LIBERTY

PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

Liberty's Submission to the Science and Technology Committee's Inquiry into Algorithms in Decision-Making

April 2017

About Liberty

Liberty (The National Council for Civil Liberties) is one of the UK's leading civil liberties and human rights organisations. Liberty works to promote human rights and protect civil liberties through a combination of test case litigation, lobbying, campaigning and research.

Liberty Policy

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
http://www.liberty-human-rights.org.uk/policy/

Contact

Silkie Carlo
Policy Officer (Technology & Surveillance)
Direct Line 020 7378 5255
Email: silkiec@liberty-human-rights.org.uk

Rachel Robinson
Policy Officer
Direct Line: 020 7378 3659
Email: rachelr@liberty-human-rights.org.uk

Sam Hawke
Policy Assistant
Direct Line 020 7378 5258
Email: samuelh@liberty-human-rights.org.uk

1. Liberty welcomes the opportunity to provide a written submission to the Science and Technology Committee's inquiry into the use of algorithms in decision-making. We thank the Committee for launching this important and timely inquiry, which touches on novel issues that are of increasing relevance to the upholding of human rights, and of great interest to Liberty.

2. Liberty advises that:

    - The use of algorithms in the public sector could lead to discriminatory policing and intelligence, behavioural influence, and large-scale invasions of privacy;

    - The use of algorithms to make decisions in the private sector could lead to discrimination in areas such as hiring and employment, access to services and finance, differential pricing, and more;

    - The increasing trend of using algorithms in decision-making may pressurise individuals and services into sacrificing privacy, and could further deteriorate attitudes towards the right to respect for a private life.

Algorithms in the public sector

3. One of Liberty's greatest areas of concern is the use of algorithms for policing and intelligence in the UK, as there is considerable potential for abuses of rights to occur, and to do so in secrecy.

4. The passage of bulk surveillance powers into law, via the Investigatory Powers Act 2016 (IPA), indicates that algorithms are used extensively by the security and intelligence agencies to analyse the public and citizens' communications. The 'surveillance first' approach, collecting and processing the communications and data of many millions of people, could only be worthwhile with the deployment of advanced algorithmic processing to monitor known targets and indeed to discover new ones, as per the Government's expressed aims for the powers.[1] The controversial approach of requiring all the 'haystack' to find a 'needle', reversing the traditional relationship between suspicion and surveillance in which suspicion must come first, essentially refers to aspirations for the computational potential of algorithmic processing.

[1] *Draft Investigatory Powers Bill 2015: Guide to Powers and Safeguards*, p.20 para. 33

5. Liberty is concerned that the notion of reasonable suspicion is being critically subverted in the age of big data and corresponding algorithmic processing. Whereas suspicion has traditionally been based on observable and relevant 'data', it can now be generated from masses of 'unseen' data. Our phones record where we go and who we speak to; ANPR cameras can track our cars; social media sites record what we think and how we feel; our bank cards record a great amount of our activity; smart meters even record when we are home and how much energy we use; and now voice activated 'intelligent personal assistants' like Amazon's Alexa record activity from inside the family home. With powers allowing much of this data to be available to the State, suspicion can now be generated from comprehensive digital footprints rather than from a careful assessment of relevant evidence. Liberty is particularly concerned about the use of algorithms to ingest personal data for 'target discovery' – that is, to find new suspects. This approach appears to employ algorithms to passively analyse data, treating all citizens as suspects until proven otherwise.

6. Wide-scale suspicionless surveillance is based on what will often be circumstantial factors. It follows that algorithmic judgements of suspicion derived from amalgamated data rather than observable actions will be increasingly predictive in nature.

7. It has been argued that such algorithmic decisions are, or will one day be, more accurate than traditional human observations, helping to reduce the discrimination and error inherent in 'instinct'. On the other hand, some scholars have cautioned that:

> "*Without the requirement of some observable activity, the odds increase that predictive stops will target innocent people, criminalize by association, and negatively impact individuals based on little more than a hunch supported by non-criminal facts."*[2]

A serious question to be asked is whether putting indiscriminately collected, bulk data in the State's hands for algorithmic processing is and could ever be compliant with human rights law, or indeed healthy in a democracy. Regardless of the accuracy of such algorithmic processing, Liberty's view is that it is not.

[2] *Big Data and Predictive Reasonable Suspicion* – A. G. Ferguson, January 2015, p.387

8. We are concerned that discriminatory biases that have traditionally been risked in human decision-making in policing and surveillance will be transmitted to algorithmic decision-making – only, in the context of such voluminous data and complex analytics, with many more vectors by which discrimination can occur, with more subtlety and with less direct accountability. Such discriminatory biases may interfere with religious and political freedoms, or involve racial, ethnic, age, gender, disability, and socio-economic discrimination and risk contravening a number of rights protected by the Human Rights Act (HRA) as well as the Equality Act.

9. There is evidence that data science has additionally perpetuated discrimination in the criminal justice system in the US. A recidivism algorithm called COMPAS (Correctional Offender Management Profiling for Alternative Sanctions, by Northpointe, Inc.) was found to be twice as likely to incorrectly judge black defendants as at high risk of reoffending than white defendants.[3] This is despite race not being one of the categories of information ingested. Since this is proprietary software, we cannot know exactly how or why the algorithm came to these conclusions. Such decision-making should be challengeable and subject to an adversarial court proceeding - this opaque application of algorithmic decision-making is discriminatory and highly inappropriate.

10. Test datasets, or in fact any data collected from society, may be reflective of patterns of discrimination and existing inequalities: *"to the extent that society contains inequality, exclusion or other traces of discrimination, so too will the data"*.[4] Social data come with complex histories, which may silently haunt the logic underpinning social policy if uncritically used. We must be cautious that *"algorithmic vision derives authority from its association with science (…) an aura of neutrality and objectivity, which can be used to defend against the critique that they carry any social prejudice."* [5] In fact, patterns of social inequalities can be perpetuated through algorithmic processes, which may have significant legal effects on individuals in the context of law enforcement.

[3] *Machine Bias* - Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, ProPublica, May 23, 2016
[4] *European Union regulations on algorithmic decision-making and a "right to explanation"* – B. Goodman, S. Flaxman, Aug 2016, p.3
[5] *Algorithmic paranoia and the convivial alternative* – Dan McQuillan, Big Data & Society, July-December 2016, p.4

11. We are unaware of any formal processes for the independent oversight of the algorithms used by the intelligence community. We strongly believe that there should be independent oversight of the mechanisms and operation of algorithms in any context that results in legal and other significant effects.

12. Algorithmic processing is increasingly used in law enforcement. The availability of new data sources including social media data, biometrics and facial recognition software creates opportunities for concerning interferences with the right to privacy at an individual and social level.

13. As the Department for Business, Innovation and Skills and the Department for Culture, Media and Sport previously described to the Committee, by analysing 800 million monthly credit and debit card payments and matching these with other datasets, HMRC has been able to "*more effectively target tax enforcement activity*".[6] Whilst a legitimate aim by law enforcement, this scale of data analysis constitutes an extraordinary interference with innocent people's right to respect for a private and family life as protected by article 8 HRA. It is important to apply a human rights analysis to these new trends in data analysis, which requires that any privacy infringement must be necessary and proportionate rather than merely useful.

14. Liberty is also concerned about the possibility of wider algorithmic processing for public service delivery, as indicated by powers proposed in the Digital Economy Bill, which is currently going through Parliament.

15. The Digital Economy Bill contains clauses that would permit mass data sharing across public authorities and private companies such as utilities suppliers for extremely broad aims to "*improve public services through better use of data*"[7], or indeed to improve individuals' "*physical and mental health*", "*emotional well-being*", "*the contribution made by them to society*", and "*their social and economic well-being*".[8] An example provided in the accompanying factsheet is to "*identify families in need of help*" from the Troubled Families Programme – potentially using algorithmic processes – which seeks to "*put adults in*

[6] Joint written evidence submitted by the Department for Business, Innovation and Skills, and the Department for Culture Media & Sport (BIG0069), for the Science and Technology Committee's 'Big Data Dilemma' report
[7] Digital Economy Bill Factsheet: Better Public Services, Department of Culture, Media and Sport
[8] Digital Economy Bill, 2016, Part 5.

employment (…) and cut youth crime and anti-social behaviour".[9] However, processing bulk data to 'identify' and intervene in the lives of 'troubled families' arguably amounts to profiling and may breach Chapter 3 of the EU's new General Data Protection Regulation (GDPR), set to be enforced from 25th May 2018, as well as breaching privacy and non-discrimination provisions contained in the HRA.

16. We note the similar risks of algorithmic processes being used for ostensibly benevolent purposes, such as enhanced behavioural influencing, or 'nudging'. The Behavioural Insights Team or 'Nudge Unit', partly owned by the Cabinet Office,[10] has for example doubled the number of applicants for the army through behavioural influencing, which it views as a social good.[11] Liberty urges caution against the use of algorithmic processing and personal data in State efforts for behavioural influence, which clearly risks anti-democratic tendencies and undermining trust in public institutions.

17. Part 5 of the Digital Economy Bill states that other than fulfilling the purposes for which the data was ostensibly shared, information shared within and between the state and private companies 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. The processing of such vast data for multiple administrative, law enforcement and public service purposes is likely to require complex algorithmic processing. In Liberty's view, this growing trend indicates a data-enabled enlargement of the State that is highly unlikely to constitute a proportionate interference with privacy rights.

Algorithms in the private sector

18. Liberty is concerned that the increasing use of algorithms in the private sector to make eligibility decisions, such as access to credit, may risk increasing discriminatory outcomes.

[9] Digital Economy Bill Factsheet: Better Public Services, Department of Culture, Media and Sport
[10] https://www.gov.uk/government/organisations/behavioural-insights-team
[11] https://www.theguardian.com/public-leaders-network/2015/jul/23/rise-nudge-unit-politicians-human-behaviour

19. Longstanding patterns of social inequalities can be perpetuated and entrenched through algorithmic processes – for example, Google advertises highly paid jobs to men more often than to women.[12]

20. Even where 'sensitive' data categories such as race are prohibited as a category of profiling data (as may well be the case under the GDPR), combinations of other categories of data can unintentionally serve as a proxy. For example, "*if a certain geographic region has a high number of low income or minority residents, an algorithm that employs geographic data to determine loan eligibility is likely to produce results that are, in effect, informed by race and income*."[13] [14] In order to monitor and challenge such discriminatory effects, it is important that transparency is encouraged as to where algorithms are used, what data they process and how they work.

21. Many of us are now accustomed to algorithms presenting us with targeted advertisements online, which sometimes risk being insensitive and causing people to feel monitored. Perhaps more problematic is the use of analytics to generate customised pricing. It is vital that equality rights and data protection law are carefully observed, particularly by online retailers. The ICO, among others, should monitor developments in customised pricing, ensure retailers do not discriminate against consumers, and encourage online retailers to be transparent[15] about their use of data and any attempts to customise pricing.

22. In limited circumstances, EU citizens may soon have the right not to be subject to algorithmic decisions that would significantly or legally affect them. Article 22 of the GDPR states:

> *"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."*[16]

This principle does not apply if the decision is authorised by EU or state law so long as the data subject's rights, freedoms and legitimate interests are safeguarded.[17] It also disapplies if

---

[12] *Artificial Intelligence's White Guy Problem* – Kate Crawford, The New York Times, 25th June 2016
[13] *European Union regulations on algorithmic decision-making and a "right to explanation"* – B. Goodman, S. Flaxman, Aug 2016, p.4
[14] Big Data: Seizing Opportunities, Preserving Values – Executive Office of the President (US), May 2014, p.53
[15] Personalised Pricing: Increasing Transparency to Improve Trust – Office of Fair Trading, May 2013
[16] *General Data Protection Regulation, Article 22(1)*

it is necessary under a contract between the data controller and the subject,[18] or the subject has given explicit consent.[19] Nevertheless, this Article may prohibit private corporations using algorithmic decision-making in various applications. Although Liberty would like to see these protections extended to data subjects in the context of algorithms used in the public sector, we view these protections as welcome developments.

23. Article 22 of the GDPR, discussed above, further offers citizens 'the right to explanation' regarding an algorithmic decision made about them with consent or under contracts. Again, the right to explanation does not apply to the State's use of algorithms. Article 22(3) states that the subject maintains,

> "(…) *the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision."*[20]

Furthermore, Articles 13 and 14 state that subjects have the right to be given "*meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing".*[21] Article 12 states that communication with data subjects must be in "*concise, transparent, intelligible and easily accessible form".*[22] These regulations go some way to addressing concerns about transparency but, given the exceptions, do not satisfy concerns about the transparency of the State's algorithmic processing.

Attitudes towards privacy

24. The increasing use of algorithms to make automatic data-based decisions relies on masses of data, and often personal data. To make well-informed decisions, it is important that personal data is accurate – inaccurate data benefits neither data controllers nor data subjects. The increasing need to provide comprehensive accurate data about oneself, particularly in the context of a technological revolution driven by personal data, may gradually erode the importance of privacy in society.

---

[17] *General Data Protection Regulation, Article 22(2)(b)*
[18] *General Data Protection Regulation, Article 22(2)(a)*
[19] *General Data Protection Regulation, Article 22(2)(c)*
[20] *General Data Protection Regulation, Article 22(3)*
[21] *General Data Protection Regulation, Article 13(2)(f)* and *Article 14(2)(g)*
[22] *General Data Protection Regulation, Article 12*

25. Inclusion, especially accurate inclusion, in big datasets is increasingly seen by marginalised and vulnerable groups as important and necessary for access to services, visibility and fair treatment. Algorithms may not produce fair decisions for minority groups if there is too small a sample of data from which to generate predictions with confidence. For this reason, minorities are sometimes oversampled in public policy research.[23] An early example of inadequate training data resulting in discrimination was seen in Google's photo app, which classified black people as gorillas. Similar examples of algorithmic discrimination include Nikon software reading photos of Asian people as blinking and HP webcam software having difficulty recognising users with dark skin tones.[24] As algorithmic systems are increasingly used, there must be oversight and careful attention paid to the representativeness and diversity of the data input, as per good data science practice. Output must be carefully tested before systems are operational, and continually monitored, as such discriminatory flaws may not be easily discoverable and too often only come to attention once they already have had a negative effect.

26. Indeed, it is possible to use data and algorithmic design to control for and thus reduce discrimination. It has been described as a "*silver lining"* that "*for certain types of algorithmic profiling, it is possible to both identify and implement interventions to correct for discrimination. This is in contrast to cases where discrimination arises from human judgement."*[25] However, as discussed, any algorithmic tool and even the datasets they process can contain hidden biases, reflecting longstanding patterns of discrimination. Social justice and equality are not simple equations that can be solved, but ongoing social, political, legal processes.

27. Importantly, *exclusion* from data collection and the maintenance of privacy remains a right and in many circumstances, a democratic protection. 'Inclusion' in a dataset may not always be in an individual's or a certain group's best interests – and individuals retain the right to a private life. This must be recognised when evaluating the appropriateness of using algorithmic

[23] *European Union regulations on algorithmic decision-making and a "right to explanation"* – B. Goodman, S. Flaxman, Aug 2016, p.4
[24] *Artificial Intelligence's White Guy Problem* – Kate Crawford, The New York Times, 25th June 2016
[25] *European Union regulations on algorithmic decision-making and a "right to explanation"* – B. Goodman, S. Flaxman, Aug 2016, p. 7

decision-making. We also urge for greater consideration of the rights issues that wide-scale data processing engages – particularly upholding the right to privacy.

28. We must also consider the psycho-social impact of increasing algorithmic, data-based decision-making both in the public and private sectors. Citizens may increasingly feel deterred, whether consciously or not, from certain lawful behaviours due to the awareness that their actions create data points that may later affect them. Such a chilling effect erodes the natural freedom that all citizens should enjoy. It has been suggested that:

> *Possessing the information, and letting citizens know the government possesses the information, might alone shape individual choices. Citizens may be more reluctant to associate with certain groups, participate in certain activities, or even take political stances because of the information the government knows about their private lives. The collection of the information may be as threatening as its potential use.*[26]

Recommendations:

- **Algorithmic processing must not be the sole basis for a decision which produces legal effects or engages the rights of any individual.**

- **The creators of algorithms should always maintain the ability to provide transparency as to their algorithmic output and explanations for decisions made.** Where it is argued that algorithmic systems cannot be transparent or provide explanation for decisions, for example where they are used in the intelligence community, the maximum possible public transparency should be offered with full transparency allowed in a closed independent review or adversarial procedure. This is important to verify that the subject's rights and freedoms are safeguarded, particularly where a system has legal or other significant effects on a subject. **Algorithmic decisions that engage the rights and liberties of individuals should always be challengeable.**

- **Liberty urges caution against any algorithmic decision-making that involves the unconsented collection, sharing and/or analysis of personal data – including for purposes considered by Government to provide individual or social benefits.** The

[26] *Big Data and Predictive Reasonable Suspicion* – A. G. Ferguson, January 2015, pp.403-4

importance of privacy as an individual right and a feature of a democratic society must be carefully upheld in throughout technological developments.

Silkie Carlo