

Written evidence submitted by Liberty (DPB02)

Data Protection Bill

March 2018

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/>

CONTENTS

Introduction.....	4
<u>Delegated powers</u>	
Amendments.....	5
Effect.....	5
Briefing.....	6
<u>The “immigration control” exemption</u>	
Amendment.....	10
Effect.....	10
Briefing.....	10
The scope of the exemption.....	11
A full-frontal attack on access to justice.....	14
Home Office use of data, human rights and proportionality.....	16
Compliance with the GDPR.....	24
<u>Automated decision-making</u>	
Amendments.....	26
Effect.....	26
Briefing.....	26
The threat to human rights from purely automated decision-making.....	27
The critical distinction between automated data processing and automated decision-making.....	29
The Bill’s safeguards on automated decision-making are inadequate.....	30
<u>National security exemptions</u>	
The lack of a definition of “national security” and “defence purposes”.....	31
The lack of independent oversight of national security certificates.....	33
The lack of independent oversight of intelligence agencies generally.....	34
<u>Data Processing Framework for Government</u>	
Amendment.....	35
Effect.....	35
Briefing.....	35

INTRODUCTION

Liberty welcomes the opportunity to provide briefing and amendments to the Data Protection Bill 2017 for Committee Stage in the House of Commons.

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.

This briefing sets out the following proposals:

- To **remove excessively broad delegations** of law-making power to the Secretary of State
- To **maintain individuals' basic data rights where data is being processed for the "maintenance of effective immigration control"**, or "the investigation or detection of activities that would interfere with effective immigration control"
- To **protect individuals from being subjected to significant automated decisions that engage their fundamental rights**
- To **define "defence purposes" and "national security"** in order to restrict worryingly broad exemptions to people's data protection rights on these bases
- To ensure **adequate oversight** of national security certificates and the intelligence services more generally in relation to their data processing practices
- To **remove overly broad powers to create an unnecessary Data Processing Framework for Government**, or at the very least to involve Parliament meaningfully in its drafting.

DELEGATED POWERS

Amendments

Delegated powers to amend safeguards for processing of sensitive personal data

Clause 10, page 6, line 19, leave out sub-section (6)

Clause 10, page 6, line 25, leave out sub-section (7) (*consequential to the amendment above*)

Delegated powers to make further exemptions from data protection rights

Clause 16, page 9, line 13, leave out clause 16

Delegated powers to amend safeguards for processing of sensitive personal data for law enforcement

Clause 35, page 21, line 29, leave out sub-section (6)

Clause 35, page 21, line 32, leave out sub-section (7) (*consequential to the amendment above*)

Delegated powers to amend safeguards for processing of sensitive personal data by intelligence services

Clause 86, page 50, line 33, leave out sub-section (3)

Clause 86, page 50, line 36, leave out sub-section (4) (*consequential to the amendment above*)

Delegated powers to make further exemptions from data protection rights regarding intelligence services processing

Clause 113, page 63, line 1, leave out clause 113

Effect

These amendments would remove from the Bill excessively broad delegations of law-making power to the Secretary of State. Removing clauses 16 and 113 would prevent the Secretary of State subverting Parliament's judgment and circumventing robust Parliamentary review of the scope of proper derogations from data protection rights. Removing clauses 10(6-7), 35(6-7) and 86(3-4) would keep with Parliament any power to alter the legislative

determination of the proper balancing of individual privacy and public and social interests in the processing of sensitive personal data set forth in clause 9 and Schedules 1, 8 and 10.

Briefing

1. In its current form, the Data Protection Bill grants unacceptable power to Ministers to create statutory instruments that are highly likely to undermine the Bill's legislative scheme by creating new exemptions to data protection rights not considered or endorsed by Parliament. Liberty is particularly concerned by the sweeping powers granted to the Secretary of State by clauses **10(6), 16, 35(6), 86(3) and 113**; described by one member of the House of Lords during the Bill's Committee Stage as a "*constitutional car crash*".¹

2. The core purpose of this Bill is to strike a balance between individuals' right to data privacy and the proper use of data by defining the legitimate reasons that a person's data may be collected and processed, and setting important procedural safeguards on that collection and processing.

3. To that end, Schedules 2, 3, and 4 of the Bill set forth several exemptions from individual data protection rights, many of which are themselves the subject of significant debate by this Parliament. But **clause 16** of the Bill would grant to the Secretary of State additional power to add further exemptions, or vary existing ones, for a broad range of reasons generally relating to vaguely-defined purposes such as "the public interest," or "the exercise of official authority," without any guarantee of meaningful Parliamentary debate, scrutiny or amendment.

4. The Bill also delegates broad powers to expand permissible processing of sensitive personal data, including data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic or biometric data, health data, and data concerning a person's sex life or sexual orientation.

5. Consistent with the GDPR, the Bill allows processing of sensitive personal data only for defined, considered purposes and places procedural protections on such processing. However, **clauses 10(6), 35(6) and 86(3)** delegate power to unilaterally "vary" the conditions and safeguards governing the general processing of sensitive personal data in Schedule 1, and to "add" new "conditions" to Schedules 1, 8 and 10, which would have the effect of

¹ Lord McNally in Data Protection Bill Committee Stage in the House of Lords, 15th November 2017 – Hansard, vol. 785, col 1638

expanding the permissible reasons for allowing the processing of sensitive personal data both generally and for law enforcement and intelligence agencies.

6. Finally, **clause 113** delegates unlimited authority to create new exemptions to Part 4 of the Bill, which governs processing by intelligence agencies by permitting the Secretary of State to vary or add to the existing list of exemptions set forth in Schedule 11 without limitation.

7. The Constitutional Committee and the Delegated Powers and Regulatory Reform Committee of the House of Lords have expressed serious concerns about the scope of these delegated powers. The Constitutional Committee noted that:

“The Government’s desire to future-proof legislation, both in light of Brexit and the rapidly changing nature of digital technologies, must be balanced against the need for Parliament to scrutinise and, where necessary, constrain executive power.”²

8. The Delegated Powers and Regulatory Reform Committee went further, arguing:

“[I]t is not good enough for Government to say that they need “flexibility” to pass laws by secondary instead of primary legislation without explaining in detail why this is necessary — particularly in the case of widely-drawn Henry VIII powers. While we recognise that the affirmative procedure would apply to regulations under clauses 15 and 111 [clauses 16 and 113 of the Bill as brought forward from the House of Lords], this is not an adequate substitute for a Bill allowing Parliament fully to scrutinise proposed new exemptions to data obligations and rights.”³

9. In response to the Committees’ concerns and debate during Committee Stage in the House of Lords, the Government laid amendments to the delegated powers clauses at Report Stage. Regrettably, those amendments are meaningless. They removed the word “omit” from the list of Minister’s ability to “add, vary or omit” conditions and exemptions to data privacy rights in the original Bill, granting power of omission only in relation to conditions and exemptions added by the exercise of delegated power. But this does nothing to address the fundamental concern, which is that Ministers will be able to *add* new

² Select Committee on the Constitution, Data Protection Bill [HL] 6th Report of Session 2017-19, 26 Oct 2017, para. 11 (available at <https://publications.parliament.uk/pa/ld201719/ldselect/ldconst/31/31.pdf>)

³ Delegated Powers and Regulatory Reform Committee 6th Report of Session 2017-19, 24 Oct 2017, para. 34. (available at <https://publications.parliament.uk/pa/ld201719/ldselect/lddelreg/29/29.pdf>).

exemptions to the long list of exemptions to data privacy rights currently codified in the Schedules to the Bill.

