BIG BROTHER WATCH

DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

SUBMISSION TO THE UN SPECIAL RAPPORTEUR ON EXTREME POVERTY AND HUMAN RIGHTS AHEAD OF UK VISIT NOVEMBER 2018

Dear Professor Philip Alston,

I am writing to you on behalf of Big Brother Watch, a non-profit campaign organisation leading the protection of civil liberties in the UK at a time of great technological change. We welcome your UK visit, and I am very grateful for the opportunity to make a written submission to you in advance.

In this submission, I specifically wish to address the matter of new technologies in the welfare system. We are concerned that the use of new technologies are engaging human rights in ways that are difficult to assess due to a concerning lack of transparency and ineffective legal protections, and that this could negatively impact the UK's poorest people.

Big Brother Watch's work on new technologies and welfare

In the course of our work protecting rights, we use research, investigations, and legal and policy analysis to identify practices that enact prejudice - especially where those practices are systemically embedded in public authorities. We seek to engage stakeholders and decision makers to achieve change to practice and policy.

We are aware that local authorities are rapidly adopting new software to conduct automated processing and even predictive analytics, particularly for use in the complex fields of welfare and social care. Whilst this shift is often attributed to

the climate of austerity, we have not yet found conclusive evidence of money saving. There is undoubtedly a tidal wave of technological solutionism also driving this shift.

Human rights issues and opaque technologies in welfare

The UK's welfare state reflects principles that are at the heart of human rights frameworks: fairness, equality and the duty of the state to ensure all of its citizens, regardless of sex, race, age, ability or disability, enjoy a minimum standard of living.

In practice, the UK's welfare system touches on a spectrum of rights: the right to life, the right to health, the right to be free from inhuman or degrading treatment, freedom from discrimination, the right to education, the rights of children, the right to fair work, access to justice, and the right to peaceful enjoyment of property.

In the context of welfare estimations and decisions, the stakes could not be higher. This myriad of rights is engaged and people's lives, health and social integration are often at risk.

Therefore, decision-making in this context should be transparent, comprehendible to officials and claimants, and challengeable - not just for highly trained lawyers, but for disadvantaged and vulnerable people. Moreover, according to both ethics and the law, those decisions must be human decisions. However, we believe that some decisions may be automated and given merely administrative sign-off by staff. The transparency, accessibility and contestabilty of decision-making processes appears to be largely obstructed by the adoption of new technologies. Claimants already have to deal with a frequently changing and punitive assessment process[1] - now they are being affected by complex

1 For example: https://www.theguardian.com/commentisfree/2016/jun/07/pip-disaster-disabled-access-report-benefits

technological systems they rarely know about, cannot understand, and are not able to challenge.

Human decisions for human rights

We must not ignore the great potential of new technologies to benefit society – but not must we turn a blind eye to the risks they pose.

We believe that where human rights would be engaged by automated decisions, those decisions should ultimately be human decisions. That also means that the human involvement in decision-making that involves automated processing should be meaningful.

GDPR

Fortunately, the GDPR clarifies and extends safeguards for individuals against significant decisions based solely on automated processing.[2]

Article 22(1) of the GDPR provides that:

> *"**Automated individual decision-making, including profiling***
> *"1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her".*[3]

Article 22(2)(b) of the GDPR allows Member States to create certain exemptions from this right, as long as "*the data subject's rights, freedoms and legitimate interests*" are safeguarded.

---

2 GDPR, Article 22

3 GDPR, Article 22(1)

Automated decisions under the Data Protection Act 2018

However, the UK's Data Protection Act 2018 fails to provide sufficient safeguards for data subjects' rights where it makes exemptions from this important GDPR right in section 14.

Section 14 of the Data Protection Act 2018 permits purely automated decisions with legal or similar significant effects to be made about a subject, in absence of the subject's consent – so long as the subject is notified that the decision was purely automated after the fact. The subject is then to be afforded just one month to request a new decision if they wish.

During the passage of the (then) Data Protection Bill 2018, we lobbied for a safeguard to this exemption that would prevent purely automated decisions with legal or similar significant effects from being made where those decisions would engage the subject's human rights as protected by the Human Rights Act 1998. This would have ensured procedural fairness and provided much needed protection against discriminatory decisions – issues that have become increasingly prevalent alongside the growing use of automated or algorithmic systems.

There are some chilling case studies of such discriminatory decisions from the US. For example, an automated benefits system[4] in the US resulted in a million benefits applications being denied over a three year period – a 54% increase from the three years before. It often blamed its own mistakes on claimants' "failure to co-operate". One such claimant was a woman suffering ovarian cancer.[5] Without welfare, she lost the ability to pay for her medication, her transport to medical appointments, and even her rent. She died the day before she won her appeal against the system.

