BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

Big Brother Watch's Briefing on the Data Protection Bill for Report Stage in the House of Commons

May 2018

CONTENTS

INTRODUCTION

The Data Protection Bill was published on the 13th September 2017.

Incorporating the EU General Data Protection Regulation (GDPR), which comes into force in the UK on 25th May 2018, the Data Protection Bill is the biggest transformation of data protection law in the UK since 1998.

In anticipation of Report Stage of the Data Protection Bill in the House of Commons, commencing on **Wednesday 9th May 2018,** we would like to draw your attention to a number of concerning issues within the Bill, and we propose amendments that are required in order to protect well-established privacy rights, maintain adequacy with EU law, and uphold the public's data protection rights.

We propose amendments, which have been tabled for Report stage, to:

- **Ensure that where human rights are engaged by automated decisions, there are always ultimately human decisions;**
- **Ensure that the protection of human involvement in automated decision-making is always meaningful;**
- **Uphold the existing application of data protection rights in the broad context of immigration data processing;**

We urge Members of Parliament to support these amendments to the Bill.

1. THE RIGHT NOT TO BE SUBJECT TO AUTOMATED DECISION-MAKING: ADDITIONAL SAFEGUARDS

Amendments

GENERAL PROCESSING[1]

Amendment No. 5 tabled by Brendan O'Hara, Stuart C. McDonald and Caroline Lucas[2]

Clause 14, page 8, line 11, 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)."
>
> "(2B) A decision is "based solely on automated processing" for the purposes of this section if, in relation to a data subject, there is no meaningful input by a natural person in the decision-making process."

Effect of the amendment

The first amendment (2A) to **Clause 14** would require that where human rights are engaged by decisions based solely on automated processing, the ultimate decision is always made by a human. This is achieved by clarifying that **the exemption set out in Clause 14**, which allows significant decisions based solely on automated processing, **does not apply to solely automated decisions that engage an individual's human rights.** The amendment to Clause 14 would install this vital protection for human rights with regards to the general processing of personal data.

The second amendment (2B) to **Clause 14** would **clarify the meaning of a decision "based solely on automated processing**", as a decision **lacking "meaningful human input**". This reflects the intent of the GDPR, and provides clarification that purely administrative human approval of an automated decision does make an automated decision a 'human' one.

[1] Data Protection Bill, Part 2, Chapter 2

[2] HC Notices of Amendments, Wednesday 2 May 2018 (https://publications.parliament.uk/pa/bills/cbill/2017-2019/0190/amend/data_rm_rep_0502.pdf)

LAW ENFORCEMENT PROCESSING[3]

Amendment No. 2 tabled by Brendan O'Hara, Stuart C. McDonald and Caroline Lucas

Clause 50, Page 30, line 28, at end insert –

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

Effect of the Amendment

The amendment to **Clause 50** would apply the same human rights protection as the amendment to Clause 14, but in the context of law enforcement processing

INTELLIGENCE SERVICES PROCESSING[4]

Amendment No. 3 tabled by Brendan O'Hara and Stuart C. McDonald

Clause 96, Page 56, line 38, after "law" insert –

> "unless the decision engages an individual's rights under the Human Rights Act 1998."

Effect of the Amendment

The amendment to **Clause 96** would apply the same human rights protection as the amendment to Clause 14 and Clause 50, but to intelligence services processing.

[3] Data Protection Bill, Part 3, Chapter 3

[4] Data Protection Bill, Part 4, Chapter 3

BRIEFING

Data is the lifeblood of our rapidly expanding information society.

Data aggregation, where a large amount of data is collated or collected together from multiple sources and analysed and observed for patterns, often using automated programs, systems or algorithms, is becoming a central tool in both the public and the private sector, used by businesses, public service providers, and the police.

This combination of advancing technology and hugely increasing volumes of data is leading to the categorisation of many aspects of people's lives by automated computer programs, from their shopping habits to biometric identifiers like faces or fingerprints, their record of accessing public services to their history of contact with law enforcement.

As a result, we are seeing a huge increase in the use of such automated processing to categorise and profile people, and subsequent automated decision-making systems making significant decisions on essential and important elements of people's lives.