10. Moreover, Ministers can achieve any change that might have been characterised as an “omission” by instead drafting it as a “variance” of a condition or exemption. As Lord Clement-Jones noted:

“[V]ariation can be extremely broad and virtually equivalent to omitting. It seems that one can vary a right all the way down to a minuscule situation which can impinge on the human rights of an individual, even though it is not technically an omission where a safeguarded is provided.”⁴

11. The Government acknowledged that its amendment falls far short of what was proposed by the Delegated Powers and Regulatory Reform Committee. Baroness Chisholm, speaking for the Government, argued that:

“[A]ccepting the Committee’s recommendations in full would leave the Government unable to accommodate developments in data processing and the changing requirements of certain sectors. This in turn could render the UK at a disadvantage internationally if, for example, we were unable to make appropriate future provision for sectors, including those such as insurance, where the UK is a world leader, to reflect advances and changes in their approach to data processing.”⁵

12. But the Government does not explain why it should be the decision of the Secretary of State rather than Parliament to alter the framework of data protection in the UK in response to external developments. In this Bill, Parliament has set out general principles and frameworks designed to balance individual privacy with the valid reasons for processing sensitive personal data, and it is for Parliament to decide, in this Bill, how to strike that balance. Parliament should not abdicate that responsibility and empower Government to fundamentally recalibrate the approach. Secondary legislation may be necessary and appropriate to **interpret and implement** the application of the Bill’s general principles in particular contexts, but there is no persuasive argument for permitting Ministers to constantly

⁴ Lord Clement-Jones in Data Protection Bill Report Stage in the House of Lords, 11th December 2017 – Hansard, vol. 785, col 1467

⁵ Baroness Chisholm in Data Protection Bill Report Stage in the House of Lords, 11th December 2017 – Hansard vol 785, col 1464-65

alter the legislative framework governing data protection in response to every technological development or every call from a representative of the insurance industry.

13. Moreover, the delegated powers in the Bill are not limited to making amendments to keep up with changes in the industrial and business sectors. They also allow Ministers to revise the data protection rules governing their own departments— especially in the law enforcement and intelligence agencies. Yet the Government has not sufficiently justified removing legislative control over how Government departments themselves recalibrate data protection rights over time. The fact that technology changes quickly cannot justify eroding democratic control over the actions of Government agencies.

14. This delegation of power is even more unprecedented when considered in the context of the pending EU (Withdrawal) Bill, which, in combination with this Bill, risks eliminating the GDPR as a check on the misuse of ministerial authority to undermine data privacy rights. The EU (Withdrawal) Bill gives Ministers power to make secondary legislation to amend any “retained EU law” – which would include a variety of critical EU directives governing data protection rights that should continue to apply in the UK through the incorporation provisions of that Bill.⁶ The Withdrawal Bill, as currently drafted, also eliminates an important data protection right contained in the Charter on Fundamental Rights: Article 8, which would otherwise constrain ministers’ ability to erode fundamental data privacy protections.⁷ Through both of these Bills, the Government is attempting to arrogate to itself the power to eliminate all rights-based barriers to the exercise of governmental power to process personal data. Parliament should not cede such unprecedented power to it.

⁶ European Union (Withdrawal) Bill, Schedule 8, paragraph (3), page 55, line 33

⁷European Union (Withdrawal) Bill, Clause 5(4), page 3, line 20. As the court noted in *Davis v. Secretary of State for the Home Department* [2015] EWHC 2092, the Charter “clearly goes further, is more specific, and has no counterpart” in other privacy laws.

THE “IMMIGRATION CONTROL” EXEMPTION

Amendment

Schedule 2, page 136, line 30, leave out paragraph 4.

Effect

This amendment removes an exemption to data subjects’ rights where personal data is being processed for the maintenance of effective immigration control, or for the investigation or detection of activities that would undermine it.

Briefing

15. The GDPR, which this Data Protection Bill applies, allows Member States a margin of appreciation within which to adapt it to national circumstances.

16. Schedule 2, part 1, paragraph 4 of the Bill, hereafter referred to as “the immigration control exemption,” proposes to create a new exemption from individuals’ data protection rights when their personal information is processed for:

- a) the maintenance of effective immigration control,⁸ or
- b) the investigation or detection of activities that would interfere with effective immigration control,⁹

to the extent that the fulfilment of their rights would prejudice these activities. The exemption would affect the rights and principles listed at sub-paragraph 2;¹⁰ they are summarised as follows and set out in full in the GDPR:

- 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 erasure (Article 17(1)-(2))
- right to restriction of processing (Article 18(1))

⁸ Data Protection Bill 2017 (as brought from the House of Lords), Schedule 2, Part 1, paragraph 4(1)(a)

⁹ Data Protection Bill 2017, Schedule 2, Part 1, paragraph 4(1)(b)

¹⁰ Data Protection Bill 2017, Schedule 2, Part 1, paragraph 4(2)

- right to object (Article 21(1))
- principle of lawful, fair and transparent processing (Article 5(1)(a))
- principle of purpose limitation (Article 5(1)(b))
- 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 the rights set out above.

17. While the Home Office is most likely to apply and benefit from the exemption, to the extent that it outsources immigration control functions to private companies or other entities (as it does to G4S to run immigration detention centres), those entities could also apply and benefit from it.¹¹

The scope of the exemption

- Broad and wide-ranging, and open to abuse

18. The Government is at pains to describe this exemption as a “*targeted*” one.¹² However, as Lord Clement-Jones noted at Committee Stage in the House of Lords, it is in fact “*broad and wide-ranging*” and “*open to abuse*”¹³; a concern echoed by Lord Kennedy.¹⁴ The only limitation as to which entities may benefit from the exemption, and which individuals may be subject to it, rests on the notion of “the maintenance of effective immigration control”, which has not been clearly defined anywhere by the Government, as Baroness Jones took care to highlight.¹⁵

19. During discussion in the House of Lords of Amendment 80, an amendment to strip the exemption from the Bill, Government Minister Baroness Williams (Home Office) argued that (emphasis added):

“The exemption would apply to the processing of personal data **by immigration officers and the Secretary of State** for the purposes of maintaining effective

¹¹ Data Protection Bill 2017, Schedule 2, Part 1, paragraph 4, sub-paragraphs (3) and (4) – page 137, lines 12-29

¹² Baroness Williams of Trafford in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1913

¹³ Lord Clement-Jones in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1909

¹⁴ Lord Kennedy in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1912

¹⁵ Baroness Jones in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1911

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.**¹⁶

20. Baroness Williams' description of the exemption is deeply misleading. To the extent that the Home Office outsources immigration control functions to third parties, those entities also benefit from the exemption.¹⁷

As the ICO notes:

“[T]he term ‘maintenance of effective immigration control’ is wide and would presumably apply to private organisations carrying out functions for the state – such as private sector organisations running immigration detention centres. It could also draw in organisations who are processing personal data for the purposes of checking the right-to-work status of individuals.”¹⁸

21. For example, in autumn 2012 the Home Office contracted a private company, Capita, to contact individuals suspected of being in the UK without the requisite leave.¹⁹ Approximately 39, 000 texts were sent advising those individuals that they were believed to be in the UK unlawfully. Some of them were advised to make plans to leave, causing them significant distress.²⁰ The data provided to Capita by the Home Office was clearly of poor quality, as it resulted in several individuals with outstanding applications or leave to remain in the UK being contacted, including veteran anti-racism campaigner Suresh Grover. Hundreds of complaints were filed.²¹ This incident is a stark demonstration of why **companies contracted to fulfil immigration control functions must be subject to the same data protection obligations as the rest of Government**, especially if the accuracy of the records they receive from the Home Office cannot be relied upon.

