PRIVACY INTERNATIONAL

Briefing

Briefing On The Data Protection Bill For The Report Stage In The House Of Lords

December 2017

About Privacy International

Privacy International (PI) was founded in 1990. It is a leading charity promoting the right to privacy across the world. It is based in London and, within its range of activities, investigates how our personal data is generated and exploited and how it can be protected through legal and technological frameworks. It has focused on the General Data Protection Regulation (GDPR) and its passage through the EU institutions since 2009. It is frequently called upon to give expert evidence to Parliamentary and Governmental committees around the world on privacy issues and has advised, and reported to, among others, the Council of Europe, the European Parliament, the Organisation for Economic Co-operation and Development, and the United Nations.

Contacts:

Camilla Graham Wood
Legal Officer
020 3422 4321
camilla@privacyinternational.org

Ailidh Callander
Legal Officer
020 3422 4321
ailidh@privacyinternational.org

Table of Contents

1. Summary

1.1. Privacy International welcomes the aim of the Data Protection Bill "to create a clear and coherent data protection regime", and to update the UK data protection law, including by bringing the EU General Data Protection Regulation (GDPR) and the Data Protection Law Enforcement Directive (DPLED) - into the UK domestic system.

1.2. A strong data protection framework is essential for the protection of human rights (including the right to privacy). It is also key to the granting of adequacy by the EU Commission following the UK's exit from the European Union.

1.3. Privacy International published three briefings during the consideration of the Bill at the 2nd Reading and Committee stages in the House of Lords.[1] This briefing consolidates our previous submissions and responds to some of the key arguments put forward by the Government at the Committee stage. References are to the Data Protection Bill [HL] [as amended in Committee][2]

2. Key concerns:

2.1. **Delegated powers:**
The Bill has many regulation making powers, and grants an unacceptable amount of power to the Secretary of State to introduce secondary legislation, bypassing effective parliamentary scrutiny. We recommend that the Bill is amended to limit such broad powers. We propose amendments to **Clauses 9, 15, 33, 84, 111 and 169** to address these concerns.

2.2. **Representation of living individuals:**
The Bill does not provide for qualified non-profit organisations to pursue data protection infringements of their own accord, as provided by EU General Data Protection Regulation (GDPR) in its

[1] See Privacy International's briefings for the Second Reading in the House of Lords (https://www.privacyinternational.org/node/1522); Committee Stage re General Processing (https://www.privacyinternational.org/node/1543); and Committee Stage re Law enforcement and Intelligence services processing (https://www.privacyinternational.org/node/1550).
[2] https://publications.parliament.uk/pa/bills/lbill/2017-2019/0074/18074.pdf)

article 80(2). We, along with UK digital rights and consumer organisations strongly recommend that the Bill is amended to include this provision to ensure data breaches, dangerous security flaws and unlawful conduct are remedied in an effective and efficient manner. We propose amendments to **Clause 173** to address these concerns.

2.3. **Exemptions for processing on grounds of public interest:**
We have specific concerns regarding some of the wide-ranging conditions for processing and exemptions to the obligations and rights in the Bill/ GDPR. We recommend that these be narrowed or removed. We propose amendments to **Clause 7, Paragraph 18 of Schedule 1, Paragraph 4 of Schedule 2, and relevant paragraphs in Schedules 9 and 11 as they refer to Part 4** to address these concerns.

2.4. **Automated decision-making**:
Profiling and other forms of decision-making without human intervention should be subject to very strict limitations to address issues including discrimination. The Bill provides insufficient safeguards for automated decision making. We recommend the Bill to be amended to include further concrete safeguards. We propose amendments to **Clauses 13 (Part 2, general processing); 47 (Part 3, law enforcement); and 94 (Part 4, intelligence services)** to address these concerns.

2.5. **National Security Certificates**:
Provisions in the Bill expands section 28 Data Protection Act 1998, with even wider exemptions. Privacy International's concerns include the timeless and retrospective nature of the certificates, lack of transparency, lack of oversight, no means to challenge, and wide powers exempt from data protection principles. We want concrete safeguards to be included in the Bill. We propose amendments to **Clauses 24, 25, 26 (Part 2, general processing), clause 77 (Part 3, law enforcement) and clauses 108, 109 (Part 4, intelligence services)** to address these concerns.