Fortunately, the GDPR clarifies and extends safeguards for individuals against significant decisions based solely on automated processing.[5]

Article 22(1) of the GDPR provides that:

> "***Automated individual decision-making, including profiling***
>
> *"1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her"*.[6]

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

However, the Data Protection Bill currently **fails to provide sufficient safeguards** for data subjects' rights where it makes exemptions from this extremely important GDPR right in Clauses 14, 50 and 96.

[5] GDPR, Article 22

[6] GDPR, Article 22(1)

(i) AUTOMATED DECISION-MAKING (GENERAL PROCESSING):

a. *HUMAN RIGHTS ACT SAFEGUARD*

Clause 14 of the Bill permits exemptions from the right not to be subject to an automated decision in relation to "General processing" of personal data.[7] However, we believe that **such an exemption from this vital right should not be allowed where automated decisions engage human rights.**

Automated decisions may be relatively trivial, such as Amazon suggesting which books its customers might like, or they may be made in circumstances that can have critical consequences for someone's health, financial stability or employment. As Shadow Minister Liam Byrne MP (Digital, Culture, Media and Sport), noted at Committee in the House of Commons, "*In a number of areas of our lives—particularly our economic and social lives—such algorithms will become more and more important*."[8]

It is well documented that automated decision-making processes can carry discreet biases hidden in the datasets used, perpetuating discrimination. Automated decisions often involve opaque, unaccountable processes – preventing the reasons for a decision being examined, and potentially allowing such discrimination to fester.

The risks and unaccountability of automated systems are too great to permit purely automated decisions to be made where fundamental rights are at stake. Preventing automated decision-making from being used where it engages an individual's rights under the Human Rights Act 1998 would ensure procedural fairness and provide much needed protection against discriminatory decisions – issues which have become increasingly prevalent alongside the growing use of automated or algorithmic systems.[9]

Brendan O'Hara MP noted his concerns with this exemption at Committee stage:

> "*We strongly believe that automated decision making without human intervention should be subject to strict limitations to ensure fairness, transparency and*

[7] Data Protection Bill, Clause 14

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

[9] For example, there have been growing reports of AI or machine learning systems evidencing racial or gender biases, such as a Google job advert algorithm which was proven to show adverts for high-paying jobs much more often to men than to women, or multiple instances of image recognition algorithms erroneously recognising or failing to recognise people with dark skin. Recently, an algorithm was used to determine people's sexuality based on pictures of their face.

> *accountability, and to safeguard against discrimination. As it stands, there are insufficient safeguards in the Bill.*"[10]

Shadow Minister Liam Byrne MP also spoke about the dangers posed by allowing people's right to be engaged and affected by automated decisions: "*There are great risks in algorithms taking decisions in ways ungoverned by us.*"[11]

As a result, Big Brother Watch believes that it is paramount to provide a base level of fundamental human rights protection in relation to automated decisions, for people in the UK. The opportunity to deliver the right to human intervention and oversight in the most vital cases – where rights are at stake – is in this Bill.

Lord Clement-Jones, Lord Paddick, Baroness Hamwee, and Baroness Jones tabled this amendment to Clause 14 at Committee Stage in the House of Lords, and it was tabled by Brendan O'Hara MP and Stuart McDonald MP at Committee stage in the House of Commons.

In the Lords, Lord Ashton, Parliamentary Under-Secretary (Department for Digital, Culture, Media and Sport), incorrectly stated at Committee that the amendment would not allow *any* decisions based on automated decision-making:

> *"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."*[12]

Baroness Williams (Minister of State, Home Office) also repeated the mischaracterisation that "*practically all decisions would be caught by the prohibition.*"[13] However, it is not the case that "practically all decisions" would be affected by the amended clause.

Only **decisions** that are **purely automated**, **produce significant legal effects**, *and* **engage an individual's fundamental rights** would be required to have human involvement – a simple and vital protection.