¹⁶ Baroness Williams of Trafford in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1913

¹⁷ Data Protection Bill 2017, Schedule 2, Part 1, paragraph 4, sub-paragraphs (2) and (3) - page 126, lines 1-18

¹⁸ Information Commissioner's Office, *Data Protection Bill, House of Commons Second Reading – Information Commissioner's briefing*, available here at para 45:

<https://ico.org.uk/media/2258304/dp-bill-house-of-commons-second-reading-briefing.pdf>

¹⁹ “Bounty hunters' hired to track down illegal immigrants” *The Telegraph*. 18/09/2012, available here:

<http://www.telegraph.co.uk/news/uknews/immigration/9551180/Bounty-hunters-hired-to-track-down-illegal-immigrants.html>

²⁰ “Diary: A text from Theresa May's Border Agency. Get out of the country. LOL”, *The Guardian*. 14/10/2013, available here:

<https://www.theguardian.com/politics/2013/oct/14/hugh-muir-diary-border-agency-may>

²¹ “Home Office ‘go home’ texts sent to people with right to remain”, *The Telegraph*. 18/10/2013, available here:

<http://www.telegraph.co.uk/news/uknews/immigration/10387658/Home-Office-go-home-texts-sent-to-people-with-right-to-remain.html>

22. Sub-paragraphs 3 and 4 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 this part of the exemption does not apply only to the Home Office or other public authorities with which it shares data, it 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. Indeed, the Home Office has already concluded such an agreement – with Cifas, a third sector anti-fraud organisation, with whom it shares data to ensure that people without leave to remain in the UK cannot access bank accounts.²² Yet, as with the Capita texts, poor data quality has also been flagged as a major concern with this scheme. 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.²³ One of the individuals refused an account had been in the UK lawfully for over a decade.

23. Immigrants are not the only people 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.** This Government, or a future Government, may 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” – indeed, as discussed below, this is precisely what is envisaged. In such a set of circumstances, people of all immigration statuses would find themselves liable to be subject to the exemption, if the Home Office judged it necessary to apply it. The scope of the exemption is therefore far wider than the Government describes. **Without a statutory definition of “the maintenance of effective immigration control”, it is virtually open-ended.**

- Non-existent safeguards

24. The Government has argued that the exemption is “targeted” and contains a safeguard 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*

²² Cifas Immigration Portal, available here: <https://www.cifas.org.uk/services/immigration-portal>

²³ 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

mentioned in paragraphs (a) and (b).²⁴ Taking the right of subject access as an example, Baroness Williams sets 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*".²⁵

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

25. 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 as such will only be available when certain rights are exempted.** As discussed below, subject access requests (SARs) are often made by individuals who need access to previous correspondence with the Home Office in order to progress their immigration cases, not to ask what enforcement action is being taken against them.²⁶ Yet the Home Office may determine that in these circumstances, fulfilling the request may prejudice the maintenance of effective immigration control, or at least, **there is nothing in the exemption that precludes it from doing so.** It is likely that a SAR applicant would be informed that Home Office exercise of the exemption is the reason for a refusal to fulfil it, and they would thus be able to exercise their right to complain to the ICO. 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. They will therefore be unable to challenge either the application of the exemption through appeal to the ICO or, more gravely, the ethics or lawfulness of the data transfer. **Application to the ICO to appeal the use of the exemption can be no safeguard if an individual is not aware that the exemption has been applied.**

²⁴ Data Protection Bill, Schedule 2, Part 1, paragraph 4(1)

²⁵ Baroness Williams of Trafford in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1914

²⁶ For further background in this regard, Liberty recommends reference to submissions made by the Immigration Law Practitioners' Association and the Bar Council, in addition to this briefing.

A full-frontal attack on access to justice

26. The exemption represents a significant threat to access to justice to the extent that it may jeopardise a person's ability to obtain their own data. The Government has stated that the Home Office will consider each application for subject access on its individual merits.²⁷ This means that the data controller most likely to benefit from the application of the exemption – the Home Office - will also be the entity deciding whether or not it applies. **A right that is contingent on Government largesse is no right at all.** The effects of its loss will be devastating.

27. Existing Home Office practice in failing to fulfil SARs fully and in a timely way already produces significantly deleterious effects for lawyers and their clients. The Joint Council for the Welfare of Immigrants (JCWI) conducted a survey to assess to what extent this was evidence of a systemic issue. In May 2017 it wrote²⁸ to the Information Commissioner's Office (ICO) requesting an urgent review of Home Office practice in fulfilling its Data Protection Act obligations on the basis of its findings. As JCWI states in its letter to the ICO:

“All 42 respondents had experienced issues with Home Office staff failing to provide full or adequate disclosure to SARs[...]. Crucially, 26 of the 42 respondents stated that this happened every single time they made a SAR. A further 5 indicated that this happened almost every time, or the majority of the time. Of the 9 remaining respondents most indicated that this was something that occurred on a regular basis.”²⁹

JCWI further sets out the human and procedural cost of these failures, stating that

“Combined with breaches of the 40-day time limit [these failures mean that] immigration cases often cannot progress expeditiously. The information needed for a client's case is often only available on the Home Office file, and the Home Office failure to disclose that information makes it impossible for the case to progress.

Our respondents reported the following impacts of this practice:

- It prolongs periods of destitution for vulnerable migrants such as asylum seekers. This results in immense hardship to vulnerable people, including causing street homelessness;

²⁷ Baroness Williams of Trafford in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1914

²⁸ *Joint Council for the Welfare of Immigrants*, 'Letter to the Information Commissioner's Office', 5 May 2017 [unpublished, seen by Liberty].

²⁹ JCWI, *ibid.*

- Without the file the client’s immigration history is unclear, so they cannot be advised to their status, and remain vulnerable;
- Clients in immigration detention are particularly impacted by this inability to advise, as the uncertainty is even more damaging when their liberty hangs in the balance.”³⁰

28. The proposed immigration control exemption will likely multiply these effects on an exponential scale. It will prevent those with unclear or precarious status from regularising their status, which is surely an activity that the Home Office wishes to encourage in its work to maintain effective immigration control. **In this regard, the exemption is not only deeply damaging to the individuals affected, it is also self-defeating.**

Home Office use of data, human rights and proportionality

- The right to data protection: not a new approach

29. The Government acknowledges that:

“It is the case that the Data Protection Act 1998 does not mention immigration control as a ground for restricting a data subject’s rights (...).

30. However, it contends that as the GDPR is a new framework, *“a new and different approach is called for.”*³¹

31. While the GDPR will modernise the data protection framework, it does not mark a departure from the overarching right to data protection protected by the Charter, the general principles governing data protection, or the fundamental rights to privacy and non-discrimination protected by the Charter and the European Convention on Human Rights (the Convention).

32. It simply does not follow that a modernised framework would require an astonishingly broad removal of long-held rights for an entirely new purpose.

33. As Lord Lucas argued at Committee Stage in the House of Lords the Bill itself is undermined *“in all sorts of insidious ways by having such a broad and unjustified clause.”*³²

³⁰ JCWI, *ibid.*

³¹ Baroness Williams of Trafford in a letter to Lord Clement-Jones, 23 November 2017: http://data.parliament.uk/DepositedPapers/Files/DEP2017-0730/2017.11.23_Letter_from_Baroness_Williams_to_Lord_Clement-Jones.pdf

³² Lord Lucas Baroness Williams of Trafford in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1911

34. The Government's assertion that a new approach to data protection and immigration control is required because of the novelty of the GDPR is unconvincing, especially in light of the existing exemption available to it in relation to crime (discussed below). Moreover, the suggestion that this exemption is analogous to an exemption under section 31 of the Freedom of Information Act obligations, as was made by the Government in the House of Lords stages of this Bill, is deeply disingenuous. The immigration exemption at section 31(1)(g)³³ of that Act restricts access to certain categories of information, under the broad banner of "Law Enforcement." The exemption proposed under this Bill is of an entirely different order: it would remove access to important rights.³⁴

- Existing Home Office powers and practice

35. In its response to the argument made in the House of Lords that the exemption is unnecessary, by virtue of the crime exemptions in paragraphs 2 and 3 of Schedule 2, the Government suggested that a law enforcement approach "*is not always the correct and proportionate response to persons who are in the UK without lawful authority and may not be the correct remedy.*"³⁵ Liberty agrees wholeheartedly with this statement. Indeed, it is Liberty's view that the criminalisation by successive governments of activities associated with the lives of undocumented people, such as working illegally or driving while unlawfully in the UK, is wholly disproportionate. Such measures should be repealed. However, for as long as immigration-related offences under the criminal law exist, should the Government deem it necessary to make exemptions to individuals' rights for immigration enforcement purposes, it already has the ability to do so using the existing law enforcement exemption at section 29 of the Data Protection Act. **It will continue to be able to do so using the exemptions at paragraphs 2 and 3 of Schedule 2 of the Bill, to the extent that fulfilling an individual's data protection rights would prejudice the prevention or detection of crime.**