2.6. **Intelligence Agencies, cross-border data transfers**:
The Bill provides for almost unfettered powers for cross-border transfers of personal data by intelligence agencies without appropriate levels of protection; this is an infringement of the requirements of Council of Europe's modernised Convention 108.

We recommend that rules for such transfers are brought into line with those required in the Bill for law enforcement purposes. We propose amendments to Clause 107 to address these concerns.

2.7. Privacy International's proposed amendments for all the clauses summarised above are gathered together in Annex A to this briefing.

3. Delegated powers

3.1. The Bill has many regulation making powers, and grants an unacceptable amount of power to the Secretary of State to introduce secondary legislation.

3.2. As noted by Peers during the second reading of the Bill, convenience and future proofing do not justify these Henry VIII clauses which are inherently undemocratic, remove parliamentary oversight and empower the executive to take away the rights of individuals without the checks and balances afforded to primary legislation through the parliamentary process.

3.3. These concerns are compounded also in light of the proposal contained in the EU Withdrawal Bill to end the application of the European Charter on Fundamental Rights and Freedoms, which includes the right to data protection in Article 8.

3.4. Further, any future changes weakening the protections afforded by GDPR could impact on a future adequacy decision on the processing of personal data in the UK, therefore effective parliamentary scrutiny is essential.

3.5. We recommend that the Bill is amended to remove or limit such broad regulation-making powers. We propose amendments to clauses 9(6), 15, 33(6), 84(3), 111 and 169 to address these concerns. Full text of the amendments is contained in Annex A.

3.6. **Clause 9(6) (General Processing): Power to add, vary or omit conditions or safeguards for the processing of special categories of personal data**

3.7. Article 9.1 of GDPR prohibits the processing of special categories of personal data (previously known as 'sensitive personal data' such as racial or ethnic origin, political opinions, religious or philosophical beliefs etc.…). This prohibition is qualified by limited exemptions set out in Article 9.2 of GDPR. The draft Bill already provides extensive conditions (32) for processing special categories of personal data in Schedule 1.

3.8. Clause 9 allows the Secretary of State, by regulations, to amend Schedule 1 by adding, varying or omitting conditions or safeguards.

3.9. Concerns about the extent of these powers have been expressed by:

Constitutional Committee: "This is a very broad Henry VIII power, potentially affecting all of the conditions and safeguards in schedule 1..."[3]

Delegated Powers and Regulatory Reform Committee: "...clause 9(6) contains a Henry VIII power to allow the Secretary of State, by affirmative procedure regulations, to amend Schedule 1 by "adding, varying or omitting conditions or safeguards" and to make consequential amendments to clause 9 itself… We do not agree that the power conferred by clause 9(6) is only "slightly" wider than the existing ones in Schedule 3 to the 1998 Act. The new power would allow the Government by regulations completely to rewrite all the conditions and safeguards about the processing of special categories of data in Schedule 1 to the Bill. In contrast, the 1998 Act only permits new conditions to be added or three existing ones to be modified...In any event, we take the view that the memorandum does not adequately justify the breadth of the power in clause 9(6) of the Bill, and that it is inappropriate for Ministers to be given carte blanche to rewrite any or all of the conditions and safeguards in Schedule 1 by regulations in order "to deal with changing

[3] Select Committee on the Constitution Data Protection Bill [HL] 6th Report of Session 2017-19 - published 26 October 2017 - HL Paper 37, available at: https://publications.parliament.uk/pa/ld201719/ldselect/ldconst/31/31.pdf

circumstances" instead of bringing forward a Bill. While the affirmative procedure would apply to the regulations, this would allow no opportunity for either House to amend what might well be highly controversial provisions—allowing for the most sensitive types of personal data to be processed in entirely new circumstances...We consider that clause 9(6) is inappropriately wide and recommend its removal from the Bill."[4]

3.10. **Clause 15 (General Processing): Power to make wide ranging exemptions to GDPR application**

3.11. Article 23 of GDPR permits Member States to restrict the application of GDPR in very limited circumstances, provided that (i) any restriction respects the essence of the fundamental rights and freedoms and is a necessary in a proportionate measure in a democratic to safeguard certain aims; and (ii) the legislative measure contains specific minimum provisions. Schedules 2, 3 and 4 of the Bill already provide for a large number of exemptions to the rights and obligations under GDPR.