Baroness Jones tabled the amendment again at Report Stage, and clarified for the Government the effect of the clause and amendment:

[10] Data Protection Bill, HC Public Bill Committee, 13 March 2018 (https://publications.parliament.uk/pa/cm201719/cmpublic/DataProtection/PBC153_Combined_1-8_22_03_2018_REV.pdf)

[11] Data Protection Bill, HL Report stage, 2nd day, 13 December 2017 (https://hansard.parliament.uk/lords/2017-12-13/debates/9622571E-8F1E-43F8-B018-C409A3129553/DataProtectionBill(HL))

[12] Data Protection Bill, HL Committee Stage, 3rd day, 13 November 2017 13 November 2017(https://hansard.parliament.uk/lords/2017-11-13/debates/F52C75EF-3CCC-4AC4-9515-A794F269FDAE/DataProtectionBill)

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

> *"My amendments do nothing to inhibit automated data processing (…). Automated data processing is unaffected by my amendments, which focus on* decisions *based on data, however the data is processed (…). [W]here human rights are engaged, the final* decision *must be made by a human being."*[14]

Brendan O'Hara MP also further clarified the intention of this protective amendment at Committee:

> "*[W]e are not talking about every automated decision. We are not talking about a tech company or an online retailer that suggests alternatives that someone may like based on the last book they bought or the last song they downloaded.* ***It is about decisions that can be made without human oversight that will or may well have long-term, serious consequences on an individual's health, financial status, employment or legal status.***"[15]

In the House of Lords, Baroness Jones concluded that:

> "*We have to have this vital safeguard for human rights. 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, (…) it is the computer's fault.*"[16]

Liam Byrne MP was also unequivocal about the need to pass this amendment to the Bill to protect people's fundamental rights from automated decisions: "*As parliamentarians, we have a particular duty to ensure that the appropriate safeguards are in place.*"[17]

We urge Members of Parliament to support this amendment to Clause 14 and provide this vital and necessary safeguard for people's human rights.

b. *MEANINGFUL HUMAN INPUT SAFEGUARD*

Clause 14 of the Bill states that the right not to be subject to an automated decision rests on whether that decision was "based *solely* on automatic processing".[18] Although this might appear to safeguard against decisions which are made "solely" based on automated processing, **this does not sufficiently protect against a situation where the human involvement**

[14] Data Protection Bill, HL Report stage, 2nd Day, 13 December 2017 (Emphasis added)
[15] Data Protection Bill, HC Public Bill Committee, 13 March 2018 (https://publications.parliament.uk/pa/cm201719/cmpublic/DataProtection/PBC153_Combined_1-8_22_03_2018_REV.pdf)
[16] *Ibid*
[17] Data Protection Bill, HC Public Bill Committee, 13 March 2018 (https://publications.parliament.uk/pa/cm201719/cmpublic/DataProtection/PBC153_Combined_1-8_22_03_2018_REV.pdf)
[18] Data Protection Bill, Clause 14(1) (emphasis added)

is so minimal as to be meaningless, such as a **merely administrative authorisation** of an automated decision by a human controller.

As it stands in the Bill, even the most minimal human input or token gesture lacking any influence over the decision could authorise an automated decision that has a significant legal effect. Such administrative input would circumvent the vital safeguard prohibiting such solely automated decisions. Big Brother Watch believes that this is not a sufficient protection.

Our concern was echoed by the Deputy Counsel to the Joint Committee on Human Rights, who has said that "*There may be decisions taken with minimal human input that remain de facto determined by an automated process*".[19]

At Committee stage in the House of Lords, Lord Ashton acknowledged that human intervention must be meaningful, stating that the Government's view is that the current phrasing of Clause 14 implies this meaning. He also stated:

> "*Mere human presence or token involvement would not be enough. The purported human involvement has to be meaningful; it has to address the basis for the decision. If a decision was based solely on automated processing, it could not have meaningful input by a natural person.*"[20]

Similarly, Baroness Williams noted at Report Stage that she was "*…sympathetic to the intention behind the amendment but the phrase… already provides for this.*"[21] She went on to state that the meaning had been clarified at Committee by Lord Ashton:

> "*…mere human presence or incidental human involvement is not sufficient to constitute meaningful input. The input must be meaningful. The level of human intervention required is already clarified in the text*".[22]

However, it is patently not the case that the Bill ensures that human input in automated processing is always meaningful. While the intended meaning of Clause 14 is as the Government has made clear, this is not reflected in its phrasing, or indeed anywhere in the Bill. There is no wording in the Bill at all that defines what constitutes an automated decision – and it would be entirely unsatisfactory to rely on Ministerial statements in Hansard to delineate the limitations of this vital right.