36. Making use of the crime exemptions for data protection purposes categorically does not require the Home Office to take a law enforcement approach in managing a person's case once the function of the exemption has been fulfilled. As Liberty set out at length in its Committee Stage briefing for the House of Lords,³⁶ using the crime exemption in the Data Protection Act 1998 to facilitate administrative action against undocumented migrants is already standard, if highly unethical and problematic, Home Office practice. It is

³³ Freedom of Information Act 2000, Section 31, paragraph 1(g)

³⁴ Baroness Williams of Trafford in a letter to Lord Clement-Jones, 23 November 2017: http://data.parliament.uk/DepositedPapers/Files/DEP2017-0730/2017.11.23_Letter_from_Baroness_Williams_to_Lord_Clement-Jones.pdf

³⁵ Baroness Williams of Trafford in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1916

³⁶ Liberty's Briefing on the Data Protection Bill for Committee Stage in the House of Lords, pages 18-20

Liberty's view that the existing exemption on data protection obligations on law enforcement grounds should be narrowed to exclude low-level offences relating to immigration. However, for as long as those offences fall within the scope of the crime exemption, **the Home Office has more than sufficient powers to meet its objectives.**

37. Baroness Williams set out two case studies at Committee Stage in the House of Lords to illustrate circumstances in which the proposed exemption might be used. In one, a person who has overstayed their visa makes a subject access request about what measures are being taken to track their whereabouts and effect removal, with the Home Office using the proposed exemption to avoid fulfilling the request.³⁷ In the second, an individual is suspected of providing false information to the Home Office as part of an application to extend their leave in the UK, and the Home Office checks this against third-party sources to verify the information provided, invoking the exemption to ensure that the individual does not find out that the Home Office makes such checks.³⁸ However, Baroness Williams failed to acknowledge **that suspected criminality is already an aspect of both of these case studies**, to the extent that overstaying and attempting to obtain leave by deception are offences under Section 24 of the 1971 Immigration Act. As such the Home Office could already invoke existing crime exemptions for the aims that it sets out, **even if purely administrative action followed in each case**, without any need for a new immigration control exemption.

38. It is alarming, in any event, that the immigration control exemption is untethered from any notion of criminality or wrongdoing. As such migrants who have leave to remain and who are not suspected of committing any crime, and indeed British citizens, may find themselves stripped of data protection rights if the Home Office judges that this is necessary for the maintenance of effective immigration control, distinct from the prevention of immigration-related crime, or even the fulfilment of immigration enforcement functions. What is illuminating about the second case study provided by Baroness Williams is that by her account, Home Office exercise of the exemption is not fact-specific to the individual that is subjected to it. Rather the exemption is exercised to prevent certain Home Office practices, such as "accessing records held by third parties" becoming "common knowledge". **How can the exemption be exercised on a case-by-case basis if any disclosure that reveals a practice that the Home Office would prefer to keep concealed engages it?**

³⁷ Baroness Williams of Trafford in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1914

³⁸ Baroness Williams, *ibid.*

39. NHS Digital currently claims to undertake 'case-by-case' consideration of whether it is in the public interest to disclose a person's confidential medical information to the Home Office for immigration enforcement purposes under a Memorandum of Understanding (MoU) concluded between the two departments and the Department of Health (discussed further below). At an oral evidence session of a Health Committee inquiry into the MoU, Sarah Wilkinson, Chair of NHS Digital stated in response to a question about this 'case-by-case' consideration:

"There are **two categories** of application that are used by the Home Office today. One is the category A application, where they suspect somebody to be potentially guilty of an immigration crime. That is more than 99% of the applications from them that we respond to. There is a smaller proportion that we respond to that are category 2 requests, which is where there is a welfare concern. If there is a welfare concern, we do have a process for looking at individual public interest test considerations, because those are, by nature, just more complex, more bespoke, and they have more information in them, whereas for the category A requests, which are the bulk of it, it is really quite a simple process.

The Home Office has to say, very specifically, which immigration offence it suspects this individual to have committed and it has to tick a bunch of other boxes. If it does that, our existing public interest test for category A applications says that we should process those requests."

40. Dr Sarah Wollaston, Committee Chair, responded:

"So, **there is not somebody looking genuinely on a case-by-case basis**, as clinicians would understand it."³⁹

41. **It is clear from this exchange that any assertion by the Home Office that an exemption to a person's data protection rights on immigration control grounds would only be applied on a case-by-case basis must not be taken at face value.** Indeed, what Baroness Williams' admission at Committee Stage in the House of Lords shows, is that the exemption is likely to be exercised in a blanket fashion to prevent individuals finding out how the Home Office uses data to carry out its immigration control functions, even when they have done no wrong. In light of what is known about existing Home Office practice, and its plans to use data in the future, this is a chilling prospect.

³⁹Health Committee Oral evidence: Memorandum of understanding on data-sharing between NHS Digital and the Home Office, HC 677, at Questions 58-59: <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/health-and-social-care-committee/memorandum-of-understanding-on-datasharing-between-nhs-digital-and-the-home-office/oral/77354.html>

42. Since 2012, the Home Office has operated with a public commitment to creating a “hostile environment”⁴⁰ for undocumented migrants. Its effects reverberate well beyond its stated target group to affect migrants with regular status, settled black and minority ethnic (BAME) communities, and indeed the very fabric of the society in which we live through the requirement it imposes on public servants and private citizens to check individuals’ entitlements to goods and services, as well as the racially discriminatory impacts routinely felt by individuals who are subject to such checks.⁴¹

43. Data-sharing schemes currently operate to allow the Home Office to use children’s school records⁴² and confidential medical records⁴³ to obtain up-to-date contact details for people who are suspected of committing an immigration offence. Until early last year, the Greater London Authority (GLA) also shared aggregated, sensitive personal data collected by homelessness outreach services with the Home Office in the form of a map to facilitate enforcement activity against migrant rough sleepers, under a former Home Office policy that has now been deemed unlawful.⁴⁴ It has also been reported that in some circumstances, police have shared the personal information of victims of crime with Home Office immigration enforcement – in one circumstance in relation to a survivor of rape.⁴⁵ The impact of one of these data-sharing schemes was set out in harrowing detail earlier in January during an oral evidence session of the Health Committee’s inquiry into the Mou between NHS Digital and the Home Office, with a support project for domestic workers, Voice of Domestic Workers, recounting the story of a woman who, having been held in domestic servitude and abused by her employer, subsequently died because she feared that seeking medical care would make her vulnerable to immigration enforcement.⁴⁶

44. Across the board, individuals are not informed when they interact with frontline services that their data may be processed in this way, in part because the Home Office relies on the crime exemption at section 29 of the Data Protection Act to avoid fulfilling data subjects’

⁴⁰ *The Telegraph*, ‘Theresa May interview: ‘We’re going to give illegal migrants a really hostile reception’, May 2012 <http://www.telegraph.co.uk/news/uknews/immigration/9291483/Theresa-May-interview-We-re-going-to-give-illegal-migrants-a-really-hostile-reception.html>

⁴¹ A 2017 report by the Joint Council for the Welfare of Immigrants, *Passport Please*, found that an enquiry from a British Black Minority Ethnic (BME) tenant without a passport was ignored or turned down by 58% of landlords, in a mystery shopping exercise. Available here: https://www.jcwi.org.uk/sites/default/files/2017-02/2017_02_13_JCWI%20Report_Passport%20Please.pdf

⁴² ‘Memorandum of Understanding Between The Home Office And Department for Education In Respect of the Exchange Of Information Assets’ 7 October 2016 http://defenddigitalme.com/wp-content/uploads/2016/12/20161016_DfE-HO-MoU-redacted-copy.pdf

⁴³ ‘Memorandum of Understanding Between Health and Social Care Information Centre and the Home Office and the Department of Health’ 27 September 2016 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/585928/MOU_v3.pdf

⁴⁴ *Home Office policy guidance*, ‘European Economic Area nationals: misuse of rights and verification of EEA rights of residence’ 1 February 2017 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/588682/Misuse-of-rights-and-verification-of-EEA-rights-v2_0EXT.pdf

⁴⁵ Politics.co.uk, *Met police hands victims of crime over to the Home Office for immigration enforcement*, 5 April 2017: <http://www.politics.co.uk/news/2017/04/05/met-police-hands-victims-of-crime-over-to-the-home-office>

⁴⁶ The Huffington Post, *Dying Migrants Too Scared To See A Doctor For Fear of Deportation, MPs Are Warned*, 16 January 2018: http://www.huffingtonpost.co.uk/entry/dying-migrants-too-scared-to-see-a-doctor-for-fear-of-deportation-mps-are-warned_uk_5a5e1f26e4b0fcbc3a13c963

rights, and crucially, because many frontline workers are unaware of the existence of these data-sharing agreements. Bulk data-sharing also occurs in relation to bank accounts,⁴⁷ driving licences,⁴⁸ and benefits and employment.⁴⁹ The overall effect of this information sharing is the destruction of vital trust between frontline workers and people interacting with essential services. That the secret sharing of information could be dramatically facilitated by this exemption, targeting lawful migrants and British citizens as well as undocumented people, is incredibly worrying.

45. While the exemption does not in itself create new powers to share data, it allows data-sharing agreements to operate in secret by virtue of sub-paragraphs 3 and 4. **In practice, this removes a significant barrier to data-sharing** – the obligation to notify an individual that their data has been passed to a third party. In conjunction with the broad statutory gateway for data-sharing created by Part 5 of the Digital Economy Act, it has the potential to facilitate unscrutinised and unchallengeable bulk data-sharing on everyone in society, **in effect paving the way for a digital ID card.**

- Future Home Office use of data

46. In November 2017, the Public Accounts Committee heard evidence from Patsy Wilkinson, Second Permanent Secretary to the Home Office as part of its inquiry into “Brexit and the borders”. She made a series of statements outlining Home Office intentions to make more extensive use of data, including (emphasis added):

“Immigration enforcement is another area where we have more data available to us, and we are making more use of that data, and have plans to make more use of that.”⁵⁰

*“Because we are using technology, so that **if we can have the maximum chance of making connections between information about someone’s whereabouts and contact arrangements**, we can work more efficiently with local policing and we can work with other partners.”⁵¹*

⁴⁷ Cifas is a third sector organisation that holds the UK’s largest anti-fraud database. A data-sharing agreement between it and the Home Office is referenced at paragraph 2.6 in *Independent Chief Inspector of Borders and Immigration (ICIBI)*, ‘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

⁴⁸ ICIBI, *ibid.*

⁴⁹ Agreements obtained by Liberty and journalists through FOI request, and referenced in Vice Magazine, ‘Theresa May’s ‘Anti-Slavery’ Agenda Is About Deporting Migrants’ 21 September 2017: https://www.vice.com/en_uk/article/8x8qbv/theresa-mays-anti-slavery-agenda-is-about-deporting-migrants

⁵⁰ Patsy Wilkinson, Second Permanent Secretary to the Home Office, response to Question 64. Public Accounts Committee, Oral evidence: Brexit and the Borders, HC 558 20/11/2017

⁵¹ Patsy Wilkinson, Second Permanent Secretary to the Home Office, response to Question 65. Public Accounts Committee, Oral evidence: Brexit and the Borders, HC 558 20/11/2017

“We are using more data wherever we can. One key element that that data enables us to do is to automate contact.”⁵²

“In terms of retaining contact with people, and nudging people when their visa expiry time might be [...].”⁵³

“We need to make sure that we make it easy for landlords, et cetera, to check someone’s status.”⁵⁴

47. Moreover, in its technical note on *Citizens’ Rights – Administrative procedures in the UK*, the Government expresses at paragraph 6 its intention to “develop a system which draws on existing government data⁵⁵” to assist it in verifying the claims of EEA nationals applying for settled status. The Government’s direction of travel is clearly towards the increased use of data, bulk-sharing across departments, and automation in its exercise of immigration control functions. This may be a laudable aim, but **it is astonishing that such measures could be implemented at the same time as the safeguards that would help uphold such a system – data subjects’ rights – are at risk of being removed.**

48. At present the majority of bulk data-sharing schemes targeting undocumented migrants operate to provide the Home Office with up-to-date contact details for specific individuals. It is likely that data-sharing schemes will begin to operate to establish an individual’s entitlement to a good or a service (as they currently do between the Home Office and the DVLA, and the Home Office and Cifas), and to enable the Home Office to verify the substance of an individual’s claim to remain in the UK, as envisaged by the second case study discussed by Baroness Williams. As this kind of processing extends beyond undocumented migrants to include migrants with regular status and British citizens, **it is incredibly important that data subjects’ rights are preserved as a vital human check on inaccuracies in Government databases**, and in the case of undocumented migrants, reinstated.

- Human rights, necessity and proportionality

⁵² Patsy Wilkinson, Second Permanent Secretary to the Home Office, response to Question 68. Public Accounts Committee, Oral evidence: Brexit and the Borders, HC 558 20/11/2017

⁵³ Patsy Wilkinson, Second Permanent Secretary to the Home Office, response to Question 69. Public Accounts Committee, Oral evidence: Brexit and the Borders, HC 558 20/11/2017

⁵⁴ Patsy Wilkinson, Second Permanent Secretary to the Home Office, response to Question 72. Public Accounts Committee, Oral evidence: Brexit and the Borders, HC 558 20/11/2017

⁵⁵ TECHNICAL NOTE: CITIZENS’ RIGHTS - ADMINISTRATIVE PROCEDURES IN THE UK”, *HM Government*. 7/11/2017 available here: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/657694/TECHNICAL_NOTE_CITIZENS_RIGHTS_-_ADMINISTRATIVE_PROCEDURES_IN_THE_UK.pdf

49. In the House of Lords, Baroness Williams described the immigration control exemption in the Bill as “a necessary and proportionate measure to protect the integrity of our immigration system”.⁵⁶

50. The Joint Committee on Human Rights has nevertheless expressed significant concerns to the contrary, stating:

“The immigration exemption represents a departure from the current regime under the DPA. **It is not clear why this exemption is “necessary in a democratic society”.** Firstly, the Bill provides for exemptions in relation to the investigation and detection of crime, which could be applied in the context of illegal immigration in some instances. Secondly, even where the crime exemption would not apply, **it is unclear why immigration control requires exemptions from fundamental principles such as lawfulness, fairness, and accuracy in order to maintain its effectiveness.**”⁵⁷

51. The existence of this exemption means that an individual could be wrongly determined as having no leave to be in the country, or refused access to essential public services, without knowing what information was used to make that decision about them, to correct it or to ask for it to be deleted. These are very serious effects. As Dr Mohsen Danaie, a research scientist with a valid work visa who was wrongly told that he must leave the country asked:

“How could they possibly get my name wrong, but my address right? Did someone just type that information off a physical dossier? How advanced is the infrastructure at the Home Office? Should we not fear for our safety?”⁵⁸

52. It is worth remembering that “the maintenance of effective immigration control” is not a freestanding legitimate aim in the pursuit of which individuals’ Convention right to privacy (under Article 8) can be restricted. Even if it is accepted as a legitimate aim, the Government has done little to demonstrate why an immigration control exemption over and above the existing crime exemption is necessary. Nor has it attempted any proportionality analysis. It has made no attempt to show why the detriment suffered by an individual through the removal of their data protection rights is a proportionate way of meeting legitimate immigration control aims. Nor has it attempted to show that the detriment to other public

⁵⁶ Baroness Williams of Trafford in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1913

⁵⁷ Joint Committee On Human Rights, *Note from Deputy Counsel: The Human Rights Implications of the Data Protection Bill*, 6 December 2017, para. 50 https://www.parliament.uk/documents/joint-committees/human-rights/correspondence/2017-19/Note_Deputy_Counsel_DPBill.pdf

⁵⁸ ‘Leave UK immediately’: scientist is latest victim of Home Office blunder’, *The Guardian*. 26/09/2017, available here: <https://www.theguardian.com/uk-news/2017/sep/26/leave-uk-immediately-scientist-is-latest-victim-of-home-office-blunder>

policy objectives (such as the protection of public health or safety) caused by the removal of data protection rights is proportionate.

