a robust EIA to be undertaken in advance of any further legislative progress on these proposals. In particular, the proposals to enable processing of health data when necessary for reasons of substantial public interest in relation to public health or other emergencies may deter people from accessing health services, with a particularly disproportionate impact on migrant and minoritised communities. As mentioned above, depending on what form transparency reporting takes, we are concerned that people with protected characteristics may experience excessive – and therefore disproportionate – processing of their data, particularly given the fact that certain communities are more likely to access public services or interact with State institutions, such as the police and criminal justice

[164] Wangari-Jones, P., Loyola-Hernández, L., and Humphris, R. (2021) *STOP THE SCAN: Police use of mobile fingerprinting technology for immigration enforcement*, UK. Racial Justice Network and Yorkshire Resists, available at: https://racialjusticenetwork277579038.files.wordpress.com/2021/06/stop-the-scan-report.pdf

[165] Pg. 111, Data: A new direction

system. Finally, we are highly concerned that any expansion of police powers to collect, use, and retain biometric data will have a disproportionate impact on already-overpoliced communities, including and especially communities of colour.

CHAPTER 5: REFORM OF THE INFORMATION COMMISSIONER'S OFFICE

Public safety duty

Q5.2.10.

To what extent do you agree with the Government's proposal to introduce specific language recognising the need for the ICO to have due regard to public safety when discharging its functions? Please explain your answer and provide supporting evidence where possible.

100. **Liberty strongly disagrees with this proposal.** We note first that this proposal is difficult to meaningfully respond to since the Government has not suggested a definition for "public safety" in the consultation document. Should the Government wish to pursue this proposal further, it should set out what it means by "public safety" in this context, and should seek out the views of stakeholders when it has determined its definition. Liberty notes that the protection of data/privacy rights by the ICO, i.e. its core functions, is a fundamental part of promoting public safety. We are more safe when our privacy is upheld.

101. The proposed new statutory duty[166] is at best unnecessary, and at worst an attempt to weaken vital data protection. We note that, in respect of public safety, the ICO already works to support the "appropriate and responsible sharing of data".[167] Indeed, the ICO's data sharing code,[168] for example, sets out the situations in which organisations can share data in an emergency. This includes situations where data sharing is necessary for the protection of public health and where there is an immediate need to protect national security.[169] It also includes the prevention of serious physical harm to a person and the loss of human life.[170] A new statutory duty, whose purpose and impact is unclear, is unnecessary. Indeed, the Government acknowledges that the introduction of this duty would be "to reiterate an important factor that already exists".[171] The need for such reiteration is not apparent.

102. Without further explanation, it appears that the Government's purpose in introducing this new statutory duty is to inappropriately weaken individuals'

[166] Pg 121, para 343, *Data: A new direction.*
[167] Pg 10, ICO, *Response to DCMS Consultation "Data: a new direction"*, 6 October 2021, available at: https://ico.org.uk/media/about-the-ico/consultation-responses/4018588/dcms-consultation-response-20211006.pdf
[168] ICO, *Data sharing code of practice*, 17 December 2020, available at: https://ico.org.uk/media/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice-1-0.pdf
[169] Pg 66, ICO, *Data sharing code of practice*, 17 December 2020, available at: https://ico.org.uk/media/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice-1-0.pdf
[170] Ibid.
[171] Para 343, pg 121, *Data: A new direction.*

data/privacy rights and/or the regulatory oversight of the ICO to help individuals enforce those rights. Indeed, there is no evidence to suggest that the balancing exercise already carried out by the ICO in respect of public safety and individuals' data/privacy rights results in unmanageable threats to public safety. It is therefore unclear how this new duty would operate or change current practice, and there is no case for it.

103. The ICO is a body with an extremely wide and important remit. Data is now ubiquitous throughout all sectors of private sector and state activity. Accompanying that ubiquity and increasing value of data as a commodity are growing opportunities for the unlawful exploitation of data and private information, and greater risks of data loss and data breaches. All have become more common and frequently affect the rights of very large numbers of people. The ICO is already facing a significant strain on its resources and capacity to carry out its core functions. Introducing a new statutory duty, and the associated administrative burden of evidencing compliance with that duty, would detract from the ICO's ability to focus on those core functions. The Government notes in its consultation document that this new duty "would not supersede the ICO's overarching objective"; while that might be true as an intention, the realities of evidencing compliance with the duty might very well undermine the ICO's ability to achieve that objective. Rather than introducing an unnecessary new duty, the Government should focus on better equipping the ICO with the staff and resources it needs to carry out its essential core functions.

Governance Model and Leadership

Q.5.3.4

To what extent do you agree with the use of the Public Appointment process for the new CEO of the ICO?

104. **Liberty strongly disagrees with this proposal**. We echo the concerns of the IC that "the current proposals for the Secretary of State to approve ICO guidance and to appoint the CEO do not sufficiently safeguard this independence".[172]

Setting the Information Commissioner's salary

Q5.3.5.

To what extent do you agree that the salary for the Information Commissioner (i.e. the proposed chair of the ICO in the future governance model) should not require Parliamentary approval?