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

[20] Data Protection Bill, Committee stage, 3rd day, 13 November 2017(https://hansard.parliament.uk/lords/2017-11-13/debates/F52C75EF-3CCC-4AC4-9515-A794F269FDAE/DataProtectionBill)

[21] Data Protection Bill, Report stage, 2nd day, 13 December 2017 (https://hansard.parliament.uk/lords/2017-12-13/debates/9622571E-8F1E-43F8-B018-C409A3129553/DataProtectionBill(HL))

[22] *Ibid*

Baroness Williams also referred to Recital 71 of the GDPR, which she said "*already provides for this* [safeguard]", satisfying the Government that there is no need to make the protection explicit in the Bill.[23] However, Recital 71 only states that automated decisions are those "*without any human intervention*"[24] – not those without *meaningful* intervention, as Big Brother Watch, and, indeed, the Government agree must be the case.

As the lines between human and automated decisions become increasingly blurred and the stakes grow ever higher, the Bill provides an important opportunity to introduce a clear and simple safeguard – not a safeguard which is fundamentally flawed.

This amendment would **ensure clarity of the meaning of a decision based "solely on automated processing"** and **ensure it is unequivocally one that has "no meaningful human input".**

Big Brother Watch urges Members of Parliament to amend Clause 14 to reflect the intent of the GDPR, and prevent purely administrative human approval of automated decisions.

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

[24] GDPR, Recital 71 (emphasis added)

(ii) AUTOMATED DECISION-MAKING (LAW ENFORCEMENT PROCESSING): HUMAN RIGHTS ACT SAFEGUARD

The Bill also allows an exception from the right not to be subject to an automated decision in relation to "law enforcement processing",[25] allowing law enforcement agencies, such as UK police forces, to make decisions based solely on automated processing.

In the context of law enforcement processing, the potential for people's rights and liberties to be infringed by automated decisions is extremely serious.

Our amendment to Clause 50 would therefore prevent decisions based *solely* on automated processing which both have significant effects *and* engage an individual's rights under the Human Rights Act 1998.

AI systems are currently being used by UK police to predict crime,[26] predict people's likelihood of re-offending,[27] and to monitor and identify people's faces in crowds, leading to detention and arrest.[28] The use of AI in policing gives rise to new and complex concerns. Crucially, at present, these systems are subject to an officer's review and are not used to make solely automated decisions. However, the exemptions drawn in this Bill would permit these systems to make potentially life-changing decisions autonomously.

Predictive policing tools are used by Kent Police and have been trialled by Greater Manchester, West Midlands, Yorkshire and the Metropolitan Police. Multiple studies and reports have found that such systems can reinforce existing prejudice and bias.[29]

Durham Police have recently begun using an AI system which assesses the risk that a suspect may reoffend (Harm Assessment Risk Tool, known as HART),[30] influencing decisions on whether to prosecute or not. However, the researchers recently accepted that the AI system's use of postcode data may unfairly class people from deprived communities as 'high risk'.

Our recent investigations into Durham's HART custody decision-system have found that it used commercial profiling data on local postcodes to inform its risk assessments.[31] This profiling

[25] Data Protection Bill, Clause 50

[26] BBC Online (http://www.bbc.co.uk/news/technology-29824854)

[27] BBC Online (http://www.bbc.co.uk/news/technology-39857645)

[28] Sky News Online (https://news.sky.com/story/legal-questions-surround-police-use-of-facial-recognition-tech-11001595)

[29] Ensign et al, (2017) 'Runaway Feedback Loops in Predictive Policing', Cornell University Library 29 June 2019 https://arxiv.org/abs/1706.0984). Reported in the New Scientist (https://www.newscientist.com/article/mg23631464-300-biased-policing-is-made-worse-by-errors-in-precrime-algorithms/)

[30] BBC Online (http://www.bbc.co.uk/news/technology-39857645)

[31] Big Brother Watch, 'A Closer Look at Experian Big Data and Artificial Intelligence in Durham Police', 6 April 2018 (https://bigbrotherwatch.org.uk/2018/04/a-closer-look-at-experian-big-data-and-artificial-intelligence-in-durham-police/)

data, provided by data aggregation and marketing firm Experian, used, among others, GCSE results and benefits claimed, and included postcode stereotypes such as ‘Asian Heritage’.[32] Crucially, an officer currently reviews the risk assessment provided by the AI system before making a decision. This amendment would seek to protect the provision of such human involvement.