53. 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, and non-discrimination by virtue of its Articles 7, 8 and 21 respectively.

Compliance with the GDPR

54. The Government's future partnership paper on the exchange and protection of personal data⁵⁹ outlines its desire to ensure that the UK's data protection framework is adequate for the free flow of data between the UK and the European Union (EU) to continue after the UK leaves the EU in March 2019. But the inclusion of an immigration control exemption in the Bill jeopardises that entire endeavour. As such, the Government describes this exemption as one made under Article 23 of the GDPR.⁶⁰ Yet the GDPR makes no express provision for exemption to data subjects' rights on immigration control grounds. 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 matters, public health and social security", no express mention is made of immigration control, and the Government has made no attempt to explain why it considers that immigration control is a legitimate aim for the purposes of Article 23.

55. An exemption is permitted under Article 23(1), if and only if it "*respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society.*"⁶¹ Lack of necessity, proportionality, and a risk to the fundamental

⁵⁹HM Government, 'The exchange and protection of personal data: a future partnership paper' 24 August 2017: <https://www.gov.uk/government/publications/the-exchange-and-protection-of-personal-data-a-future-partnership-paper>

⁶⁰ Baroness Williams of Trafford in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1913

⁶¹ GDPR, Article 23(1)

human rights and freedoms have been highlighted above. But even if the exemption were not incompatible with human rights as set out by the Charter and the Convention, Article 23(2) of the GDPR stipulates that where relevant, the exemptions it provides for should include a number of procedural provisions, including 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.⁶²

56. No meaningful attempt has been made by the Government to include provisions to this effect in the Bill. The exemption is therefore highly unlikely to meet the requirements of Article 23 of the GDPR on several grounds. And thus the pursuit of adequacy in data protection arrangements, like so many other important public policy objectives, is defeated by the Government's attempt to bring border controls into every aspect of our lives no matter the cost.

⁶² GDPR, Article 23(2)

AUTOMATED DECISION-MAKING

Amendments

General automated processing

Clause 14, page 7, line 30, at end insert –

“(2A) A decision that engages an individual’s rights under the Human Rights Act 1998 does not fall within Article 22(2)(b) of the GDPR (exception from prohibition on taking significant decisions based solely on automated processing for decisions that are authorised by law and subject to safeguards for the data subject’s rights, freedoms and legitimate interests).”

Law enforcement automated processing

Clause 50, page 30, line 5, at end insert –

“() does not engage the rights of the data subject under the Human Rights Act 1998.”

Effect

These amendments would clarify that the exemption from prohibition on taking significant decisions based solely on automated processing must apply to purely automated decisions that engage an individual’s human rights.

Briefing

57. Clauses 14, 50, 96 and 97 must be amended to prevent data controllers making decisions that affect human rights by purely automated means. A human should be meaningfully involved in any decision that engages a person’s human rights.

58. Article 22 of the GDPR sets out 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.”⁶³

⁶³ GDPR, Article 22(1)

59. The GDPR permits UK law to create some exemptions to this right, provided that that law “lays down suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests.”⁶⁴

60. **Clauses 14 and 50** of the Bill establish that, for purposes of general processing and law enforcement processing of data, automated decision-making is allowed where it is “authorised by law”, and (a) notice is given to the person affected (clause 14(4)(a)), and (b) the person may seek reconsideration or a new decision not based solely on automated processing (clauses 14(4)(b), 14(5)).⁶⁵

61. Liberty urges Parliament to consider an amendment to these clauses prohibiting decisions based solely on automated processing of data, where those decisions engage rights protected by the Human Rights Act 1998.

The threat to human rights from purely automated decision-making

62. Human rights protected by the Human Rights Act 1998 should be safeguarded rigorously. There is no justification for permitting those rights to be assessed or affected by decisions that involve no human judgment or review, even with the “safeguards” that the Government has proposed.

63. Automated decisions have the potential to discriminate. The notion that algorithms and software are neutral or objective has been exposed as a fallacy. Google’s translation algorithm translates ungendered languages in a manner that perpetuates gender stereotypes; the algorithms governing voice-based assistants like Amazon’s Alexa struggle with certain accents; Netflix’s recommendation algorithm incorporates class biases; and a “Microsoft chatbot on Twitter started spewing racist posts after learning from other users on the platform.”⁶⁶ An investigation into software marketed for predicting risk of reoffending revealed that it was twice as likely to be inaccurate when assessing black people than white people.⁶⁷

64. These tools also threaten to perpetuate discrimination by giving data processors access to private information people had no intention of disclosing. A recent study suggested that a facial recognition tool was able to ‘detect’ people’s sexuality based on photographs taken

⁶⁴ GDPR, Article 22(2)(b)

⁶⁵ Under section 12 of the Data Protection Act 1998, people have a qualified right not to be subject to purely automated decision making. To the extent that automated decisions are permitted, people have a right to access information relating to such decisions about them.

⁶⁶ Li Zhou, *Is Your Software Racist?* Politico (8 Feb 2018) (<https://www.politico.com/agenda/story/2018/02/07/algorithmic-bias-software-recommendations-000631>)

⁶⁷ Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, *Machine Bias*, ProPublica (May 23, 2016) (<https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>)

from online dating sites with greater accuracy than humans.⁶⁸ Another recent study claimed that a machine learning tool was able to diagnose depression by scanning people's photos posted on the social media platform Instagram with greater accuracy than the average doctor.⁶⁹ The rapidly growing field of machine learning and algorithmic decision making clearly presents new and very serious risks.

65. During the debate in the House of Lords, 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".⁷⁰

66. Baroness Jones argued further:

"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."⁷¹

67. The authorisation of automated decision-making in the law enforcement environment is especially concerning. A broad range of significant decisions made by police and security services—from stops to searches to arrests—are "authorised by law," meaning that the Bill as drafted allows police to make almost *any* decision based solely on automated processing. This could include decisions to arrest, deny bail, issue search warrants, conduct surveillance, add people to the Gangs Matrix (a database of suspected gang members maintained by the Metropolitan Police) or other databases used to inform various law enforcement actions.

68. Decisions made by computers rather than by humans undermine democratic accountability. As Baroness Jones noted,

⁶⁸ Deep neural networks are more accurate than humans at detecting sexual orientation from facial images ([preprint](#)) - Yilun Wang & Michal Kosinski, OSF, 15 Feb 2017

⁶⁹ Instagram photos reveal predictive markers of depression - Andrew G Reece & Christopher M Danforth, EPJ Data Science, 8 August 2017

⁷⁰ Lord Lucas in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1874

⁷¹ Baroness Jones of Moulsecoomb in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1867

“After all the automated processing has been carried out, a human has to decide whether or not it is a reasonable decision to proceed. In this way we know where the decision lay and where the responsibility lies. No one can ever say, ‘We messed up your human rights. We interfered with your human rights and it is the computer’s fault.’”⁷²

69. Parliament should be very wary of expanding the role for automated decision-making in our society. Increasingly, academics are raising concerns of the risks of turning over policy to computers and artificial intelligence. As two experts in health policy recently noted:

“Automation in digital systems and sub-systems . . . is creating a new type of social regulation, one that is (deliberately) unmediated by human compassion or even the consideration of individual circumstances. This is social policy as an *iron cage*: designed, implemented and monitored via digital mechanisms that can operate in ways that leave them unaccountable to the public, designed with features developed with social regulation foremost in mind. As we have noted elsewhere, this is coercive big data in action.”⁷³

The critical distinction between automated data processing and automated decision-making

70. An amendment to prohibit automated decision-making where decisions engaged human rights would not affect anyone’s ability to engage in automated data processing. Data controllers would have unfettered ability to use automated data processing tools in any number of ways—including to make recommended decisions, so long as a human is meaningfully involved in those final decisions. For example, a police department could, consistent with the amendment, use an algorithm to assist in assessing patterns of criminal activity in order to inform deployment decisions. But those deployment decisions—and any subsequent operational decisions that flowed from such deployment—must be made by humans. Likewise, public health authorities could use automated data processing to generate information about where certain public health interventions are likely to have the most impact. But the decision about how to actually distribute public health resources must be made by humans.