105. **Liberty strongly disagrees with this proposal**, which would enable the Secretary of State for DCMS to amend the IC's salary. We believe this suggestion –

[172] Pg. 23, ICO, *Response to DCMS consultation "Data: A new direction",* 6 October 2021, available at: https://ico.org.uk/media/about-the-ico/consultation-responses/4018588/dcms-consultation-response-20211006.pdf

combined with DCMS's proposal to appoint the CEO – is highly likely to undermine the independence and integrity of this office (or at the very least give the appearance of this, which itself will cause harm).

Independent review

Q5.4.6.

To what extent do you agree with the proposal to empower the DCMS Secretary of State to initiate an independent review of the ICO's activities and performance? Please explain your answer, and provide supporting evidence where possible.

106. **Liberty strongly disagrees with this proposal.** We are concerned that this suggestion risks undermining the independence of the ICO. The IC has noted that "clarification of this being a 'last resort' and the intention to introduce criteria for triggering a review are welcome, reducing the risk to the principle of independence".[173]

Codes of Practice and Guidance

Q.5.5.3

To what extent do you agree with the proposal to give the Secretary of State a parallel provision to that afforded to Houses of Parliament in Section 125(3) of the Data Protection Act 2018 in the approval of codes of practice, and complex and novel guidance? Please explain your answer, and provide supporting evidence where possible.

107. **Liberty strongly disagrees with this proposal, which in the IC's words "effectively amount to the right of veto for government over key pieces of guidance".[174]** It is important to note that there already exist obligations on the ICO to consult with the Secretary of State in the preparation of statutory codes of practice, and the Secretary of State must lay such codes before parliament for approval. The IC has commented that this proposal "would reduce regulatory certainty for organisations and wider trust and confidence in the ICO's guidance".[175] In our view, giving the Government a veto power over the ICO's codes of practice will undermine its independence and potentially hinder its work as regulator, for example its ability to effectively scrutinise Government proposals that impact on people's data rights. We are concerned that the Government's attempt to bookend the production of codes of practice by an ostensibly independent regulator is an attempt to insulate itself from challenge.[176] At the very least, there is clear appearance of ICO non-

[173] Pg. 84, ICO, *Response to DCMS consultation "Data: A new direction",* 6 October 2021, available at: https://ico.org.uk/media/about-the-ico/consultation-responses/4018588/dcms-consultation-response-20211006.pdf
[174] Pg. 85, ICO, *Response to DCMS consultation "Data: A new direction",* 6 October 2021, available at: https://ico.org.uk/media/about-the-ico/consultation-responses/4018588/dcms-consultation-response-20211006.pdf
[175] Pg. 22, ICO, *Response to DCMS consultation "Data: A new direction",* 6 October 2021, available at: https://ico.org.uk/media/about-the-ico/consultation-responses/4018588/dcms-consultation-response-20211006.pdf
[176] In the ICO's words: "[T]his proposal also reduces the ability of government to effectively hold the ICO to account. We expect and need government to maintain the ability to hold independent regulators to account for the consequences of

independence and a conflict of interest in one of the bodies overseen by the ICO controlling the ICO that should be avoided if the public is to have confidence in the functioning of the ICO.

Biometrics Commissioner and Surveillance Camera Commissioner

Q5.8.1.

To what extent do you agree that the oversight framework for the police's use of biometrics and overt surveillance, which currently includes the Biometrics Commissioner, the Surveillance Camera Commissioner and the ICO, could be simplified? Please explain your answer, and provide supporting evidence where possible.

108. **Liberty somewhat disagrees with this proposal.** As a preliminary point, we believe that the drafting of the question should have been framed in normative terms. The oversight framework could, of course, be simplified by the absorption of the roles of the Biometrics Commissioner (BC) and Surveillance Camera Commissioner (SCC) into the ICO as suggested by the consultation document.[177] However, this question does not invite answers which explore whether simplification of the framework *should* occur. If the question had been framed in normative terms, this would have likely engaged a much more meaningful discussion about the pros and cons of the current oversight framework.

109. Beyond our issues with the framing of the question, we are extremely concerned about the apparent intention of the Government in this proposal to dilute important oversight currently conducted by different regulatory bodies separately. Liberty was likewise concerned by the appointment of one individual to the positions of both BC and SCC in March 2021, indicating as it did a devaluing of the expertise and role offered by both offices in overseeing different aspects of overt surveillance. At a time when private companies and state bodies are rapidly expanding their surveillance capabilities, regulatory bodies must be supported and enhanced in their powers and resources, not weakened. Not only do the officers of the BC, SCC and IC offer different and specific expertise, which would be lost in merging them further, they also have extremely wide remits and heavy workloads[178] (see our response to Q5.2.10 on the ICO's wide remit). Further absorption of the functions from one into another is highly likely to overburden and significantly reduce the effectiveness of

---

the products they produce and decisions they take. This is made more challenging if government is the final approver of the guidance and products which establish the standards of legal compliance and regulatory certainty for stakeholders." See Pg. 23, ICO, *Response to DCMS consultation "Data: A new direction",* 6 October 2021, available at: https://ico.org.uk/media/about-the-ico/consultation-responses/4018588/dcms-consultation-response-20211006.pdf