---

4 https://www.npr.org/sections/alltechconsidered/2018/02/19/586387119/automating-inequality-algorithms-in-public-services-often-fail-the-most-vulnerab

5 https://www.npr.org/sections/alltechconsidered/2018/02/19/586387119/automating-inequality-algorithms-in-public-services-often-fail-the-most-vulnerab

The Data Protection Bill amendments we supported received great traction in parliament but regrettably were rejected by Government.

Humans administrating automated decisions

We are not aware of individuals being notified of purely automated decisions by local authorities in relation to welfare or social care.

This is likely because under section 14 of the Data Protection Act 2018, automated decisions that have significant legal or similar effects on a subject are not necessarily classified as "purely automated" if a human has administrative input. For example, if a human merely ticks to accept and thus enact a serious automated decision, the decision would not need to be classified as "purely automated" under law and as such, the minimal safeguards of notification and re-evaluation would not even apply.

This means that welfare decisions could be being made that are for all intents and purposes automated decisions, without individuals being notified of this fact or their right to appeal.

We raised concerns about this during the passage of the (then) Data Protection Bill 2018, which were echoed by the Deputy Counsel to the Joint Committee on Human Rights who said, "*There may be decisions taken with minimal human input that remain de facto determined by an automated process*".[6]

Clearly, the Act does not sufficiently protect against a situation where the human involvement is so minimal as to be meaningless. Even the most minimal human input or token gesture lacking any influence over the decision could authorise an automated decision that has a significant legal effect whilst circumventing safeguards.

---

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

There is no wording in the Data Protection Act 2018 to define what constitutes an automated decision. We lobbied for an amendment to the Bill to address this issue that, similarly, received traction in parliament but was rejected by Government. The Minister Baroness Williams made reference to Recital 71 of the GDPR, which she said "*already provides for this* [safeguard]", satisfying the Government that there is no need to make further clarification explicit in the Bill.[7] However, Recital 71 only states that automated decisions are those "*without any human intervention*"[8] – not those without *meaningful* intervention, which is a vital clarification needed if this were to constitute a safeguard. The Government's resistance to this simple amendment concerned us.

Digital Economy Act 2017

Part 5, Chapter 1 of the Digital Economy Act 2017 permits mass data sharing between public authorities and private companies for the improvement or targeting of a public service or benefit provided to individuals or households. Government provided a factsheet during the passage of the (then) Bill that explicitly stated that such data sharing could be conducted to "identify families in need of help" from the Troubled Families Programme.[9]

Whilst ensuring access to state benefits is a worthy aim, it must be pursued in a proportionate manner and in accordance with data protection law. Critically, this Act lacks provisions for consent, access to one's data, knowledge of where one's data is held or how and by whom it is used, or indeed any framework for transparency around the data sharing agreements that are made. Furthermore, using bulk data to "identify" and intervene in the lives of "troubled families" arguably amounts to profiling and risks breaching Chapter 3 GDPR.

---

7 Baroness Williams of Trafford in Data Protection Bill, Report stage, 2nd day, 13 December (https://hansard.parliament.uk/lords/2017-12-13/debates/9622571E-8F1E-43F8-B018-C409A3129553/DataProtectionBill(HL))

8 GDPR, Recital 71 (emphasis added)

9 **Digital Economy Bill Factsheet: Better Public Services, Department of Culture, Media and Sport**

Nevertheless, the purposes for which data can be shared, as written into this Act, extend to improving "their physical and mental health", "emotional well-being", "the contribution made by them to society", and "their social and economic well-being". Although well-intended, these incredibly permissive purposes for data sharing enable a new form of intrusion on the private lives of those who are most vulnerable. Data sharing to evaluate and improve the "contribution" one makes to society plainly risks amplifying the punitive potential of some welfare sanctions, such as work schemes that have adversely impacted those with disabilities and ill health.[10]

Section 41 of the Digital Economy Act further extends the applications of data sharing within and between the state and private companies. Other than fulfilling the purposes for which the data was ostensibly shared, information can be used to prevent or detect crime or anti-social behaviour, for criminal investigations, for legal proceedings, for "safeguarding vulnerable adults and children", for HMRC purposes, or as required by EU obligations. In effect, personal data could be shared across government departments to investigate, penalise or otherwise intrude on the lives of those in receipt of welfare, pensioners, and some of the country's most vulnerable people. This section negates the claim that data sharing is only permitted for individuals' benefit and reveals potential applications for administrative and policing purposes.

It is unacceptable that the Act does not provide adequate safeguards or transparency mechanisms around data sharing between authorities and/or service providers. Vulnerable citizens are not be afforded an opportunity to consent to their data being shared or accessed and have no way of knowing exactly how, when or why their personal information is being used.

10 https://www.theguardian.com/society/2015/aug/24/benefits-shakeup-aims-to-force-more-disabled-peopleinto-jobs and https://www.theguardian.com/society/2015/aug/27/thousands-died-after-fit-for-work-assessment-dwpfigures

Risk Based Verification

Risk Based Verification (RBV) was introduced in 2011 as an alternative verification process for claimants' benefits entitlements to the vague requirements set out previously.