Further, UK police including the Metropolitan Police and South Wales Police are currently using commercial facial recognition technology to monitor and track individuals in public spaces.

Liam Byrne MP pointed out the chilling possibilities allowed by the exemption in Clause 50:

> “*On facial recognition at public events, for example, it would be possible under the [Bill] for the police to use facial recognition technology automatically to process those decisions and, through a computer, to have spot interventions ordered to police on the ground.*”[33]

These examples make clear the very serious threat that automated decisions by UK law enforcement could pose to people’s rights and liberties. Significant decisions in the context of law enforcement typically engage individuals’ rights under the Human Rights Act 1998 including the right to liberty, the right to a fair trial, the right to a private life, freedom of expression, freedom of assembly and the prohibition of discrimination. Those significant decisions must ultimately be human decisions.

However, the exemptions in the Bill in Clauses 49 and 50 would currently allow UK police to make decisions based purely on automated processing, engaging these fundamental rights, without any human input whatsoever. This not only poses a very current risk, but could lead to even greater future risks as automated technologies advance.

At Second Reading in the House of Commons, Liam Byrne MP recognised that algorithmic decision-making may “*hard-code old injustice into new injustice*”, and noted the serious concern that “*the Bill does not include adequate safeguards against that at the moment*”.[34]

Brendan O’Hara MP described the Clause 50 exemption as “*fraught with danger*”. He noted that the amendment to Clause 50 to ensure human intervention in law enforcement automated decisions which engaged human rights would provide “*transparency and accountability, and*

[32] *Ibid*

[33] Data Protection Bill, HC Public Bill Committee, 13 March 2018 (https://publications.parliament.uk/pa/cm201719/cmpublic/DataProtection/PBC153_Combined_1-8_22_03_2018_REV.pdf)

[34] Liam Byrne in Second Reading of the Data Protection Bill in the House of Commons, 5 March 2018

ensure that the state is not infringing an individual's fundamental rights, liberties and privacy" – values which are "*beyond the concept of an algorithm".*[35]

Baroness Hamwee summarised the principle in the Report Stage debate very succinctly: "*human rights, so human decision*".[36]

Big Brother Watch urges Members of Parliament to amend the Bill and ensure that any significant law enforcement decisions, which engage human rights, require human input.

[35] Brendan O'Hara in Second Reading of the Data Protection Bill in the House of Commons, 5 March 2018

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

(iii) AUTOMATED DECISION-MAKING (INTELLIGENCE SERVICES PROCESSING): HUMAN RIGHTS ACT SAFEGUARD

The Bill also provides for an exception from the right not to be subject to an automated decision in relation to "intelligence services processing".[37] The amendment to **Clause 96** would provide the same minimum protection, based on human rights law, as the amendments proposed to Clause 14 and Clause 50.

This amendment 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. However, crucially, this amendment would **prevent decisions based *solely* on automated processing, and which have significant effects*, if those decisions engage an individual's rights under the Human Rights Act 1998*.**

We urge Members of Parliament to support the amendment to Clause 96, rejecting the exemption from this vital right where decisions based *solely* on automated processing have both significant effects *and* engage an individual's rights under the Human Rights Act 1998.

This amendment would prevent UK citizens being subject to decisions based purely on automated-processing which affect their right to liberty, privacy and the prohibition of discrimination.

At Report stage in the House of Lords, Baroness Williams responded to this tabled amendment as follows:

> *"The intelligence services may use automated processing in their investigations, perhaps in a manner akin to a triage process to narrow down a field of inquiry. The **decision arising from such a process may be to conduct a further search** of their systems; arguably, **that decision significantly affects a data subject and engages that individual's human rights.** As such, it would be prohibited by the amendment, potentially impeding appropriate investigative work around identifying national security threats…"*[38]

Baroness Williams appeared to suggest that the intelligence services would automatically "conduct a further search" relating to an individual/s, **based on purely automated processing. This is precisely the situation that must be prohibited, not only in light of the GDPR, but indeed in any modern rights-respecting democracy.**

[37] Clause 96(2)

[38] Data Protection Bill, Report stage, 2nd day, 13 December 2017 (https://hansard.parliament.uk/lords/2017-12-13/debates/9622571E-8F1E-43F8-B018-C409A3129553/DataProtectionBill(HL))

This issue is of growing importance as investigative technologies are advancing with unprecedented pace - and it is of particular relevance in the context of the intelligence services, where the processing of bulk datasets and bulk intercept is routine. Individual warrants are not necessarily required for intelligence agencies to process or access an individuals' personal data, but an assessment of necessity and proportionality *is* required. Therefore, human input is clearly required.