3.12. Clause 15 gives the Secretary of State wide powers to alter the applications of the GDPR, including notably new legal bases to share personal information in the public interest or in the exercise of public authority, restricting the rights of individuals as well as further restrictions on when the rights under GDPR apply.

3.13. Concerns about the extent of these powers have been expressed by:

Constitutional Committee: "This is a potentially extensive power, as it would allow the Secretary of State to alter the application of the GDPR, creating new legal bases for the performance of tasks in the public interest or in the exercise of official authority, and to alter significantly the range of data that are exempt from the protections in the Bill."[5]

---

[4] Delegated Powers and Regulatory Reform Committee 6th Report of Session 2017-19 - published 24 October 2017 - HL Paper 29, available at: https://publications.parliament.uk/pa/ld201719/ldselect/lddelreg/29/29.pdf

[5] Select Committee on the Constitution Data Protection Bill [HL] 6th Report of Session 2017-19 - published 26 October 2017 - HL Paper 37, available at: https://publications.parliament.uk/pa/ld201719/ldselect/ldconst/31/31.pdf

Delegated Powers and Regulatory Reform Committee: "This is a Henry VIII power because the regulations may amend or repeal any provision in clause 14 of and Schedules 2 to 4 to the Bill...We regard this is an insufficient and unconvincing explanation for such an important power. As we have observed in several reports, it is not good enough for Government to say that they need "flexibility" to pass laws by secondary instead of primary legislation without explaining in detail why this is necessary—particularly in the case of widely-drawn Henry VIII powers. While we recognise that the affirmative procedure would apply to regulations under clauses 15 and 111, this is not an adequate substitute for a Bill allowing Parliament fully to scrutinise proposed new exemptions to data obligations and rights...We consider that the delegations of power in clauses 15 and 111 are inappropriately wide, and recommend their removal from the Bill"[6]

3.14. These concerns were echoed by Peers at Committee Stage, for example, Lord Stevenson of Balmacara, highlighting the importance of restricting this power from the perspective of a future adequacy decision from the European Commission following the UK's withdrawal from the EU.[7]

3.15. **Clause 33(6) (Law Enforcement): Power to amend conditions for processing personal data**

3.16. Clause 33 in Part 3 of the Bill, sets out the first data protection principle, that processing must be lawful and fair. Sensitive processing is only permitted when certain conditions are met, including that the processing meets at least one condition in Schedule 8 to the Bill.

3.17. Paragraphs 2 and 3 of Schedule 8 transpose two conditions expressly provided for in Article 10 of the Law Enforcement Directive, namely to protect the data subject's vital interests or where the personal data is already in the public domain. Article 10 also allows further conditions to be specified in legislation passed by the Member States. Paragraphs 1 and 4 to 6 of Schedule 8 to the Bill therefore specify a number of further conditions (which replicate

[6] Delegated Powers and Regulatory Reform Committee 6th Report of Session 2017-19 - published 24 October 2017 - HL Paper 29, available at: https://publications.parliament.uk/pa/ld201719/ldselect/lddelreg/29/29.pdf

[7] House of Lords, Committee day 4, https://goo.gl/oSRx1z

conditions in Article 9(2) of the GDPR), that is judicial and statutory purposes, legal claims and judicial acts, preventing fraud and archiving, research and statistical purposes.

3.18. Clause 33(6) provides the Secretary of State with the broad power to add, vary or omit these conditions.

3.19. Concerns on these broad powers have been expressed by:

> ***Delegated Powers and Regulatory Reform Committee***: "Clause 33(6) confers a Henry VIII power to allow the Secretary of State, by affirmative procedure regulations, to amend Schedule 8 by adding, varying or omitting conditions… For essentially the same reasons that we give above in relation to clause 9(6), we consider it inappropriate for the Bill to confer such widely drawn and far-reaching powers; and we therefore recommend the removal of clauses 33(6) and 84(3)."[8]

3.20. Concerns were raised at Committee stage by Peers, including Lady Hamwee and Lord Stevenson.[9]

3.21. **Clause 84(3) (Intelligence agencies): Power to amend conditions for processing personal data**

3.22. The Bill limits the basis on which the Intelligence Services can process special categories of personal data. These are set out in Schedule 10.

3.23. Concerns on these broad powers have been expressed by:

3.24. ***Delegated Powers and Regulatory Reform Committee***: "Clause 84(3) contains a Henry VIII power analogous to that in clause 33(6) to allow the Secretary of State to add, vary or omit conditions in Schedule 10...For essentially the same reasons that we give above in relation to clause 9(6), we consider it inappropriate for the Bill to

[8] Delegated Powers and Regulatory Reform Committee 6th Report of Session 2017-19 - published 24 October 2017 - HL Paper 29, available at: https://publications.parliament.uk/pa/ld201719/ldselect/lddelreg/29/29.pdf

[9] House of Lords, Committee day 4, https://goo.gl/oSRx1z

confer such widely drawn and far-reaching powers; and we therefore recommend the removal of clauses 33(6) and 84(3)."[10]

3.25. **Clause 111 (Intelligence Agencies): Power to make further exemptions**

3.26. Certain exemptions to the obligations of the Intelligence Services are set out in Part 4 of the Bill, including in Schedule 11 to the Bill. Clause 111 permits a very wide regulation-making power for the Secretary of State, to provide for further exemptions from any provision of Part 4 or to amend or repeal the provisions of Schedule 11.

3.27. Concerns on these broad powers have been expressed by:

Constitutional Committee: "Clause 111 creates a Henry VIII power enabling the Secretary of State by regulations to add to, amend or repeal the exemptions prescribed by schedule 11.[11]

Delegated Powers and Regulatory Reform Committee: "This is also a Henry VIII power, because clause 111(2) allows the regulations to amend or repeal any provision of Schedule 11. According to the memorandum, the power would be used "if the Secretary of State considers that the exemption is necessary for safeguarding the interests of data subjects or the rights and freedoms of others"; but clause 111 itself contains no such limitation on the circumstances in which the power could be used."

3.28. **Clause 169 (Enforcement): Require public consultation on regulations**

3.29. The wide regulation making powers under the Bill grant an unacceptable amount of power to the Secretary of State to introduce secondary legislation. The concerns regarding secondary legislation, have been voiced by the Delegated Powers and Regulatory Reform Committee and the Select Committee on the

[10] Delegated Powers and Regulatory Reform Committee 6th Report of Session 2017-19 - published 24 October 2017 - HL Paper 29, available at: https://publications.parliament.uk/pa/ld201719/ldselect/lddelreg/29/29.pdf

[11] Select Committee on the Constitution Data Protection Bill [HL] 6th Report of Session 2017-19 - published 26 October 2017 - HL Paper 37, available at: https://publications.parliament.uk/pa/ld201719/ldselect/ldconst/31/31.pdf

Constitution, as set out above, and by Peers during the Second Reading and Committee Stage.

3.30. Consultation is one way to seek to ensure oversight and scrutiny of regulations. As well as an obligation to consult the Information Commissioner, the Secretary of State should be under a statutory duty to consult data subjects and those who represent the interests of data subjects. Furthermore, the rationale for excluding section 21 (Power to make provision in consequence of regulations related to the GDPR) from the duty to consult is not established and this exception should be removed from clause 169.

4. Representation of data subjects (Article 80(2) of GDPR)

4.1. Clause 173 – representation of data subjects

4.2. In order to protect and uphold the right to privacy and data protection, individuals need effective remedies when their rights are infringed.

4.3. However, despite a commitment that the Government would use the Bill to ensure effective redress for those impacted by data breaches and for unlawful actions undermining data protection safeguards, Clause 173 does not provide for qualified non-profit organisations to pursue data protection infringements of their own accord, as provided by in Article 80(2) of the GDPR.

4.4. Personal data is incredibly valuable and with the increased generation of personal data in every aspect of our lives there is also an increased risk of infringement or breaches of individual's data protection rights. In addition to mass data breaches, security flaws result in connected devices such as children's toys being vulnerable to third party intrusion.[12] There is also a risk where individuals are subject to automated decision-making using their data, that organisations do not provide clear information to consumers about how their data is processed and used, that privacy protection by design and default is not built into products and services and that excessive amounts of data are collected and shared about individuals.

[12] https://www.forbrukerradet.no/side/significant-security-flaws-in-smartwatches-for-children/

4.5. The failure to address vulnerabilities in devices threatens not only the safety of customers and children, but breaches of data protection have the ability to impact upon society as a whole, as we have seen from the recent WannaCry ransomware attack and the Uber mass data leak. These impact the UK economically, socially and politically, and are of particular concern with respect to issues such as cyber security.