[177] Pg. 141, paras 409-410, *Data: A new direction.*

[178] Open Democracy recently found that the ICO were "backsliding" in respect of dealing with complaints – e.g. in 2016, 66% of complaints were resolved within 180 days; however, by 2020, only 37% of complaints were resolved within the same time frame: Open Democracy, 'Art of Darkness: How the government is undermining Freedom of Information'(November 2020), pg 21. This is a significant departure from the statutory 20 working-day deadline (S.10(1), Freedom of Information Act 2000), suggesting that the ICO is already struggling to keep up with the demands of its existing functions.

these already overstretched bodies. This is clearly harmful in and of itself but will also undermine public trust in the ability of these bodies to carry out their functions and protect the public's rights. The Government notes in the consultation document that absorbing functions into the ICO will "bring benefits…with a single route for advice, guidance and redress";[179] however none of these benefits will manifest if the ICO is overrun and cannot perform its functions.

110. Notwithstanding the above, we agree that there are elements of the current oversight framework which could be simplified, in the sense of clarification of responsibilities but not reduction of those responsibilities. We agree with the current Biometrics and Surveillance Camera Commissioner (BSCC) that there is potential for streamlining some of the existing arrangements between the offices of the BC, SCC and IC, for example in how they work together on data protection matters involving the use of surveillance camera technology and in producing guidance like the Surveillance Camera Code.[180] There is potential in such co-working for it to be unclear as to who is responsible for what. For instance, there was some uncertainty over the last few years as to who was responsible between the BC, SCC and IC in overseeing what aspects of the deployment of LFR. Clarity over responsibilities is important to avoid not only for the functioning of the oversight framework itself, but also for public confidence in the framework. The Government should be led by the regulatory bodies as to what clarification is required and how to achieve that.

Q.5.8.2

To what extent do you agree that the functions of the Biometrics Commissioner and the Surveillance Camera Commissioner should be absorbed under a single oversight function exercised by the ICO? Please explain your answer, and provide supporting evidence where possible.

111. **Liberty strongly disagrees with this proposal.** See our answer to Q5.8.1 above. In addition, we make the following points.

112. The functions of the BC and SCC go far beyond the remit of data protection, and are therefore not best served by absorption into the ICO, whose staff and structure is not set up for carrying out such functions. By way of summary, the functions of each entity are noted below:
    - The ICO has a regulatory function and is responsible for upholding the information rights contained within the Freedom of Information Act 2000, the

[179] Pg. 141, para 410, *Data: A new direction.*
[180] Pg. 15, para 9.8, Biometrics and Surveillance Camera Commissioner, *DCMS Consultation: "Data: A new direction" – Response by the Biometrics and Surveillance Camera Commissioner*, 2 November 2021, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1030248/BSCC_DCMS_Consultation_Response.pdf

Environmental Information Regulations 2004, the Data Protection Act 2018 and the Privacy and Electronic Communications (EC Directive) Regulations 2003.[181]

- The BC has quasi-judicial functions covering police retention and use of DNA and fingerprints.[182]
- The SCC has a more strategic role and is responsible for providing oversight of the surveillance of public space by the police and local authorities.[183]

113. Further, while the need to ensure lawful processing of personal data underpins the functions of all three entities, the legal framework governing biometrics and surveillance goes much further than data protection, requiring specific safeguards, accountability mechanisms and governance frameworks.[184] This is because the personal data collected by the police is often gathered by deliberately and necessarily intrusive tools, tactics and techniques.[185] Such measures pose a significant threat to our fundamental rights and freedoms. Therefore, we argue that the absorption of the roles of BC and SCC into the ICO is flawed – it not only misunderstands the specific and specialised nature of the BC and SCC's functions, but also the importance of those functions in protecting fundamental rights.

114. Finally, we echo the views of the BSCC that absorbing the functions of:

- the BC into the ICO is flawed as it would require the ICO to carry out the non-regulatory judicial functions previously held by the BC. This may also lead to a situation where the ICO authorises police retention of biometrics and an individual, hoping to challenge such authorisation, is unable to turn to the ICO, as a separate regulator, to uphold their information rights;[186] and
- the SCC into the ICO would, if the consultation document's proposals to reconstitute the ICO are fully implemented and the IC's independent status replaced, dilute some of the current advantages and safeguards of the current oversight framework.[187]

[181] Pg. 4, ICO, *A Guide to the Legislation the ICO Regulates: Upholding Information Rights For All*, August 2012, available at: https://ico.org.uk/media/1042840/upholding_information_rights_for_all.pdf
[182] *Policy Paper: Press Release*, 2 November 2021, available at: https://www.gov.uk/government/publications/data-a-new-direction-commissioners-response/press-release
[183] Ibid.
[184] Pg. 8, para 6.5, Ibid.
[185] Pg. 3, para 3.4, Ibid.
[186] Pg. 13, para 9.2, Ibid.
[187] Pg. 15, para 9.9.