We do not believe that it would or should be legally defensible to subject an individual to further intrusion by the intelligence agencies, significantly engaging their Article 8 rights, on the basis of a purely automated decision – human involvement in a decision must always be explicitly required.

Big Brother Watch urges Members of Parliament to include this safeguard in the Bill in order to protect fundamental rights in relation to automated processing by the intelligence services.

2. THE IMMIGRATION EXEMPTION

Amendment

Amendment No. 15, tabled by a number of Members of Parliament[39]

Schedule 2

Page 141, line 17, leave out paragraph 4.

Effect of the Amendment

This amendment removes the exemption to data subjects' rights where personal data is being processed for the maintenance of effective immigration control.

BRIEFING

Schedule 2, paragraph 4 of the Bill, hereafter referred to as the "immigration exemption", sets out an extremely broad and wide-ranging exemption allowing the restriction of the majority of data subject's key GDPR rights where their personal data is processed for "*the maintenance of effective immigration control*" or for "*the investigation or detection of activities that would interfere with effective immigration control*".

The immigration exemption would introduce a new and unprecedented removal of rights in the UK's data protection framework. The breadth of data protection rights this exemption removes is completely unnecessary and disproportionate.

The exemption removes the following rights from individuals:

- **A range of vital GDPR rights** (right to access, right to erasure, right to restrict processing, right to object to processing); and

- **All the principles** in Article 5 of the GDPR (which require that processing must be lawful, fair and transparent, accurate, adequate, for explicit and legitimate purposes, processed in a manner that is secure, and limited to the specific original processing purpose).

[39] HC Notices of Amendments, Wednesday 2 May 2018 (https://publications.parliament.uk/pa/bills/cbill/2017-2019/0190/amend/data_rm_rep_0502.pdf)
Tabled by: Tom Watson, Liam Byrne, Louise Haigh, Chris Elmore, Sir Edward Davey, Layla Moran, Tim Farron, Christine Jardine, Caroline Lucas, Jamie Stone, Jo Swinson, Tom Brake, Stephen Lloyd, Wera Hobhouse, Mr Alistair Carmichael

There is no similar provision in the current Data Protection Act 1998. This is an entirely new and far-reaching exemption from crucial data protection rights. A similar provision was included in a draft of the 1983 Data Protection Bill, but was removed after being called "*a palpable fraud on the public if [it] were allowed to become law*" by the House of Lords' Committee on the Data Protection Bill at the time.[40]

The Bill already contains data protection exemptions in relation to criminal immigration offences, in Schedule 2, paragraphs 2 and 3. The immigration exemption is an entirely unrelated and additional power. This removal of rights has nothing to do with those who are suspected to have committed immigration offences, or even those who have actually committed immigration offences.

There is no definition in the Bill of "*immigration control*", or "*the effective maintenance of immigration control*". As demonstrated by recent political divides not only in the UK but in the US and elsewhere, "effective immigration control" is, as described by Brendan O'Hara MP at Committee, "*highly subjective and highly politicised*".[41] The impact of various approaches renders individuals' rights vulnerable to political whims.

Lord Lucas argued at Committee stage that the Bill is undermined "*in all sorts of insidious ways by having such a broad and unjustified clause*",[42] while Baroness Hamwee noted at Report that "*this [exemption] is very far-reaching indeed*".[43] She added that the second limb of the exemption "*gives scope for quite considerable fishing expeditions*",[44] allowing the restriction of people's data protection rights in extremely broad circumstances.