Central policy in this area is out-dated. The Department for Work and Pensions' guidance manual for councils on RBV for housing and council tax benefit claims dates to 2011, before the advent of most of the modern algorithmic tools now in use.[11] The guidance states that local authorities using RBV must develop their own policies – but that these should be shielded from the public:

> *"The information held in the Policy, which would include the risk categories, should not be made public due to the sensitivity of its contents."*[12]

We are concerned about this devolution of responsibility and the additional lack of transparency. In one council's risk assessment, it is clear that the evaluation of the potential impact of RBV tools is highly limited. York Council reported "no implications" were involved for "equalities", "property" or "legal" issues. In fact, the council asserted that the "key risk" associated with RBV is:

> *"ensuring that staff receive appropriate training to ensure they trust the risk scores and process the claims correctly to deliver efficiencies".*[13]

The fact that the council is primarily concerned with ensuring that staff trust the risk scores exposes the reality that many of the algorithmic and automated tools

---

11 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/633018/s11-2011.pdf

12 Para 14, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/633018/s11-2011.pdf

13 http://democracy.york.gov.uk/documents/s99616/Report.pdf

emerging in the welfare system are decisive rather than merely advisory. In practice, very few staff members will challenge the recommendations of seemingly sophisticated algorithmic tools.

New technologies in the welfare system

There is a distinct lack of transparency around authorities' precise uses of algorithms and new technologies in decision-making, both in central government and local authorities. As such, we do not know exactly what use authorities make of new technologies in the context of decision-making in the welfare system. This, in itself, is a problem.

As you identified in your call for submissions, there is no mechanism in place for reporting the use of algorithms for public purposes, despite the UK claiming the place of a world leader in technology innovation. Furthermore, our legal frameworks fail to require that vital transparency and in fact enable the use of automated decisions that may well have negative human rights implications – and worse still, with the ability to circumvent the minimal safeguards that do exist by involving tokenistic human involvement.

Our Freedom of Information project

At the present time, the main route for us to attempt to gain insight into authorities' uses of new technologies in decision-making is via requests for information made under the Freedom of Information Act 2000. This is a burdensome process that is obstructive of effective transparency and accountability.

Big Brother Watch started a national freedom of information (FOI) campaign in the summer of this year, asking every local authority in the UK (418 in total) for information about their uses of artificial intelligence (AI), algorithms and automated decision-making tools in the provision of their services. We continue

to process the responses and have sent many hundreds of follow-up requests in attempt to gain further clarity.

The obstacles to gaining clear and accurate information via this route have been many. The following information is based on our preliminary findings. More detailed explanations of specific technologies are provided in Appendix I.

Defining and understanding technologies

A major obstacle in this route of information discovery is that many information officers handling FOI requests appeared not to be familiar with the practice or even the concept of automated decisions. We received many replies asking for definitions of AI, algorithms and automated decision-making.

Reluctance to share information

Some authorities replied telling us that they had no relevant information to disclose – and some of those authorities, we later discovered through other means (e.g. journalism), are indeed using those technologies in their provision of social care and/or welfare. This was, in many cases, despite us providing definitions of these new technologies.

We reviewed the wording of our FOI requests carefully and have concluded that the incorrect responses we received are likely either due to information officers' enduring misunderstanding or lack of knowledge as to the existence or concept of the new technologies in use, or simply due to a reluctance to thoroughly disclose information.

High levels of data integration

The systems in use are likely to be complex, which may frustrate accurate disclosure via FOI. Holistic data management systems may involve multiple

departments, making no one departmental responder able to disclose the full functions of a system.

Agnosticism towards technological functions and impact

The vast majority of new technological applications we have discovered in use by authorities is proprietary, sourced from private companies. This means that the public sector staff working with the tools may not fully understand their inner workings.

We have experienced a high degree of agnosticism within authorities towards the machinations of the technologies they use, sometimes with a wilful blindness to the data fields ingested by the tools, and frequently with apathy towards their socio-economic and human rights impact. Such software appears to be perceived as merely administrative. However, the administration of welfare and social care can have enormous impact and so any changes must be carefully considered and analysed. Where we have requested copies of equality impact assessments and privacy impact assessments we often find that no such impact has been assessed at all.

Human rights are engaged in complex ways by new and emerging technologies. The impact must be assessed – but vital scrutiny is currently obstructed by an unacceptable opacity on the part of the authorities who use these technologies, and legal frameworks that fail to protect rights in the context of this technological revolution.

I sincerely hope that you are able to gain further insight into the relationship between poverty, human rights, and authorities' uses of new technologies during your official visit. Should you require any further information from us, please do not hesitate to contact me.

Yours sincerely,

Silkie Carlo

Director, Big Brother Watch

BIG BROTHER WATCH

DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY