LIBERTY

PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

# Liberty's written evidence on the Data Protection Bill 2017 for the Joint Committee on Human Rights

**November 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 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**

Corey Stoughton
Advocacy Director
Direct Line 020 7378 3667
Email: coreys@liberty-human-rights.org.uk

Silkie Carlo
Senior Advocacy Officer
Direct Line 020 7378 5255
Email: silkiec@liberty-human-rights.org.uk

Gracie Mae Bradley
Advocacy and Policy Officer
Direct Line: 0207 378 3654
Email: gracieb@liberty-human-rights.org.uk

**CONTENTS**



**INTRODUCTION**

Liberty welcomes the opportunity to provide written evidence to the Joint Committee on Human Rights regarding the Data Protection Bill 2017.

The Bill represents an important opportunity to safeguard individuals' rights in a rapidly changing environment, where personal data is growing exponentially and increasingly interacting with access to, and breaches of, human rights.

In this written submission, Liberty seeks to draw particular attention to two areas of the Bill that require amendment: exemptions on the right not to be subject to purely automated decision-making, and exemptions from multiple rights on immigration control grounds.

## EXEMPTIONS ON IMMIGRATION CONTROL GROUNDS

The Data Protection Bill (the Bill), currently at Committee Stage in the House of Lords, applies the EU General Data Protection Regulation (GDPR). The GDPR enters into force in May 2018 and will remain in force until the UK leaves the EU, after which it will, according to the Government, be incorporated into domestic law. The GDPR allows Member States a margin of appreciation within which to adapt it to national circumstances. In particular, article 23(1) sets out a number of legitimate aims in the pursuit of which a state may make exemptions to data subjects' rights, such as national security and defence. Although article 23(1)(e) of the GDPR allows Member States to restrict subjects' rights to safeguard "other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security", nowhere in the GDPR is immigration control expressly noted as a legitimate ground for exemption.

Schedule 2, Part 1, paragraph 4 of the Bill (hereafter "the immigration control exemption") nevertheless creates an exemption from certain provisions of the GDPR on immigration control grounds. It reads as follows:[1]

> (1) The listed GDPR provisions do not apply to personal data processed for any of the following purposes –
>
> (a) the maintenance of effective immigration control, or
> (b) the investigation or detection of activities that would undermine the maintenance of effective immigration control,
>
> to the extent that the application of those provisions would be likely to prejudice any of the matters mentioned in paragraphs (a) and (b).
>
> (2) Sub-paragraph (3) applies where –
>
> (a) personal data is processed by a person ("Controller 1"), and
>
> (b) another person ("Controller 2") obtains the data from Controller 1 for any of the purposes mentioned in sub-paragraph (1)(a) and (b) and processes it for any of those purposes).

[1] Data Protection Bill 2017, Schedule 2, Part 1, paragraph 4 - page 125, line 40

(3) Controller 1 is exempt from the obligations in the following provisions of the GDPR

(a) Article 13(1) to (3) (personal data collected from data subject: information to be provided),

(b) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided),

(c) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers), and

(d) Article 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in paragraphs (a) to (c),

to the same extent that Controller 2 is exempt from those obligations by virtue of sub-paragraph (1).

The "listed GDPR provisions" to which the exemption relates are set out at Schedule 2, Part 1, paragraph 1 of the Bill. As Baroness Hamwee highlighted at Committee Stage, *"those listed provisions include many which are very important indeed*."[2] They encompass almost every data protection right afforded to an individual by the GDPR, as well as the general principles governing the processing of personal data to the extent that they correspond to those rights. Specifically, the exemption relates to the following fundamental data protection rights:[3]

- right to information (article 13(1)-(3))
- right to information where data is obtained from a third party (article 14(1)-(4))
- right of subject access (article 15(1)-(3))
- right to rectification (article 16)
- right to erasure (article 17(1)-(2))

[2] Baroness Hamwee in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1915
[3] Data Protection Bill 2017, Schedule 2, Part 1, paragraph 1 - page 124, line 5

- right to restriction of processing (article 18(1))
- right to data portability (article 20(1)-(2))
- right to object (article 21(1))
- the data protection principles set out under article 5: lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality and accountability, to the extent that they correspond to articles 13-20.

