LIBERTY

PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

Liberty's briefing on the Data Protection Bill 2017 for Report Stage in the House of Lords

December 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 briefing and amendments to the Data Protection Bill 2017 for Report Stage in the House of Lords.

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 **uphold individuals' basic data rights where data is being processed for the "maintenance of effective immigration control"**
- To **protect individuals from being subjected to significant automated decisions that engage their fundamental rights**
- To **remove excessively broad delegations** of law-making power to the Secretary of State

EXEMPTIONS ON IMMIGRATION CONTROL GROUNDS

Amendment

Schedule 2, page 129, line 18, 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

The Data Protection Bill (the Bill) 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.

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 guaranteed under the GDPR when their data is processed for:

a) the maintenance of effective immigration control,[1] or
b) the investigation or detection of activities that would interfere with effective immigration control,[2]

to the extent that the fulfilment of their rights would prejudice these activities. The exemption would affect the rights listed at paragraph one of schedule 2,[3] and set out in full in the GDPR at Articles 13(1)-(3), 14(1)-(4), 15(1)-(3), 16, 17(1)-(2), 18(1), and 20(1)-(2). The exemption also covers the general principles set out in Article 5 as they apply to these rights.

Sub-paragraphs 2 and 3 of paragraph 4 exempt data controllers that process and share data with a second controller for the purposes of immigration control or investigation of activities that would undermine it from their obligations under GDPR Articles 13(1)-(3), 14(1)-(4), 15(1)-(3) and Article 5, to the extent that the second controller is also exempt from the generally applicable safeguards contained in those GDPR provisions.

[1] Data Protection Bill 2017, Schedule 2, Part 1, paragraph 4(1)(a)
[2] Data Protection Bill 2017, Schedule 2, Part 1, paragraph 4(1)(b)
[3] Data Protection Bill 2017, Schedule 2, Part 1, paragraph 1(a)-(b)

The scope of the exemption

- Broad and wide-ranging, and 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]; a concern echoed by Lord Kennedy.[6] 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 has taken care to highlight.[7]

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****."*[8]

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.[9] In autumn 2012 the Home Office contracted a private company, Capita, to contact individuals suspected of being in the UK without the requisite leave.[10] 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.[11] The data provided to Capita by the Home Office was clearly of poor quality, as it resulted in several individuals with outstanding applications or

[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] Lord Kennedy in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1912
[7] Baroness Jones in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1911
[8] Baroness Williams of Trafford in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1913
[9] Data Protection Bill 2017, Schedule 2, Part 1, paragraph 4, sub-paragraphs (2) and (3) - page 126, lines 1-18
[10] "'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
[11] "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

leave to remain in the UK being contacted, including veteran anti-racism campaigner Suresh Grover. Hundreds of complaints were filed.[12] 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 the Government, especially if the accuracy of the records they receive from the Home Office cannot be relied upon.

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 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.[13] 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.[14] One of the individuals refused an account had been in the UK lawfully for over a decade.

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

[12] "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

[13] Cifas Immigration Portal, available here: https://www.cifas.org.uk/services/immigration-portal

[14] 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

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

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 mentioned in paragraphs (a) and (b)*."[15] 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*".[16] 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.

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. 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. 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

[15] Data Protection Bill, Schedule 2, Part 1, paragraph 4(1)
[16] Baroness Williams of Trafford in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1914

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.

Home Office use of data, human rights and proportionality

- The right to data protection: not a new approach

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 (…).*

However, it contends that as the GDPR is a new framework, "*a new and different approach is called for.*"[17]

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).

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

As Baroness Hamwee has pointed out, the listed provisions to which the exemption pertains are numerous and "*very important indeed*".[18] The affected rights are as follows, and encompass almost every right granted by 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 rectification (Article 16)
- right to erasure (Article 17(1)-(2))

[17] 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

[18] Baroness Hamwee in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1915

- 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.

As Lord Lucas argued at Committee Stage the Bill itself is undermined "*in all sorts of insidious ways by having such a broad and unjustified clause*."[19]

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 law enforcement (discussed below). Moreover, the suggestion that this exemption is analogous to an exemption under section 31 of the Freedom of Information Act obligations is deeply disingenuous. The immigration exemption at section 31(1)(g)[20] 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.[21]

- Existing Home Office powers and practice

The Government has 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*."[22] 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

[19] 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
[20] Freedom of Information Act 2000, Section 31, paragraph 1(g)
[21] 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
[22] Baroness Williams of Trafford in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1916

of the Data Protection Act. It will continue to be able to do so using the exemptions at Part 3 of the Bill, to the extent that fulfilling an individual's data protection rights would prejudice the prevention or detection of crime.

Making use of the law enforcement exemption 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 has already set out at length in its Committee Stage briefing,[23] using the law enforcement exemption in the Data Protection Act to facilitate administrative action against undocumented migrants is already standard, if highly unethical and problematic, Home Office practice. It is Liberty's view that 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 law enforcement exemption, the Home Office has more than sufficient powers to meet its objectives.

Baroness Williams set out two case studies at Committee Stage 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.[24] 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.[25] 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 law enforcement 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.

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-

[23] Liberty's Briefing on the Data Protection Bill for Committee Stage in the House of Lords, pages 18-20
[24] Baroness Williams of Trafford in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1914
[25] Baroness Williams, ibid.

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?