4.6. Through increased obligations and rights, GDPR seeks to address these issues. However, in order to address the power imbalance between individuals and those processing their data, empower individuals and improve controller and processor practices, these obligations and rights need to be enforced and upheld.

4.7. Implementing Article 80(2) of the GDPR would create a collective redress regime for breaches of data protection law. This would complement the existing collective redress regime introduced under the Consumer Rights Act 2015 which applies to infringements of competition law. The Courts have procedures and practices in place for the Consumer Rights Act, including ensuring only cases that have merit proceed, which could be adapted to apply to an Article 80(2) regime.

4.8. Introducing collective redress as provided in Article 80(2) of GDPR would allow qualified organisations to seek effective judicial remedies against those handling personal data where the organisation considers that the data protection rights of individuals have been breached.

4.9. Many breaches of data protection law, including notably data breaches, processing without a legal basis, failure to provide fair notice, unlawful data sharing and data retention practices affect hundreds of thousands rather than single individuals, so a mechanism of collective redress would save significant administrative and court time, avoiding a myriad of individual claims. Furthermore, not all breaches of data protection impact a clearly defined group of individuals. During Committee, the Government referred to an existing claim, with over 5,000 data subjects, as an example that effective remedy is already guaranteed. This may refer to the case of Morrisons' workers following a data breach, where the impacted individuals are a

clearly defined group and in a position to co-ordinate. This would not be the case in dozens of other situations where the controllers practice unlawful activities, such as third-country and third-party data transfers or using personal data for purposes unrelated to those for the original processing, without the individuals' knowledge or consent. Individuals lack the technical skills and research capacity that allows organisations such as Privacy International to identify and seek to remedy unlawful practices.

4.10. Individuals are highly unlikely to have the resources to take legal action when their data protection rights are infringed, due in part to a lack of understanding of the data protection practices of organisations, the complexity of the data protection legal framework, the time and money required to seek an effective judicial remedy.

4.11. During Committee stage, the introduction of an amendment including Article 80(2) in the Bill was supported by Lord Stevenson, Lord Clement-Jones, Baroness Jones of Mouslecoomb, Baroness Kidron and Lord Lucas. As put by Baroness Jones of Mouslecoomb, this provision "gives teeth to data protection" and Lord Lucas "without these amendments, I do not see how the Bill can provide an adequate remedy when a large number of people suffer a small degree of damage".[13] In its response Lord Ashton, in behalf of the government, questioned the motives of non-governmental organisations and charities to demand the provision for collective redress, implying that some would do such actions for personal promotion. Privacy International, a respected professional registered charity, respectfully reminds the government and its Ministers that the legislation provides for very strict rules of engagement for such organisations even for Article 80 (1), and that embarking on collective actions involves serious research, evidence building, legal expertise and a lot of resource. No organisation would undertake such an action lightly.

4.12. The existing mechanisms for collective address in the UK are insufficient to guarantee that controllers and processors uphold and respect the rights of data subjects.

[13] House of Lords, Committee, Day 6, https://goo.gl/d7eUks

4.13. GDPR affords increased enforcement power to regulators, in the UK the ICO, however, there will be resource limitations on the action they can take. Furthermore, GDPR guarantees both the right to take action via the regulator and that of effective judicial remedy. Therefore, it is essential that qualified civil society and consumer organisations who already have the investigative, technical and legal understanding of this area have the necessary legal tools to hold data controllers and processors to account by pursuing effective judicial remedies.

4.14. Privacy International, along with UK digital rights and consumer organisations strongly recommend that **Clause 173** of the Bill is amended to include this provision.

5. Public interest as ground for processing personal data

5.1. The Bill contains conditions for processing in the public interest and exemptions from data protection obligations that are wide-ranging, poorly defined and where no justification is provided as to the legitimate aim pursued.

5.2. We recommend that the Data Protection Bill is amended to better define "public interest", "substantial public interest", and such exemptions are removed or limited.

5.3. In particular, we propose amendments on the following clauses:

- Restrict the grounds for processing in the public interest (**Clause 7**);
- Add a requirement to publish a code of practice/guidance on "public interest" (**new Clause, Part 5**);
- Remove or improve provision for processing by political parties of special category personal data, revealing political opinions (**paragraph 18 of Schedule 1** of the Bill);
- Remove the exemption for processing personal data for effective immigration purposes (**paragraph 4 of Schedule 2** of the Bill);
- Restrict conditions and exemptions provided to the Intelligence Services (**paragraphs 5(e) and 6 of Schedule 9**

and paragraphs 1, 10,12, 13 and 14 of Schedule 11 related to Part 4 of the Bill).

5.4. Clause 7 – Lawfulness of processing: public interest

5.5. The lack of clarity is exacerbated by Clause 7 of the Bill, which includes a non-exhaustive definition of processing that is necessary for the performance of a task carried out in the public interest or in the exercise of the controller's official authority.

5.6. Article 6(2) of GDPR provides that whilst a Member State may maintain or introduce more specific provisions with regard to processing for compliance with part (e) (processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority) this should be done to determine more precisely specific requirements for the processing and other measures to ensure lawful and fair processing. Article 6(3) provides that the basis for processing in point (e) must be laid down by law, and that the specific provisions should include measures to ensure fair and lawful processing. Furthermore, the law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

5.7. Clause 7 should therefore be amended to make the list of activities which fall within the "public interest" specific and exhaustive. If there is a concern that clause 7 does not cover scientific or historic research by public authorities, then this should be specifically provided for in an exhaustive list as an additional sub clause in clause 7.

5.8. New Clause (after 119) - Add a requirement to prepare a code of practice on "public interest"

5.9. The term 'public interest' is used throughout the Bill and is key to applying many of its provisions.[14] These include consideration of the legal basis/ condition for processing, whether an exemption applies, whether the data can be transferred and as a defence to certain offences. In relation to special categories of personal data, the term 'substantial public interest' is used in the Bill (as in GDPR).

[14] Clauses 7, 15, 17, 39, 74, 74, 85, 127, 162, 171, 173, Sch 1 paras 3, 4, 6, 8, 9, 10, 13, Sch 2 para 7, 24, 26.

5.10. However, neither 'public interest' or 'substantial public interest' are defined terms in the Bill nor is there any requirement on the Information Commissioner (ICO) to publish statutory guidance in this regard. This may result in misapplication or interpretation of these terms which could lead to personal data, including sensitive personal data being processed without a valid legal basis or being incorrectly subject to an exemption.

5.11. Further clarification on the scope of "public interest" and "substantial public interest" in the Bill is required. Guidance on the application of these terms from the ICO would provide clarity and greatly assist controllers and processors in carrying out their obligations and data subjects in understanding whether their data is being processed in accordance with the terms of the legislation. Guidance would be an important tool to prevent misapplication/ interpretation of these terms which could lead to individuals' personal data being processed without a valid legal basis or being incorrectly/arbitrarily subject to an exemption.

5.12. Under the current Bill it is at the discretion of the ICO as to whether to publish guidance or a code of practice on the public interest (see Clause 124 – Other codes of practice.) No such guidance has been published to date, despite the use of both public interest and substantial public interest in the Data Protection Act 1998 and associated statutory instruments. Given the increased importance of these terms under the GDPR and the Bill (which aims to strengthen the rights of data subjects and imposes higher penalties on controllers and processors for breaches as well as further individual offences), it is critical to the consistent application of the terms of the Bill (and GDPR) that guidance on the public interest is available and that controllers and processors take this guidance into account when interpreting and applying the relevant provisions of the Bill/ GDPR. In the context of freedom of information, both the ICO and the Scottish Information Commissioner have produced guidance on the application of the public interest test.

5.13. During the Committee stage comprehensive discussions on this issue in the Bill, Lord Clement-Jones has stated that "The idea of a specific code seems the way forward; the way forward is not by granting over mighty powers to the Government to change the definitions according to the circumstances. I think that that was the phrase that the Minister used—they wish to have that flexibility so

that the public interest test could be varied according to circumstances. If there is a power to change, it has to be pretty circumscribed. Obviously, we will come back to that in a later group."[15]

5.14. The desired form of guidance would be a statutory Code of Practice which would require the ICO to produce such guidance and allow for it to be consulted upon and scrutinised by Parliament. Whilst failure to act in accordance with the Code would not in itself make a person liable to legal proceedings it could be taken into account by a Court or the ICO when considering proceeding or regulatory action and there would therefore be a strong incentive for controller's and/or processors to take into account and comply with the Code.

5.15. **Paragraph 18 of Schedule 1 - Conditions for processing special categories of personal data - political parties**

5.16. Part 2 of Schedule 1 to the Bill, sets out the conditions for processing special categories of personal data based on Article 9(2)(g) of GDPR which provides that: "processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".