71. Automated data processing may well have a significant role to play in making law enforcement—and other parts of government—more effective and efficient. Where automated tools are not prone to error or bias, they may wisely be used to **inform** law

⁷² Ibid., col. 1578.

⁷³ Hamish Robertson and Joanne Travalgia, “An Emerging Iron Cage? Understanding the Risks of Increased Use of Big Data Applications in Social Policy,” LSE Impact Blog <http://blogs.lse.ac.uk/impactofsocialsciences/2018/02/07/an-emerging-iron-cage-understanding-the-risks-of-increased-use-of-big-data-applications-in-social-policy/>

enforcement decisions rather than **make** those decisions. Tools such as risk assessment algorithms and facial recognition technology are currently being trialled for purposes of **supporting** officers' decisions on issues such as setting bail and making arrests. There is no operational case for authorising law enforcement to replace human decision-making with automated decision-making.⁷⁴

The Bill's safeguards on automated decision-making are inadequate

72. The Bill's provision for 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. The burden should not be on individuals to address the threat posed by automated decision-making. Concerns about discrimination, fairness, legitimacy and democratic accountability go beyond any one individual.

73. In particular, individual challenges to automated decision-making cannot address the risks that automated decisions will perpetuate discrimination or disproportionately harm certain communities. Such discrimination will not be revealed in ad hoc review of individual decisions, nor could the harm from discrimination be adequately remedied through case-by-case review. Liberty strongly recommends that exemptions to the prohibition on automated decision-making are amended to ensure **that in all circumstances, human rights are protected by meaningful safeguards.**

⁷⁴ 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>

NATIONAL SECURITY EXEMPTIONS

74. The current Bill provides for overly broad and excessively vague exemptions to nearly all of its data protection rules and privacy safeguards, as well as to the rules and safeguards of the applied GDPR, based on national security (and defence).⁷⁵ The Bill does not provide any definition of the terms “national security” or “defence.” These exemptions are not, on the surface, limited to the UK’s intelligence and security services, but—by applying to Part 2, which deals with “general processing” of people’s data—broadly permit public authorities and even private corporations to invoke national security and defence as a reason to cast aside privacy rights. Whether an action involving personal data falls within these exemptions is determined solely by a Minister issuing a national security certificate, reviewable only by the Investigatory Powers Tribunal applying a judicial review standard that cannot second-guess the Minister’s discretionary determinations.

75. The Government has not provided any justification for the breadth and indeterminate meaning of the national security exemption. In response to amendments laid in the House of Lords to limit the exemption, the Government merely noted that the Data Protection Act 1998 also contains a national security exemption. That is no response to the significant legal and policy concerns raised by the undefined scope of and lack of safeguards around the exemption, particularly in light of developments in Government practice, case law since 1998 and the GDPR itself, which did not exist in 1998. Moreover, the Bill expands the scope of the exemption beyond the 1998 Act, including by augmenting “national security” to include a further undefined range of “defence purposes.”

76. A number of legal and privacy commentators have raised concerns about the scope of the national security exemptions and the process of issuing national security certificates, and in this regard, in addition to Liberty’s briefing, we encourage Peers to review the briefings of Privacy International, which provide greater detail on this subject. A few critical points are discussed below.

The lack of a definition of “national security” and “defence purposes”

77. Left undefined, the terms “national security” and “defence purposes” are unnecessarily open to broad and vague interpretation, threatening to remove important limitations on power when doing so is not, in fact, necessary. The lack of a definition also means that people are not able to foresee or understand when their personal data rights will be

⁷⁵ Data Protection Bill 2017 (as brought from the House of Lords) clauses 26-28, 79, 110-11.

overridden by application of these exemptions – a crucial component of any exemption to fundamental rights.

78. When this issue arose previously in connection with the similarly undefined national security exemption in the Investigatory Powers Act, the Joint Committee on that draft Bill recommended that it include definitions of national security.⁷⁶ In the debate on that Bill, Ken Clarke MP remarked at Second Reading in the House of Commons:

“National security can easily be conflated with the policy of the Government of the day. I do not know quite how we get the definition right, but it is no good just dismissing that point.”⁷⁷

79. Likewise, during the debate on this matter in the House of Lords, the Government was repeatedly pressed on the meaning of the term “defence”, but could do no more than assert that a previous exemption for “combat effectiveness” was deemed insufficient.

80. The use of these broad and undefined terms risks interference with political and other lawful activity that ought to go unimpeded in a democratic society. In an era when Members of Parliament have been attacked as “*traitors*” and “*mutineers*” merely for attempting to amend legislation relating to the UK’s departure from the EU, and when Government has defined the concept of “*extremism*” to include anything in opposition to “*British values*,”⁷⁸ the continued undefined use of these terms in legislation is more than unacceptable, it is dangerous.

81. Parliament should not rely on the judiciary to bring substance or meaning to “national security” and “defence”. Empirically, courts have responded with considerable deference to Government claims of “national security,” viewing them not as a matter of law, but as Government-led policy judgements.⁷⁹ National security as a legal test is therefore meaningless when left without a statutory definition.

82. While the judiciary may not define the term for Parliament, it may correctly find that its failure to create a definition violates human rights. On the basis of a similar lack of definition, the European Court of Human Rights found that Russian national legislation granting open-ended discretion to the Russian Executive to undertake interception with the aim of

⁷⁶ *Report of the Joint Committee on the Draft Investigatory Powers Bill*, 11 February 2016, Recommendation 82

⁷⁷ See Hansard, 15 March 2016, <http://www.publications.parliament.uk/pa/cm201516/cmhansrd/cm160315/debtext/160315-0002.htm>

⁷⁸ <https://homeofficemedia.blog.gov.uk/2018/01/25/factsheet-on-the-commission-for-counteracting-extremism/>

⁷⁹ Lord Hoffman at para 50, *Secretary of State for the Home Department v Rehman* [2001] UKHL 47: Lord Hoffman has stated that whether something is ‘in the interests’ of national security “is not a question of law, it is a matter of judgment and policy” to be determined not by judges but to be “entrusted to the executive”.

“obtaining information about events or activities endangering the national, military, economic or ecological security of the Russian Federation” was incompatible with the Convention. In *Zakharov v Russia*, the Court said:

“It is significant that [Russia’s domestic interception law] does not give any indication of the circumstances under which an individual’s communications may be intercepted on account of events or activities endangering Russia’s national, military, economic or ecological security. It leaves the authorities an almost unlimited degree of discretion in determining which events or acts constitute such a threat and whether that threat is serious enough to justify secret surveillance, thereby creating possibilities for abuse.”⁸⁰

83. Parliament should not risk placing the UK alongside Russia in its approach to human rights. It should instead properly define and limit exemptions to privacy rights based on national security and defence.

84. These terms can be defined. The UN’s Siracusa Principles provide a definition of “national security.”⁸¹ Amendments defining the term were debated seriously, though not finally adopted, in considering the Investigatory Powers Act 2016. We would urge Parliament to reconsider this issue as a matter of paramount importance.

The lack of independent oversight of national security certificates

85. The lack of a clear definition of the scope of the national security exemptions is compounded by the lack of independent oversight or review of ministers’ invocation of the exemptions. The decision as to whether the exemptions apply lies with ministers. Thus, the test will be met by whatever a minister subjectively decides is related to national security or defence.

86. The decision is reviewable by the Investigatory Powers Tribunal, but the independence of that body has been repeatedly questioned,⁸² and in any case it may only apply a judicial review standard, which does not permit the court to exercise any oversight over the Minister’s subjective, discretionary determinations.