What Baroness Williams has admitted 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. Almost every known bulk data-sharing agreement that the Home Office has agreed with other government departments to target undocumented migrants has been concluded in secret, without being subject to any public or parliamentary scrutiny. In the case of data-sharing agreements that make use of information collected by frontline workers, including teachers, NHS workers and homelessness outreach workers, significant public outcry has ensued once the agreements were revealed, in each case through Freedom of Information Act requests.[26] It is already of significant concern that data-sharing agreements to target undocumented migrants have been operating, and even more so that they have been operating in secret. That further data usage by the Home Office relating to documented migrants and British citizens could be concealed using this exemption is of grave concern.

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 2 and 3. 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

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):

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

"*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.*"[27]

"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."*[28]

*"****We are using more data wherever we can****. One key element that that data enables us to do is to automate contact."*[29]

"In terms of retaining contact with people, and ***nudging people when their visa expiry time might be*** *[...].*[30]

"We need to make sure that ***we make it easy*** *for landlords, et cetera, to check someone's status*."[31]

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 data*[32]" 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.

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

[27] 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
[28] 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
[29] 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
[30] 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
[31] 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
[32]" 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

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

Baroness Williams describes the immigration control exemption in the Bill as "*a necessary and proportionate measure to protect the integrity of our immigration system*".[33]

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?"*[34]

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

---

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

[34] '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

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

The Government's future partnership paper on the exchange and protection of personal data[35] 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.[36] 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 a 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.

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*."[37] Lack of necessity, proportionality, and a risk to the fundamental human rights and freedoms have been highlighted above. But even if the exemption were

[35] *HM 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

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

[37] GDPR, Article 23(1)

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.[38]

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.

[38] GDPR, Article 23(2)

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

Amendments

General automated processing

Clause 13, page 7, line 16, 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 48, page 28, line 39, at end insert –

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

Intelligence services automated processing

Clause 94, page 54, line 31, insert after 'law' 'unless the decision engages an individual's rights under the Human Rights Act 1998'

Clause 94, page 54, line 34, leave out paragraph (c)

Clause 95, page 55, line 5, leave out paragraph (b) (*consequential to the amendment above)*

Effect

These amendments would clarify that **the exemption from prohibition on taking significant decisions based solely on automated processing must not apply to purely automated decisions that engage an individual's human rights**.

The amendments to Clause 94(2)(c) and Clause 95(2)(b) would **remove the exemption** for intelligence agencies to automatically process personal data to make decisions significantly affecting a data subject **for the purpose of considering, entering or performing a contract**.

Briefing

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.[39] 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."*[40]

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.[41] 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.[42]

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 humans.[43] Another recent study claimed that a machine learning tool was able to diagnose

[39] Data Protection Act 1998, s.12
[40] GDPR, Article 22(1)
[41] GDPR, Article 22(2)(b)
[42] 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*
[43] Deep neural networks are more accurate than humans at detecting sexual orientation from facial images (preprint) - Yilun Wang & Michal Kosinski, OSF, 15 Feb 2017

depression by scanning individuals' photos posted on the social media platform Instagram with greater accuracy than the average doctor.[44] 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[45] - if the decision is required or authorised by law.[46] 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.[47]

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.[48] 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 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

[44] Instagram photos reveal predictive markers of depression - Andrew G Reece & Christopher M Danforth, EPJ Data Science, 8 August 2017
[45] Data Protection Bill 2017, cl. 47(2)
[46] Data Protection Bill 2017, cl. 47(1) and cl. 48(1)(b)
[47] 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*
[48] 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

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[49] 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

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 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.

[49] 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*

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."*[50]

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.

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,*

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

> *proportionate, authorised under the law and fully compliant with the Human Rights Act."*[51]

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 any individual's HRA rights. Clearly, this amendment would not hinder automated decision-making with respect to decisions unrelated to individuals' HRA rights.

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."*[52]

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.

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

[52] Lord Ashton of Hyde in Data Protection Bill Committee Stage in the House of Lords, 13th November 2017 – Hansard, vol. 785, col.1872

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".*[53]

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."*[54]

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

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

[54] 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

Amendments

Delegated powers to amend safeguards for processing of sensitive personal data

Clause 9, page 6, line 4, leave out sub-section (6)

Clause 9, page 6, line 8, leave out sub-section (7).

Delegated powers to make further exemptions from data rights

Clause 15, page 8, line 42, leave out Clause 15.

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

Clause 33, page 20, line 24, leave out sub-section (6).

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

Clause 84, page 49, line 17, leave out sub-section (3)

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

Clause 111, page 61, line 20, leave out Clause 111.

Effect

These amendments would remove from the Bill excessively broad delegations of law-making power to the Secretary of State. Removing Clauses 15 and 111 would prevent the Secretary of State subverting Parliament's judgment and circumventing robust Parliamentary review of the scope of proper derogations from data privacy rights. Removing Clauses 9(6)-(7), 33(6) and 84(3) 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

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*."[55] 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.*"[56]

Liberty is calling for the five major areas of delegated powers identified above to be removed from the Bill[57] – the DPRRC has also called for the removal of those five delegated powers.[58] 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"*,[59] Baroness Williams assured the House that:

---

[55] 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).**

[56] Ibid.

[57] 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*

[58] 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).**

[59] 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.*"[60]

We urge parliamentarians 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

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