The Equality and Human Rights Commission has stated that this exemption could:

> "*…permit the authorities to access and process highly personalised data, for example, phone or social media relating to sexual lives of immigrants claiming residency rights on the basis of their relationship with a British citizen*."[45]

[40] Lord Elystan-Morgan, Data Protection Bill [H.L.] HL Deb 21 July 1983 vol 443 cc1269- 311 (http://hansard.millbanksystems.com/lords/1983/jul/21/data-protection-bill-hl#S5LV0443P0_19830721_HOL_172 - accessed 07/12/17)

[41] Data Protection Bill, HC Public Bill Committee, 13 March 2018 (https://publications.parliament.uk/pa/cm201719/cmpublic/DataProtection/PBC153_Combined_1-8_22_03_2018_REV.pdf)

[42] Data Protection Bill, Committee stage, 3rd day, 13 November 2017 (https://hansard.parliament.uk/lords/2017-11-13/debates/F52C75EF-3CCC-4AC4-9515-A794F269FDAE/DataProtectionBill)

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

[44] *Ibid*

[45] EHRC Written Evidence to the Joint Committee on Human Rights, quoted in the Note from Deputy Counsel, 'The Human Rights Implications of the Data Protection Bill', 6 December 2017 (https://www.parliament.uk/documents/joint-committees/human-rights/correspondence/2017-19/Note_Deputy_Counsel_DPBill.pdf)

The exemption is therefore extremely broad, and would also seem to apply to all individuals engaged in the immigration system – whether that is British citizens who are partners or family members of those engaged with the immigration system, or EU citizens.

The Deputy Counsel to the JCHR has described the potential for discriminatory impact against non-nationals, making it abundantly clear that "*any discrimination on the basis of nationality would engage Article 14 (in conjunction with Article 8 ECHR) as well as Articles 7, 8 and 21 of the Charter*".[46]

This exemption could be applied extremely widely. Due to the many data-sharing agreements that the Home Office has with other departments, there is the very serious likelihood that this may restrict an individual from finding out what information the government holds about them, or how that data is being used and shared, in a context entirely removed from immigration control. Baroness Hamwee considered this at Report stage:

> "*Immigration control has expanded in nature over the last few years. It stretches beyond the Home Office to the activities and functions of public bodies and private individuals in providing housing, healthcare, employment, education, social assistance, banking facilities, driving licences and marriage registration, as well as the private sector in carrying out functions for the state such as immigration removal centres*."[47]

The Information Commissioner has echoed concerns about the potential application of this exemption stating that it "*could also draw in organisations who are processing personal data for the purposes of checking right to work status of individuals for example*."[48]

Individuals involved in the asylum and immigration process would almost certainly be unable to access their data. At Report stage in the House of Lords, an amendment to the immigration exemption removed the right to rectification from the list of rights exempt; however, the exemption restricts individuals from exercising their right of access, so they will never be able to know if the data that is held about them is accurate, and/or whether any rectifications are necessary. As Liam Byrne MP noted, in response to arguments put forward by the Government at Committee stage, "*The idea that the Home Office will seek to regularise someone's*

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

[47] Data Protection Bill, Report stage, 2nd day, 13 December 2017 (https://hansard.parliament.uk/lords/2017-12-13/debates/9622571E-8F1E-43F8-B018-C409A3129553/DataProtectionBill(HL))

[48] ICO Briefing (2017),' Data Protection Bill, House of Lords Report Stage –Information Commissioner's briefing – Annexx II, https://ico.org.uk/media/about-the-ico/documents/2172865/dp-bill-lords-ico-briefing-report-stage-annex-ii-20171207.pdf

immigration status by denying them access to information that might support their case is, frankly, fanciful."[49]

The Information Commissioner has criticised the potential harm these exemptions may cause to those undergoing the asylum process:

> "*If the exemption is applied, individuals will not be able to access their personal data to identify any factual inaccuracies and it will mean that the system lacks transparency and is fundamentally unfair*."[50]

The Deputy Counsel to the Joint Committee on Human Rights (JCHR) has also questioned "*why immigration control requires exemptions from fundamental principles such as lawfulness, fairness and accuracy in order to maintain its effectiveness*. She asserted that "*it is arguably disproportionate to extend such restrictions to immigration control, particularly so in relation to lawful immigration*."[51]

The Government has failed to provide any sufficient justification for the necessity of the immigration exemption. At Committee and Report stage of the House of Lords, the Government failed to address the concerns raised and did not offer any reasonable justification. Likewise, at Committee in the House of Commons, the Government could not give any legitimate justification for the immigration exemption.