87. This year, in response to Liberty’s challenge on behalf of Tom Watson MP to the lack of safeguards and independent oversight in the UK surveillance regime, the Government

⁸⁰ *Zakharov v. Russia*, [GC], no. 47143/06, ECHR 2015, para 248.

⁸¹ Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights, Annex, UN Doc E/CN.4/1984/4 (1984)

⁸² <https://www.liberty-human-rights.org.uk/sites/default/files/2018.01.18%20liberty%20consultation%20response%20FINAL.pdf>

conceded that additional safeguards—including a far more robust system of independent oversight—were necessary.⁸³ There is no reason why, at a bare minimum, those same provisions should not apply in this context.

The lack of independent oversight of intelligence agencies generally

88. Under the Data Protection Act 1998, the intelligence agencies—like other public agencies— are subject to oversight by the Information Commissioner. The Bill, in clause 110(2), removes that oversight entirely. There is no rationale for exempting the intelligence agencies’ data processing activities from any independent oversight. To the extent that the Information Commissioner is not well-suited to address the sensitivities of data processing in the national security context, the Investigatory Powers Commissioner has an established record of exercising oversight functions in this context.

89. Liberty strongly recommends that Parliament amends this Bill to define “national security” and “defence purposes”; to limit disquietingly broad exemptions to individual’s data protection rights on national security grounds; and to introduce meaningful oversight of the operation of national security certificates, as well as data processing by the intelligence services more generally.

⁸³ <https://www.gov.uk/government/consultations/investigatory-powers-act-2016>.

DATA PROCESSING FRAMEWORK FOR GOVERNMENT

Amendment

Clause 185, page 107, line 3, leave out clauses 185 - 188

Effect

This amendment would remove from the Bill superfluous and overly broad delegations of power to the Secretary of State to create a “Data Processing Framework for Government”.

Briefing

90. A set of Government amendments to the Bill late at Committee Stage in the House of Lords introduced powers for the Secretary of State to issue a “*Data Processing Framework for Government*”, now contained at clauses 185-188 of the Bill. In its explanatory notes to the Bill, the Government states that:

This clause makes provision for the Secretary of State to issue statutory guidance (a “Framework for Data Processing by Government”) about the processing of personal data in connection with the exercise of functions of the persons or bodies listed in subsection (1). Any person carrying out such processing must have regard to this guidance. The Secretary of State may by regulations specify additional persons with functions of a public nature who are required to have regard to the Framework.”⁸⁴

91. It adds that prior to being brought into force “*the Framework must be subject to Parliamentary scrutiny through a process broadly equivalent to the negative resolution procedure*”,⁸⁵ whereby the draft Framework is laid before both Houses of Parliament and scrutinised over the course of forty days. Clause 186(2) stipulates that “*if, within the 40-day period, either House of Parliament resolves not to approve the document, the Secretary of State must not issue it.*”⁸⁶

92. The purported effect of the Framework is set out at clause 188, with obligations placed on data processors, courts and tribunals, and the Information Commissioner’s Office as follows (emphasis added):

⁸⁴Data Protection Bill [HL] Explanatory notes, para 540

⁸⁵Data Protection Bill [HL] Explanatory notes, para 544

⁸⁶Data Protection Bill 2017 (as brought from the House of Lords), clause 186(2)

“(1) When carrying out processing of personal data which is the subject of a document issued under section 186(3) which is for the time being in force, a person must have regard to the document.

(2) A failure to act in accordance with a provision of such a document does not of itself make a person liable to legal proceedings in a court or tribunal.

(3) A document issued under section 186(3), including an amendment or replacement document, is admissible in evidence in legal proceedings.

(4) In any legal proceedings before a court or tribunal, the court or tribunal must take into account a provision of any document issued under section 186(3) in determining a question arising in the proceedings if—

(a) the question relates to a time when the provision was in force, and

(b) the provision appears to the court or tribunal to be relevant to the question.

(5) In determining a question arising in connection with the carrying out of any of The Commissioner’s functions, **the Commissioner must take into account a provision of a document issued under section 186(3) if—**

(a) the question relates to a time when the provision was in force, and

(b) the provision appears to the Commissioner to be relevant to the question.”⁸⁷

93. The late-stage introduction of these clauses to the Bill means that they were not as closely scrutinised in the House of Lords as other parts, and it is crucial that they are the focus of close attention now that the Bill has reached the Commons. At Report Stage, Peers expressed a range of concerns, echoing those made by the Information Commissioner’s Office; many of which Liberty and other organisations share.

94. The Government claims that the purpose of the Framework is “*to set out the principles and processes that the Government must have regard to when processing personal data*”⁸⁸. It remains unclear, however, why data processing by Government and private companies determined to be fulfilling public functions should be subject to principles and processes

⁸⁷ Data Protection Bill 2017 (as brought from the House of Lords), clause 188

⁸⁸ Lord Ashton of Hyde in Data Protection Bill Report Stage, 10th January 2018 - Hansard, col. 292

distinct from those already set out under this Bill and the GDPR itself. Moreover, the intended effect of a requirement on courts, tribunals and the ICO to “take account” of the Framework lacks meaningful clarity. As the ICO herself points out in relation to what is now clause 188(5):

“The provision runs a real risk of creating the impression that the Commissioner will not enjoy the full independence of action and freedom from external influence when deciding how to exercise her full range of functions as required by Article 52 of the GDPR.”⁸⁹

95. Indeed, Lord Stevenson has suggested that the framework in effect amounts to an attempt to introduce “*a parallel system under which data processing undertaken by government departments could be considered to be governed*”⁹⁰ – an exemption to the provisions of the Bill and the GDPR in sheep’s clothing.

96. In addition to concerns about its purpose, Liberty is also alarmed that a Framework purporting to govern the processing of data held by Government, much of which contains the most intimate details of our lives – our school records, social services records, and medical records, for example – should be subject to a level of scrutiny that is broadly similar to the paltry scrutiny afforded a statutory instrument subject to the negative resolution procedure. Liberty’s significant concerns with that procedure and delegated powers more broadly are set out in the opening section of this briefing and apply as much here as they do there. As Lord Stevenson pointed out at Report Stage, “*citizens’ data should really belong to citizens and we should not have a situation where it is looked after by Ministers on behalf of Ministers and there is no external view.*”⁹¹ Lord Clement-Jones went further to argue “*[f]rankly, the Secretary of State can pretty much do what he or she wants[...]. [T]he framework for government data protection is not in fact data protection at all.*”⁹²

97. The overly broad latitude afforded to the Secretary of State is illuminated by clause 187(4), which sets out that in circumstances “*where the Secretary of State becomes aware that the terms of such a document [issued under the framework] could result in a breach of an international obligation of the United Kingdom*”, the SoS must remedy this by exercising their power under clause 185(4) to issue a new document or amend the existing one. So not only does the Government envisage a circumstance in which a barely-scrutinised

⁸⁹ Information Commissioner’s Office, *Annex II, Data Protection Bill House of Lords Report Stage* – Information Commissioner’s Briefing, para. 13

⁹⁰ Lord Stevenson in Data Protection Bill Report Stage, 10th January 2018 – Hansard, col. 289

⁹¹ *Ibid.*, col. 290

⁹² Lord Clement-Jones in Data Protection Bill Report Stage, 10th January 2018 - Hansard col. 291

Framework for Data Processing By Government breaches the UK's international obligations – which would include its obligations under the GDPR, the EU Charter of Fundamental Rights, and the European Convention on Human Rights – it then proposes to place the responsibility for remedying that breach solely in the hands of the Minister who caused it. If such a Framework is necessary, Parliament must be meaningfully involved not only in any amendment to it to remedy breaches of international law, but in the creation of the document in the first place.

98. The Government must now set out a robust justification for the introduction of this Framework; and the Framework itself should be included within the Bill so that it can be subject to appropriate scrutiny. Failing that, the vague, overly broad and superfluous powers set out at clauses 185-188 should be removed.

March 2018