BIG BROTHER WATCH

DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

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

March 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 in May 2018, the Data Protection Bill is the biggest transformation of data protection law in the UK since 1998.

In anticipation of Committee Stage of the Data Protection Bill in the House of Commons, commencing on **Tuesday 13 March 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 to:

- Ensure that where human rights are engaged by automated decisions, there are always ultimately human decisions;
- Ensure that the safeguard 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 would also like to draw your attention to elements within the Bill which are of concern:

- The national security certification regime which lacks oversight and time-limitation; and
- The issue of whether the UK's data protection regime is sufficiently protective to be subject to an 'adequacy' decision in order to share data freely with the EU post-Brexit.

1. **The right not to be subject to automated decision-making: exceptions and additional safeguards**

Amendments

General processing[1]

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

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

Clause 14, page 7, line 40, at end insert -

"(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."

Law enforcement processing[2]

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

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

Intelligence services processing[3]

Clause 96, Page 56, line 8, after "law" insert –

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

[1] Data Protection Bill, Part 2, Chapter 2
[2] Data Protection Bill, Part 3, Chapter 3
[3] Data Protection Bill, Part 4, Chapter 3

Effect of the Amendments

The first amendment to Clause 14 would require that where human rights are engaged by automated decisions, there are always ultimately human decisions. This is achieved by clarifying any **exemption** from the **prohibition on taking significant decisions based solely on automated processing does not apply to purely automated decisions that engage an individual's human rights**. This amendment to Clause 14 would install this vital protection of human rights with regards to the general processing of personal data; the amendment to Clause 50 would apply the protection in the context of law enforcement processing, and the amendment to Clause 96 would apply to intelligence services processing.

The second amendment to Clause 14 would clarify the meaning of a decision "based solely on automated processing", which is 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.

BRIEFING

As the Government noted in its Statement of Intent on the planned reforms made by the Data Protection Bill, "*Our digital economy is creating mind-boggling quantities of personal data*".[4]

Data aggregation, where large amounts 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 services providers, and law enforcement.

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 their biometric information, their record of accessing public services to history of contact with law enforcement.

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

[4] Department for Digital, Culture, Media and Sport, Statement of Intent, 'A New Data Protection Bill: Our Planned Reforms', 7 August 2017, page 4(https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/635900/2017-08-07_DP_Bill_-_Statement_of_Intent.pdf)

The Data Protection Act 1998 provides the right not to be subjected to 'purely automated decision-taking.' 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.

AUTOMATED DECISION-MAKING: HUMAN RIGHTS ACT SAFEGUARD

(i) General processing)

Clause 14 of the Bill permits exemptions from the right not to be subject to an automated decision in relation to "[g]eneral processing" of personal data.[7] However, we believe that such an exemption from this vital right should not be granted where 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.

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. The risks and unaccountability of automation 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 would ensure procedural fairness and provide much needed

[5] GDPR, Article 22
[6] GDPR, Article 22(1)
[7] Data Protection Bill, Article 14

protection against discriminatory decisions – issues which have become increasingly prevalent alongside the growing use of automated systems.[8]

As a result, Big Brother Watch believes that it is paramount to provide a base level of fundamental human rights protection for UK citizens in relation to automated decisions. In the 'Leaving the EU: Data Protection' debate in the House of Commons, Darren Jones MP noted "*…grave concern about whether, when we bring in machine learning and changing algorithms, it is even possible to deliver the right to human intervention."*[9] The opportunity to make human intervention not only possible but necessary 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. Lord Ashton, Parliamentary Under-Secretary (Department for Digital, Culture, Media and Sport), stated in response 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."*[10]

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

> *"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."*[11]

Despite this, Baroness Williams (Minister of State, Home Office) repeated the mischaracterisation that "*practically all decisions would be caught by the prohibition."*[12]

However, it is plainly not the case that "practically all decisions" would be affected by the amended clause. Only decisions that are purely automated, produce significant legal effects,

---

[8] 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.

[9] Leaving the EU; Data Protection, House of Commons, 12 October 2017 (https://hansard.parliament.uk/Commons/2017-10-12/debates/20F0DCC3-149D-470D-8AF0-2DE02400D4D0/LeavingTheEUDataProtection)

[10] 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)

[12] 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))

***and* engage an individual's fundamental rights would invoke the simple and vital protection of human involvement.**

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.*"[13]

We urge the Committee to amend Clause 14, and provide this vital and necessary safeguard for people's human rights in the context of automated decision-making regarding "general processing" of people's personal data.