*A broad exemption, open to abuse*

The Government is at pains to describe this exemption as a "*targeted*" one.[4] However, as Lord Clement-Jones noted at Committee Stage, it is in fact "*broad and wide-ranging*" and "*open to abuse*".[5] During discussion of Amendment 80, an amendment to strip the exemption from the Bill, Government Minister Baroness Williams (Home Office) argued that (emphasis added):

> *"[t]he exemption would apply to the processing of personal data* ***by immigration officers and the Secretary of State*** *for the purposes of maintaining effective immigration control or the detection and investigation of activities which would undermine the system of immigration control.* ***It would also apply to other public authorities required or authorised to share information with the Secretary of State for either of those purposes****."*[6]

As discussed below, the fact of broad data-sharing between public authorities and the Home Office is deeply worrying, poses a significant threat to the human rights of the individuals targeted by it, undermines wider social objectives such as the protection of public health, and is likely to be unlawful. This objection aside, Baroness Williams' description of the exemption is deeply misleading. Sub-paragraphs 2 and 3 of paragraph 4 set out that where information is obtained from a second controller and processed for immigration control purposes, the second controller is also exempt from fulfilling certain data protection rights. As such the exemption does not apply only to the Home Office or other public authorities, it

[4] Baroness Williams of Trafford in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1913
[5] Lord Clement Jones in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1909
[6] Baroness Williams of Trafford in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1913

applies to any entity from whom the Home Office obtains data for immigration control purposes, which could include profit-making data brokers, corporate entities, or third sector organisations, should the Home Office hold or conclude in future data-sharing agreements with those entities. Moreover, to the extent that the Home Office outsources immigration control functions to third parties, including corporate entities such as G4S, those entities also benefit from the exemption.[7]

Nor are non-UK nationals the only individuals who may find themselves stripped of data protection rights under the exemption. The exemption does not attach itself to any particular class of person, such as non-UK nationals, but rather to any individual whose data is processed for immigration control purposes. Should the Government decide that checking every individual's immigration status as they interact with public services, employers, landlords, or banks is necessary for the maintenance of 'effective immigration control', and that stripping people of their data protection rights as this happens is desirable, people of all immigration statuses and nationalities will find themselves sorely disadvantaged by it. While the exemption does not in itself create new powers to share data, by allowing data-sharing agreements to operate in secret by virtue of sub-paragraphs 2 and 3, it has the potential to facilitate unscrutinised and unchallengeable bulk data-sharing on everyone in society, amounting in effect to the creation of a digital ID card in the name of immigration control.

The Government has argued that the exemption is "targeted", insofar as sub-paragraph (1) sets out that an individual's rights will only be exempted "to the extent that the application of those provisions would be likely to prejudice any of the matters mentioned in paragraphs (a) and (b)." Taking the right of subject access as an example, Baroness Williams set out the Government's view that each application "*would need to be considered on its merits*" and that "*the restrictions would bite only where there is a real likelihood of prejudice to immigration controls in disclosing the information concerned*".[8] This is no safeguard at all. Without a statutory definition of 'prejudice to immigration controls', which is particularly perplexing as a non-criminal category, it is far from clear that the use of the exemption would in fact be an exception rather than the norm, given especially that the Home Office – the beneficiary of the exemption – is the adjudicator of when it should apply. Furthermore, as demonstrated by recent political swings not only in the UK but in the US and elsewhere, 'effective immigration control' is a highly subjective goal, with the parameters and the effects on individuals' human rights vulnerable to political tides. In Liberty's view it is highly

[7] Data Protection Bill 2017, Schedule 2, Part 1, paragraph 4, sub-paragraphs (2) and (3) - page 126, lines 1-18
[8] Baroness Williams of Trafford in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1914

inappropriate to predicate the eradication of basic rights on such a broad, undefined and subjective basis.

If an individual feels the exemption has been unfairly applied, they should in theory be able to apply to the Information Commissioner's Office for redress. However, exercise of this remedy relies on an individual knowing that the exemption has been applied and on what basis, and as such will only be available when certain rights are exempted. Subject access requests are often made by individuals who need access to previous correspondence with the Home Office in order to progress their immigration cases. This includes undocumented people wishing to regularise their status. If a subject access request is refused in circimustances like these, it is likely that an individual will know that Home Office exercise of the exemption is the reason for this. But where a person's data is obtained from a third party by the Home Office and the exemption is applied to their right to be informed of this, they are unlikely to know that their data has been shared in this way and thus they will be unable to challenge either the application of the exemption or, more gravely, the ethics or lawfulness of the data transfer.

*Current Home Office practice: a cautionary tale*

There is already evidence to suggest that existing data-sharing schemes administered by the Home Office involve a rate of error which, given the adversity of the consequences for affected individuals who may well have leave to remain in the UK, should be considered significant. For example, the Immigration Act 2014 prohibits banks from opening current accounts for undocumented individuals, and requires them to use a third-party database to check individuals' eligibility. A 2016 investigation by the Chief Inspector of Borders and Immigration found that of a sample of 169 refusals to open bank accounts, 10% of refusals had been made in error.[9]

The widespread and routine sharing of personal data collected by frontline agencies with the Home Office forms the cornerstone of the hostile environment, and involves data collected by schools, NHS services, police, social services, banks, charities, and the DVLA. Many of these data-sharing practices are facilitated by the crime exemption at section 29 of the Data Protection Act, and target undocumented migrants to facilitate Home Office enforcement

[9] An inspection of the 'hostile environment' measures relating to driving licences and bank accounts' October 2016: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567652/ICIBI-hostile-environment-driving-licences-and-bank-accounts-January-to-July-2016.pdf

activity. They are codified by a series of MOUs concluded between various government departments and the Home Office, although some take place on an ad hoc basis. For the most part these agreements have been concluded in secret. Their existence has been brought to light primarily through Freedom of Information Act (FOIA) requests. Public awareness of them remains low, and parliamentary scrutiny of them has been negligible. Across the board, individuals are not informed when they interact with frontline services that their data may be processed in this way, not least because many frontline workers are unaware of the existence of these data-sharing agreements.

Current data-sharing arrangements for enforcement against people suspected of committing immigration-related crimes are typified by secrecy, total disregard for any of the fundamental principles currently governing data protection, and a wholesale failure to balance immigration enforcement objectives proportionately against competing public policy objectives or fundamental human rights. The operation of these schemes and their cumulative detrimental impact on individuals' lives, far from justifying any extension in the Home Office's ability to process personal data for immigration control as proposed in the Data Protection Bill points strongly towards the opposite: that the existing exemption on data protection obligations on law enforcement grounds should be narrowed to exclude low-level offences relating to immigration.

*Human rights, equality and proportionality*

Baroness Williams described the immigration control exemption in the Bill as "*a necessary and proportionate measure to protect the integrity of our immigration system*".[10] Personal data is processed by the Home Office to make decisions about individuals' claims to remain in the country and as the basis for its exercise of other immigration control functions such as detention and removal. That this exemption would permit the exercise of these functions on the basis of secretly obtained, potentially incorrect information without an individual's consent or knowledge, or any meaningful route to redress is a deeply disquieting and manifestly disproportionate means of achieving the aim of immigration control. Other provisions in the Data Protection Act and this Bill - in themselves overly broad - are already available to the Home Office for enforcement against people suspected of committing immigration-related crimes.

[10] Baroness Williams of Trafford in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1913

While the exemption is construed so widely that it may affect individuals of any immigration status, non-UK nationals are significantly more likely than UK nationals to have their data processed for immigration control purposes. It is therefore highly likely to be discriminatory on the grounds of race and nationality to the extent that it establishes a lesser data protection regime for non-UK nationals, thus engaging article 14 of the ECHR in conjunction with article 8. The EU Charter of Fundamental Rights also protects individuals' rights to private and family life, data protection, privacy and non-discrimination by virtue of its articles 7, 8 and 21 respectively.

The Government describes this exemption as one made under article 23 of the GDPR.[11] It is wholly unclear, as has already been discussed, that immigration control is a legitimate aim for the purposes of this article. Even if it was, article 23(1) clearly stipulates that such an exemption must only be made when it "*respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society*."[12] For the reasons outlined above, the exemption clearly demonstrates a flagrant disregard for the essence of the fundamental rights and freedoms. And even where an exemption does not show such flagrant disregard, article 23(2) stipulates that where relevant, such legislative measures should include provisions as to:

- (c) the scope of the restrictions introduced
- (d) the safeguards to prevent abuse or unlawful access or transfer
- (g) the risks to the rights and freedoms of data subjects.[13]

No meaningful attempt has been made by the Government to include provisions to this effect in the Bill.

*Conclusion*

For the reasons set out above, Liberty believes that Schedule 2, Part 1, paragraph 4 of the Data Protection Bill poses a grave threat to the human rights of millions in the UK, regardless of their immigration status. This exemption is the latest in a long, grave and truly peremptory series of affronts to human rights committed by the Government in the name of immigration control, and Liberty strongly urges the JCHR to support any amendment to remove it from the Bill.

[11] Baroness Williams of Trafford in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1913
[12] GDPR, Article 23(1)
[13] GDPR, Article 23(2)

## EXEMPTIONS ON THE RIGHT NOT TO BE SUBJECT TO AUTOMATED DECISION-MAKING

Under the Data Protection Act 1998, individuals have a qualified right not to be subject to purely automated decision making and, to the extent that automated decisions are permitted, a right to access information relating to automated decisions made about them.[14] The GDPR clarifies and extends these rights.

Article 22 of the GDPR gives individuals a right not to be subject to purely automated decision making:

> *"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."*[15]

This right does not apply if the decision is authorised by EU or the Member State's law so long as the data subject's rights, freedoms and legitimate interests are safeguarded.[16] Liberty believes that the safeguarding of data subjects' rights and freedoms clearly includes their rights provided by the Human Rights Act 1998. Therefore, we are calling for amendments to the Data Protection Bill that would explicitly state that automated decisions engaging an individual's human rights are not permissible.[17]

This is an important safeguard of increasing relevance as automated decision-making, often based on big data aggregation, is of growing use.

### *General processing*

In relation to general automated processing (clause 13), the explicit protection of human rights would protect individuals from being subjected to automated decisions that could engage their fundamental rights - for example, by unfairly discriminating against them. A recent study claimed that a facial recognition tool was able to 'detect' individuals' sexuality based on their photographs, taken from online dating sites, with greater accuracy than

[14] Data Protection Act 1998, s.12
[15] GDPR, Article 22(1)
[16] GDPR, Article 22(2)(b)
[17] See, *Liberty's Briefing on the Data Protection Bill 2017 for Committee Stage in the House of Lords – October 2017:* https://www.liberty-human-rights.org.uk/sites/default/files/Liberty%20Briefing%20on%20the%20Data%20Protection%20Bill%202017%20Committee%20Stage%20Lords%20Oct%202017%20.pdf

humans.[18] Another recent study claimed that a machine learning tool was able to diagnose depression by scanning individuals' photos posted on the social media platform Instagram with greater accuracy than the average doctor.[19] The rapidly growing field of machine learning and algorithmic decision making clearly presents new and very serious risks. As a minimum, individuals' basic rights must be explicitly protected at all times, and regarded as paramount.

*Law enforcement processing*

Law enforcement agencies are exempted from the prohibition on making purely automated, significant decisions (clause 47) – 'significant' decisions being those that significantly or adversely affect the data subject[20] - if the decision is required or authorised by law.[21] We believe such a decision should not be authorised by law if it engages an individuals' human rights, and we have lobbied for amendments to clause 48 to make this protection explicit.[22]

Liberty is deeply concerned about the potential uses of purely automated decision-making in the law enforcement environment, particularly in relation to the 'significant' decisions that have adverse legal effects that are exempted here. We believe that automated processing, if used, should inform officers' decisions rather make those decisions. Controversial algorithms currently being trialled by police forces, such as the harm assessment risk tool used in bail decisions and automated facial recognition that leads to arrests, are currently used to *support* officers' decisions. They do not replace officers' decisions or remove their discretion.[23] However, such purely automated decisions could be permitted under the exemptions within clauses 47 and 48.

Sophisticated algorithms used by law enforcement agencies such as the harm assessment tool and automated facial recognition are involved in decisions that engage fundamental

[18] Deep neural networks are more accurate than humans at detecting sexual orientation from facial images (preprint) - Yilun Wang & Michal Kosinski, OSF, 15 Feb 2017
[19] Instagram photos reveal predictive markers of depression - Andrew G Reece & Christopher M Danforth, EPJ Data Science, 8 August 2017
[20] Data Protection Bill 2017, cl. 47(2)
[21] Data Protection Bill 2017, cl. 47(1) and cl. 48(1)(b)
[22] See, *Liberty's Briefing on the Data Protection Bill 2017 for Committee Stage in the House of Lords – October 2017: https://www.liberty-human-rights.org.uk/sites/default/files/Liberty%20Briefing%20on%20the%20Data%20Protection%20Bill%202017%20Committee%20Stage%20Lords%20Oct%202017%20.pdf*
[23] For example: "*While HART forecasts support the custody officer's decision making, they quite explicitly do not remove the officer's discretion*" - written evidence submitted by Durham Constabulary (ALG0041; para. 7) in response to the Science and Technology Committee's inquiry into algorithms in decision making – April 2017: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/algorithms-in-decisionmaking/written/69063.html

rights such as the right to liberty, the right to a private life, freedom of expression, freedom of assembly and the prohibition of discrimination. The right not to be subjected to a purely automated decision – in other words, the requirement of human involvement in decision-making – is thus a vital safeguard, from which we do not believe law enforcement should be exempted.

*Intelligence services automated processing*

Similarly, we are concerned that the Bill currently permits the intelligence services to make purely automated decisions that have significant effects, including legal effects, as regards an individual. This could create significant risks for the upholding of basic rights in relation to new and emerging technologies.

We are calling for amendments[24] to cl. 94(2) that would provide a bare minimum protection and would still permit intelligence agencies to make purely automated decisions that have significant effects, including legal effects, where the decision is required or authorised by law – but that critically, would disallow decisions that engage an individual's rights under the Human Rights Act 1998 from being purely automated. This amendment would protect such basic rights as the right to liberty and the prohibition of discrimination from being engaged by solely automated means.

*House of Lords Committee Stage debate*

In Liberty's view, meaningful human involvement in decision-making is a basic and vital safeguard for our fundamental rights, particularly as we traverse the technological revolution. A provision for a post-hoc human review, on request by the affected party should they be informed of the automated decision process, is a welcome development but is not sufficient to *prevent* the potential harmful impacts of purely automated decisions in areas such as criminal justice, and the multitude of areas in which algorithmic processing is increasingly used.

Lord Clement-Jones, Lord Paddick, Baroness Hamwee, and Baroness Jones tabled amendments to ensure purely automated decisions are not permitted where human rights

[24] See, *Liberty's Briefing on the Data Protection Bill 2017 for Committee Stage in the House of Lords – October 2017:* https://www.liberty-human-rights.org.uk/sites/default/files/Liberty%20Briefing%20on%20the%20Data%20Protection%20Bill%202017%20Committee%20Stage%20Lords%20Oct%202017%20.pdf

are engaged. Lord Stevenson added his and his colleagues' support for the amendments in the House. The cross-party support for this minimal, vital protection was audible in the debate.

Ministers for the Government dismissed the necessity of the amendments, and appeared to misunderstand or misrepresent the effect such amendments would have.

*The effect of the amendments: General processing*

Lord Ashton, Parliamentary Under-Secretary (Department for Digital, Culture, Media and Sport) said of the proposed amendment to general decisions (Amendment 75):

> *"Arguably, such a provision would wholly negate the provisions in respect of automated decision-making as it would be possible to argue that any decision based on automated decision-making at the very least engaged the data subject's right to have their private life respected under Article 8 of the European Convention on Human Rights, even if it was entirely lawful. All decisions relating to the processing of personal data engage an individual's human rights, so it would not be appropriate to exclude automated decisions on this basis."*[25]

However, this conflates data processing with the nature of decisions made. The Bill clearly states the features of the types of *decisions* that may be purely automated in cl. 13(2) – features that do not refer to data processing but rather the nature of the decisions made. Accordingly, it would be appropriate in our view to add a further feature that a purely automated decision should not be one that engages the HRA.

Such an amendment would permit, for example, data processing (that engages Article 8) for the purposes of basic credit checking, as the decision – whilst significant – does not engage HRA rights.

[25] Lord Ashton of Hyde in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1871

*The effect of the amendments: Law enforcement and intelligence services processing*

Debating the proposed amendments in relation to law enforcement (Amendment 135) and intelligence services decisions (Amendment 144), Government Minister Baroness Williams (Home Office) suggested:

> *"(…) the unintended consequences of this could be very damaging. For example, any intelligence work by the intelligence services relating to an individual would almost certainly engage the right to respect for private life. The effect of the amendment on Part 4 would therefore be to prevent the intelligence services taking any further action based on automated processing, even if that further action was necessary, proportionate, authorised under the law and fully compliant with the Human Rights Act."*[26]

Similarly, this representation conflates data processing with the nature of decisions made. The amendment proposed (amd. 144) to cl. 94 specifically addresses the qualities of the decisions made as delineated in cl.94(2), rather than the processing.

The amendment would specifically *not* "*prevent the intelligence services taking any further action based on automated processing*" – it would precisely require intelligence services personnel rather than solely algorithms to make those decisions (for example, to take further action), whilst recognising that those decisions may be supported by automated processing.

Similarly, the amendment proposed for law enforcement decisions (amd. 135) is to cl. 48(1), which lists the features of a 'qualifying significant decision' and addresses the nature of the decisions specifically.

Such an amendment would permit, for example, data processing (that engages Article 8) from street parking surveillance to inform a purely automated decision to issue a parking fine, as the decision does not engage HRA rights. Clearly, this amendment would not hinder automated decision-making with respect to decisions unrelated to individuals' HRA rights.

[26] Baroness Williams of Trafford in Data Protection Bill Committee Stage in the House of Lords, 15th November 2017 – Hansard, vol. 785, col.2074

*The necessity of amendments to provisions for purely automated decisions*

Liberty strongly believes that the Data Protection Bill presents a significant opportunity to safeguard individuals' rights from the new and unique risks posed by automated decision-making.

Indeed, Lord Ashton acknowledged that:

> *"Automated processing could do that [infringe rights]. However, with the appropriate safeguards we have put in the Bill, we do not think that it will."*[27]

However, it is Liberty's view that at the very least automated decision-making must not be permitted for decisions that engage human rights. This is a most minimal, and essential, safeguard.

Lord Lucas pointed to the risks that automated decision-making may perpetuate discrimination:

> *"We have made so much effort in my lifetime and we have got so much better at being equal—of course, we have a fair way to go—doing our best continually to make things better with regard to discrimination. It is therefore important that we do not allow ourselves to go backwards because we do not understand what is going on inside a computer".*[28]

Baroness Jones argued:

> *"We must have the vital safeguard for human rights of the requirement of human involvement. After the automated decision-making result has come out, there has to be a human who says whether or not it is reasonable."*[29]

Liberty strongly agrees with these analyses and urges the JCHR to support amendments to the Bill that would prohibit significant decisions that engage individuals' HRA rights being made on a purely automated basis.

[27] Lord Ashton of Hyde in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1872
[28] Lord Lucas in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1874
[29] Baroness Jones of Moulsecoomb in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1867

## DELEGATED POWERS

In its current form, the Data Protection Bill grants unacceptable power to Ministers to introduce secondary (subordinate) legislation that bypasses parliamentary control over decisions to derogate from data protection rights – rights which, increasingly, are intractably linked to human rights.

Ministers would be given broad powers to create new categorical exemptions to data protection rules (Clauses 15 and 111). They can also add exemptions to (or remove) safeguards for processing sensitive personal data (Clauses 9, 33 and 84). The purpose of the Bill is arguably undermined by such delegated powers that enable Ministers to override Parliament's judgment and erode rights without sufficient democratic accountability.

The Delegated Powers and Regulatory Reform Committee (DPRRC) agreed with this assessment. The Committee decried the "*carte blanche*" nature of the powers and described the Government's justifications for them as "*inadequate*," "*weak*," and "*insufficient and unconvincing*."[30] It noted the likelihood for new exemptions created by statutory instrument to be "*highly controversial*," and criticised the affirmative procedure as:

> "*not an adequate substitute for a Bill allowing Parliament fully to scrutinise proposed new exemptions to data obligations and rights.*"[31]

Liberty is calling for the five major areas of delegated powers identified above to be removed from the Bill[32] – the DPRRC has also called for the removal of those five delegated powers.[33] Following cross-party concern expressed in Committee Stage (House of Lords) of the Bill, including the view that such delegated powers are a "*constitutional car crash"*,[34] Baroness Williams assured the House that:

---

[30] House of Lords, Delegated Powers and Regulatory Reform Committee, 6th Report of Session 2017-19, *Data Protection Bill* (24 October 2017), paras. 20, 34, 56 (available at **https://publications.parliament.uk/pa/ld201719/ldselect/lddelreg/29/29.pdf).**

[31] Ibid.

[32] See, *Liberty's Briefing on the Data Protection Bill 2017 for Committee Stage in the House of Lords – October 2017: https://www.liberty-human-rights.org.uk/sites/default/files/Liberty%20Briefing%20on%20the%20Data%20Protection%20Bill%202017%20Committee%20Stage%20Lords%20Oct%202017%20.pdf*

[33] House of Lords, Delegated Powers and Regulatory Reform Committee, 6th Report of Session 2017-19, *Data Protection Bill* (24 October 2017), paras. 21, 35, 57 (available at **https://publications.parliament.uk/pa/ld201719/ldselect/lddelreg/29/29.pdf).**

[34] Lord McNally in Data Protection Bill Committee Stage in the House of Lords, 15th November 2017 – Hansard, vol. 785, col.1638

> "*we [Government] are carefully considering the Delegated Powers Committee's report and will respond before the next stage of the Bill.*"[35]

We urge the JCHR to support the removal of these overly broad delegations of power over data protection rights to the Secretary of State. Data protection rights are of increasing importance in many areas of human rights – where their amendment or removal is concerned, parliamentary control must not be bypassed.

**Gracie Bradley**

**Silkie Carlo**

**Corey Stoughton**

[35] Baroness Williams of Trafford in Data Protection Bill Committee Stage in the House of Lords, 15th November 2017 – Hansard, vol. 785, col.2063