At Committee stage, Victoria Atkins MP (Parliamentary Under Secretary of State at the Home Office), gave several examples of activity which would supposedly necessitate the removal of data protection rights, per this exemption, for "effective immigration control". However, as pointed out by Liam Byrne MP, these examples would all be considered 'criminal' immigration offences under the Schedule 2, paragraph 2(1)(a) exemption in relation to the prevention of crime, and are already covered.[52] The Schedule 2, paragraph 4 immigration exemption is an *additional* and much broader and further reaching exemption, which is completely unnecessary.

[49] Data Protection Bill, HC Public Bill Committee, 13 March 2018 (https://publications.parliament.uk/pa/cm201719/cmpublic/DataProtection/PBC153_Combined_1-8_22_03_2018_REV.pdf)

[50] ICO Briefing (2017),' Data Protection Bill, House of Lords Report Stage –Information Commissioner's briefing – Annexx II, https://ico.org.uk/media/about-the-ico/documents/2172865/dp-bill-lords-ico-briefing-report-stage-annex-ii-20171207.pdf

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

[52] Data Protection Bill, HC Public Bill Committee, 13 March 2018 (https://publications.parliament.uk/pa/cm201719/cmpublic/DataProtection/PBC153_Combined_1-8_22_03_2018_REV.pdf)

In response to these inaccurate examples provided by Victoria Atkins MP, Liam Byrne MP said "*I am really sorry to have to say this, but that is utter nonsense."*[53]

This exemption may be incompatible with the GDPR, leading to serious consequences in relation to a future data-sharing adequacy agreement with the EU post-Brexit. We are very concerned that the inclusion of this exemption may be incompatible with the GDPR, as well as having a significantly disproportionate and discriminatory effect.

The immigration exemption goes much further than the scope of restrictions afforded to Member States under the GDPR. Article 23(1) of the GDPR allows Member States to make restrictions to GDPR rights, as long as any restriction to GDPR rights "*respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society*" in order to safeguard any of the areas of competency that are listed. These areas include national security, defence, public security, and preventing and investigating crime.[54] Immigration is not included in that list.

At Report stage, Baroness Williams echoed this: "*It [article 23 of the GDPR] does not expressly allow restrictions for the purposes of immigration control*."[55] The Deputy Counsel to the JCHR also stated that "*The GDPR does not expressly provide for immigration control as a legitimate ground for exemption*".[56]

We believe that allowing this provision to remain would significantly encroach on the UK's ability to achieve adequacy with EU law, on the basis that it is at odds with Article 23(1) of the GDPR.

Big Brother Watch believes that this exemption has the potential to be extremely harmful. This exemption is also a serious concern for Liberty and a broad range of civil society and rights organisations that are also calling for the removal of this exemption.

We call on Members of Parliament to reject this wholesale exemption of rights for the supposed purpose of 'immigration control'.

[53] Data Protection Bill, HC Public Bill Committee, 13 March 2018 (https://publications.parliament.uk/pa/cm201719/cmpublic/DataProtection/PBC153_Combined_1-8_22_03_2018_REV.pdf)

[54] General Data Protection Regulation, Article 23(1)(a) - (j).

[55] Data Protection Bill, Report stage, 2nd day, 13 December 2017 (https://hansard.parliament.uk/lords/2017-12-13/debates/9622571E-8F1E-43F8-B018-C409A3129553/DataProtectionBill(HL))

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

BIG BROTHER WATCH

DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

About Big Brother Watch

Big Brother Watch is a civil liberties and privacy campaigning organisation. We hold to account those who fail to respect our privacy, and campaign to give individuals more control over their personal data. We produce unique research exposing the erosion of civil liberties in the UK, looking at the dramatic expansion of surveillance powers, the growth of the database state and the misuse of personal information.

Contact

Silkie Carlo

Director

Direct line: 020 7340 6042

Email: silkie.carlo@bigbrotherwatch.org.uk

Griff Ferris

Legal and Policy Officer

Direct line: 020 7340 6074

Email: griff.ferris@bigbrotherwatch.org.uk