(ii) Law enforcement processing

The Bill also provides for an exception from the right not to be subject to an automated decision in relation to "law enforcement processing",[14] 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 processing is extremely serious.

Automated decision-making systems are currently being used by UK police to predict crime,[15] predict people's likelihood of re-offending,[16] and to monitor and recognise people's faces in crowds, leading to detention and arrest.[17] The use of automated decision-making algorithms, machine learning systems, and even basic 'artificial intelligence' programs by UK police give rise to new and complex concerns, and necessitate basic human rights protections.

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 similar systems can reinforce prejudice and bias.[18]

---

[13] *Ibid*

[14] Data Protection Bill, Clause 50

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

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

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

[18] 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/)

Durham Police have recently begun using an automated decision making system which assesses the likelihood of a person to reoffend (HART – Harm Assessment Risk Tool).[19] While this is in its early stages, a comparable program used by US authorities was found to exhibit significant racial bias.[20]

Further, UK police including the Metropolitan Police and South Wales Police are currently using facial recognition technology to monitor and track individuals in public spaces. Similar technology has also been proven to display troubling accuracy biases across race and gender, in particular misidentifying women and black people.[21]

These examples make clear the very serious potential threat to people's rights and liberties by automated decision-making processes used by UK law enforcement. Automated processing in the context of law enforcement frequently engages 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.

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

At Second Reading in the House of Commons, Shadow Minister (Digital, Culture, Media and Sport) Liam Byrne MP acknowledged the risk that algorithmic decision-making may "*hard-code old injustice into new injustice",* and correspondingly, that "*the Bill does not include adequate safeguards against that at the moment, so we will need to address that".*[22]

Brendan O'Hara MP described the Government's exemption as "*fraught with danger"* and *"not only at odds with the Data Protection Act 1998, but against article 22 of the GDPR".* Big Brother Watch agrees with his analysis that human intervention would provide vital "*transparency and accountability, and ensure that the state is not infringing an individual's fundamental rights, liberties and privacy"* – values which are "*beyond the concept of an algorithm".*[23]

Big Brother Watch urges the Committee to amend the Bill and ensure that any decisions

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

[20] ProPublica (https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing)

[21] The Atlantic (https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/)

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

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

engaging human rights should require human input. Baroness Hamwee summarised the principle in the Report Stage debate very succinctly: "*human rights, so human decision*".[24]

(iii) Intelligence services processing

The Bill also provides for an exception from the right not to be subject to an automated decision in relation to "intelligence services processing".[25] **We urge the Committee to reject this 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.**

The amendment to Clause 96 would provide the same minimum protection, based on human rights norms, as the amendments proposed to Clause 14 and Clause 50 in relation to general processing and law enforcement processing respectively. 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 not allow any decisions based *solely* on automated processing which both have significant effects *and* engage an individual's rights under the Human Rights Act 1998**.

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

At Report Stage, Baroness Williams responded to this tabled amendment explaining,

> "*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…*"[26]

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.** This issue is of growing importance as investigative

---

[24] 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))

[25] Clause 96(2)

[26] 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))

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 the Committee to include this safeguard in the Bill in order to protect fundamental rights in relation to automated processing by the intelligence services.**

AUTOMATED DECISION-MAKING: MEANINGFUL HUMAN INPUT SAFEGUARD

(i) General processing:

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".[27] 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 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 actual influence over the decision could authorise an automated decision that has a significant legal effect, in order to circumvent this 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*".[28]

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 implies this meaning. He also stated:

---

[27] Data Protection Bill, Clause 14(1) (emphasis added)

[28] 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)

> "*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.*"[29]

Similarly, Baroness Williams noted at Report Stage that she was "*…sympathetic to the intention behind the amendment but the phrase… already provides for this.*"[30] 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*".[31]

However, this is patently not the case. While the intended meaning of the Clause is as the Government has made clear, this is not reflected in the phrasing of the Clause, 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.

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.[32] However, Recital 71 only states that automated decisions are those "*without any human intervention*"[33] – not those without *meaningful* intervention, as Big Brother Watch and 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 parliamentarians to amend Clause 14 to this effect.**

---

[29] 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)

[30] 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))

[31] *Ibid*

[32] 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))

[33] GDPR, Recital 71 (emphasis added)

2. Immigration exemption

Amendment

Schedule 2

Page 136, line 29, 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).

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.*"[34]

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*", asserting that "*it is arguably disproportionate to extend such restrictions to immigration control, particularly so in relation to lawful immigration.*"[35]

There is no similar provision in the current Data Protection Act 1998. A similar provision was originally 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.[36]

The Bill already contains data protection exemptions in relation to criminal immigration offences, in Schedule 2, paragraphs 2 and 3. This 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.

The Information Commissioner has criticised the breadth of data protection rights taken away under this exemption, stating that even an immigration exemption in relation to criminal offences should not restrict "*all the other 'GDPR provisions' which would be exempted*".[37]

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 a highly subjective goal and a politicised issue, with the impact of various approaches rendering individuals' rights vulnerable to political tides.

---

[34] 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

[35] 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)

[36] 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)

[37] 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

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*",[38] while Baroness Hamwee noted at Report that "*this [exemption] is very far-reaching indeed*".[39] She added that the second limb of the exemption "*gives scope for quite considerable fishing expeditions*",[40] 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*."[41]

This exemption 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*".[42]

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.

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:

---

[38] 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)

[39] 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))

[40] *Ibid*

[41] 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)

[42] 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)

"*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*."[43]

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*."[44]

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.[45] **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*."[46] The Deputy Counsel to the JCHR also stated that "*The GDPR does not expressly provide for immigration control as a legitimate ground for exemption*".[47]

The Government's response at Committee and Report stage has failed to address the concerns raised and did not offer any reasonable justification for this exemption. **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.**

---

[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] 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

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

[46] 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))

[47] 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 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 pushing for the removal of this exemption. **We call on the Committee to reject this wholesale exemption of rights for the purpose of 'immigration control'.**

3. National Security Certificates

Clause 26 and Clause 27 of the Data Protection Bill provide for a national security certification regime which allows the restriction of and exemption from a wide range of rights under the GDPR and the Bill itself, on the basis of national security and defence.[48]

The Data Protection Act 1998 also provides for the withdrawal of some data protection rights on the basis of 'safeguarding national security'.[49] However, the rights which can be restricted under a certificate in the Bill go much further than the current regime under the 1998 Act. The list of rights that can be restricted is set out in Clause 26 of the Bill and includes all the rights of data subjects under Chapter III of the applied GDPR: the right to be informed when personal data is collected from them (Article 13), the right to find out whether personal data about them is being processed (Article 15), and the right to object against automated decision-making (Article 21 and 22).

These exemptions are exercised by a certificate which is 'signed by a Minister', who certifies that an exemption from the rights and obligations is necessary 'for the purpose of safeguarding national security'.[50]An example of a certificate under this regime would be the exemption of GDPR and Data Protection Act rights and principles in relation to the use of Automatic Number Plate Recognition technology by Transport for London in relation to the Congestion Charging Zone in Central London, traffic management and enforcement in the Greater London area, and the Low Emission Zone.[51]

However, Big Brother Watch is concerned about the lack of oversight, the lack of consideration of fundamental principles of necessity and proportionality, and the indefinite nature of these certificates.

Necessity and proportionality

Currently, there are no conditions or tests imposed on the Minister's decision to withdraw individual's personal data protection rights under a national security certificate. We have no doubt that the principles of necessity and proportionality, enshrined in the European Convention on Human Rights as conditions under which a right such as the Article 8 right to privacy may be limited, would be taken into account by a Minister when considering such a restriction of individuals' rights in practice. However, **it is necessary to codify that consideration into statute,**

[48] Data Protection Bill, Clause 26.

[49] Section 28

[50] Data Protection Bill, Clause 27(1)

[51] Example: National Security Certificate under the DPA 1998 (http://amberhawk.typepad.com/files/blog-s.28-may-tfl-certificate-2011.pdf)

with a provision explicitly requiring the Minister to undertake such a necessity and proportionality test when considering whether to exempt personal data protection rights.

Judicial oversight

As Baroness Hamwee noted at Committee Stage in the House of Lords, national security certificates are "*not subject to immediate, direct oversight*".[52] They can take away all of the rights listed above, merely identifying data 'by means of a general description'.[53]

As the Bill is currently drafted, national security certificates are remarkably unusual in that people's rights could be removed by a politician without any form of oversight. We believe **it is essential that there is judicial oversight over the national security certification regime, which allows the restriction of a broad range of crucial data protection rights on a Minister's say-so.**

Time limitation

There is no limitation on the length of time a national security certificate is in operation and no duty to review the ongoing necessity of a certificate. They are, currently, open-ended and indefinite.

Baroness Williams has stated that national security certificates are "*are general and prospective in nature, and arguably no purpose would be served by a requirement that they be subject to a time limitation."*[54] However, we believe **it *is* necessary for these certificates to be time-limited**, for the same reasons that any warrant or certificate that limits citizens' rights in pursuit of state interests is time-limited. A time limitation would promote oversight of a regime that restricts a host of important personal data protection rights. Indefinite national security certificates may allow a data controller and processor to rely on a national security certificate for activities that were not considered by the Minister when the certificate was signed. Expiry of a certificate would not prevent it from being re-certified; it would simply ensure that those certificates which are no longer necessary or which are being used beyond their original remit do not continue indefinitely, and that there is some form of review after a certain period of time.

---

[52] Data Protection Bill, Committee stage, 4th day, 15 November 2017 (https://hansard.parliament.uk/Lords/2017-11-15/debates/9DC4D211-3573-4D97-82DB-92B75547B506/DataProtectionBill(HL))

[53] Data Prototection Bill, Clause 27(2)(a)

[54] Data Protection Bill, Committee stage, 4th day, 15 November 2017 (https://hansard.parliament.uk/Lords/2017-11-15/debates/9DC4D211-3573-4D97-82DB-92B75547B506/DataProtectionBill(HL))

4. Adequacy

The issue of adequacy after the UK leaves the European Union is absolutely critical for the UK post-Brexit. Adequacy refers to the level of data protection required by countries in the EU in order to share personal data across borders.

The Data Protection Bill updates our data protection laws for the digital age. In particular, it provides for the incoming General Data Protection Regulation (GDPR), which, as an EU regulation, has direct effect in the UK, and comes into force in May 2018. The Data Protection Bill makes alterations and amendments to elements of the GDPR, as well as providing for data protection rights and obligations in relation to law enforcement and intelligence services processing of personal data incorporating the EU Law Enforcement Directive[55] and the revised Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing.[56]

Only countries in the European Economic Area (EEA) (an area in which goods and services pass freely between countries, which includes all EU countries and a few others) **can transfer data between each other**, because as part of the EEA **they all have to adhere to the same high standards of protection around personal data and its transfer.** In other words these countries have, by complying with the same data protection laws, reached an agreed level of adequacy. The GDPR will represent the standard of data protection required across the EEA and EU.

If a country within the EU or EEA wants to transfer personal data to a non-EEA or non-EU country, it can only do so if a similar *"adequate"* level of protection of that personal data is guaranteed by the external country.[57] Adequacy decisions are made by the EU Commission. Whether or not a country's data protection regime is considered adequate is down to its domestic laws or the international commitments it has entered into.[58]

As noted by Wes Streeting MP in the 'Leaving the EU: Data Protection' in the House of Commons, *"the UK will… cease to be a member of the EU's safe data zone following Brexit".*[59] Therefore, in order to ensure the free flow of personal data between the UK and the EU, **the UK will have to prove our data protection framework reaches the required level of adequacy.** Lord Stevenson made it clear at Committee stage in the House of Lords that:

---

[55] European Parliament (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG)

[56] Council of Europe (https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108)

[57] European Commission (http://ec.europa.eu/justice/data-protection/international-transfers/index_en.htm)

[58] *Ibid*

[59] Leaving the EU: Data Protection, House of Commons, 12 October 2017 (https://hansard.parliament.uk/Commons/2017-10-12/debates/20F0DCC3-149D-470D-8AF0-2DE02400D4D0/LeavingTheEUDataProtection)

> "*If we are unable to reach such an agreement with the EU, there will be no legal basis for the lawful operation of countless British businesses and there will also be a significant question of whether EU companies will be able to trade with us*".[60]

An adequacy agreement is very much in the UK's interest. The Government future partnership paper, "The exchange and protection of personal data",[61] published in August 2017, makes clear that "*Any disruption in cross-border data flows would… be economically costly to both the UK and the EU*", and unequivocally states that "*it is essential that we agree a UK-EU model for exchanging and protecting personal data*".[62] It would indeed by economically costly for the UK if an adequacy agreement was not struck to allow the free flow of data to the EU; as Vicky Ford MP stated in the Commons EU data protection debate, "*the UK is home to more than 10% of all global data flows, with three quarters of those flows being between the UK and the rest of Europe*".[63] Lord Stevenson also noted in the House of Lords that:

> "*It is common ground among all the parties that it is essential that immediately after Brexit, the government should obtain an adequacy agreement from the [European] Commission so that UK businesses can continue to exchange personal data with EU countries and vice versa*".[64]

In the "Leaving the EU: Data Protection" debate in the House of Commons, the Secretary of State for Digital, Culture, Media and Sport, Matt Hancock MP, confirmed that the Government "*wish[es] to ensure the unhindered free flow of data between countries*", and that "*it is strongly in the mutual interests of the UK and the rest of the EU that such an [adequacy] arrangement is put in place".*[65] This was echoed by Vicky Ford MP in a debate on consumer protection after Brexit, who said that "*it is extraordinarily important for British and European consumers that we continue to have a free flow of data post-Brexit.*"[66]

---

[60] Data Protection Bill, Committee stage, 1st day, 30 October 2017 (https://hansard.parliament.uk/Lords/2017-10-30/debates/742E113F-2770-49B4-9985-47300C8268A4/DataProtectionBill(HL))

[61] HM Government (2017) (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/639853/The_exchange_and_protection_of_personal_data.pdf)

[62] *Ibid*

[63] Leaving the EU; Data Protection, House of Commons, 12 October 2017 (https://hansard.parliament.uk/Commons/2017-10-12/debates/20F0DCC3-149D-470D-8AF0-2DE02400D4D0/LeavingTheEUDataProtection)

[64] Data Protection Bill, Committee stage, 1st day, 30 October 2017 (https://hansard.parliament.uk/Lords/2017-10-30/debates/742E113F-2770-49B4-9985-47300C8268A4/DataProtectionBill(HL))

[65] Leaving the EU: Data Protection, House of Commons, 12 October 2017 (https://hansard.parliament.uk/Commons/2017-10-12/debates/20F0DCC3-149D-470D-8AF0-2DE02400D4D0/LeavingTheEUDataProtection)

[66] Leaving the EU: Consumer Protection, House of Commons, 10 October 2017 (https://hansard.parliament.uk/Commons/2017-10-10/debates/11FD46BC-F935-4D35-BAAF-9FCC8FAD7759/LeavingTheEUConsumerProtection)

The Information Commissioner has also stated that the *"best way forward"* after Brexit is for the UK *"to achieve an adequacy finding"* with the European Union.[67]

However, **adequacy is not guaranteed.** As Daniel Zeichner MP, the chair of the All-Party Parliamentary Group on Data Analytics, stated in the Commons EU data protection debate, "*just saying that we would like an adequacy agreement is not the same as actually getting one*".[68]

Article 45 of the General Data Protection Regulation (GDPR) considers what is required for adequacy:

> *"2. When assessing the adequacy of the level of protection [of personal data], the Commission shall, in particular, take account of the following elements:*
>
> *(a) Rule of law, **respect for human rights and fundamental freedoms**, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the **access of public authorities to personal data**."*

We have serious concerns that the current Data Protection Bill may significantly impact the UK's chances of achieving an adequacy finding with the EU. In particular, we are concerned about the lack of rights and exemptions exercised by the UK in relation to automated processing, the sweeping exemption from data protection rights in relation to the undefined concept of "effective immigration control", and the lack of oversight and limitations on the scope of national security certificates. **We urge the Committee to review these areas of the Bill and to put effective protections in place.**

[67] Elizabeth Denham, House of Lords EU Home Affairs Sub-Committee, Wednesday 8 March 2017 (http://www.parliamentlive.tv/Event/Index/125e1463-62ed-41bb-ab64-811d0f94bfee)

[68] Leaving the EU; Data Protection, House of Commons, 12 October 2017 (https://hansard.parliament.uk/Commons/2017-10-12/debates/20F0DCC3-149D-470D-8AF0-2DE02400D4D0/LeavingTheEUDataProtection)

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