5.17. Of particular concern is paragraph 18 of Schedule 1 to the Bill which permits registered political parties to process personal data 'revealing political opinions' for the purposes of their political activities. Political activities can include, but are not restricted to, campaigning, fundraising, political surveys and case-work. Whilst a variation of this condition was included in a statutory instrument to the DPA 1998, technology and data processing in the political arena have moved on. The processing of personal data plays a key part in political activities (including political parties contracting the services of specialist data mining companies), and this is only likely to increase going forward. Personal data that might not have previously revealed political opinions can now be used to infer

[15] House of Lords, Committee stage, day 2, https://goo.gl/Hap9BN

information about the political opinions of an individual (primarily through profiling).

5.18. Using voter personal information for campaigning is nothing new. For decades, political parties have been using and refining targeting, looking at past voting histories, religious affiliation, demographics, magazine subscriptions, and buying habits to understand which issues and values are driving which voters. However, what is new and has been enabled by technologies is the granularity of data available for such campaigning, to the extent that political campaigners have come to know individuals' deepest secrets.

5.19. The practice of targeting voters with personalised messaging has raised debates about political manipulation and concerns regarding the impact of such profiling on the democratic process in the UK and elsewhere.[16] However, unlike party-political broadcasts on television, which are monitored and regulated, personalised, targeted political advertising means that parties operate outside of public scrutiny. They can make one promise to one group of voters, and the opposite to another, without this contradiction being ever revealed to either the voters themselves or the media. This happened in Germany for example, where the Afd radical party publicly promised to stop sharing offensive posters, yet continued to target specific audiences with the same images online.[17] In the UK, the Information Commissioner has commenced a formal investigation into the use of analytics by political parties following the EU Referendum and the 2017 General Election campaigns.[18]

5.20. It is essential that consideration is given to the way in which this condition for processing can interfere with the right to privacy and

[16] See Privacy International, Cambridge Analytica Explained: Data and Elections, available at https://www.privacyinternational.org/node/1440 and also see page 38, How Companies Use Personal Data Against People. Automated Disadvantage, Personalised Persuasion, and the Societal Ramifications of the Commercial Use of Personal Information, Working paper by Cracked Labs, October 2017. Author: Wolfie Christl. Contributors: Katharina Kopp, Patrick Urs Riechert, available at: http://crackedlabs.org/dl/CrackedLabs_Christl_DataAgainstPeople.pdf

[17] This became known only because NGOs asked voters to screenshot the ads

[18] See ICO blog of 17 May 2017 , available at: https://iconewsblog.org.uk/2017/05/17/information-commissioner-elizabeth-denham-opens-a-formal-investigation-into-the-use-of-data-analytics-for-political-purposes/

freedom of expression, particularly in light of technological developments and the granularity of processing of personal data. If your online activities and behaviour are used to profile you and reveal information as to your political opinions and this can then be used by political parties to target you for unlimited political activities, including fundraising, then this may result in a chilling effect on those seeking and imparting information in an online environment.

5.21. A fundamental reason why in a democracy ballots are secret, is to forestall attempts to influence voters by any form of intimidation, blackmailing, or lies. This is also protected by the right to free elections by secret ballot in, the right to free elections, as protected by Article 3 of the First Protocol to the European Convention of Human Rights. Through granular profiling, political parties can obtain the political preferences and likely past voting decisions of millions of voters. This is a dangerous development for democracy going forward which impacts on the right to privacy, freedom of expression and free elections.

5.22. Whilst political parties' engagement with voters is a key part of a healthy democracy there are other conditions that political parties can rely on for processing and as a very minimum this condition must be accessible and foreseeable in its terms to prevent abuse and interference with human rights. Freedom of expression and impact on the right to free elections that could entail.

5.23. Concerns with this condition for processing were raised at Committee Stage by Peers.

5.24. Lord Kennedy stated that:

> "Health-functioning political parties are a vital part of our democracy. Campaigners and campaigning have moved on a long way from the days of handwriting envelopes to encompass much more sophisticated methods of contacting voters using all available mechanisms.
>
> Political parties and their members need clarity and certainty as to what they are required to do, what they are able to do and what they are not able to do, so that they act lawfully at all times and in all respects. We cannot leave parties, campaigners and party

members with law that is grey and unclear, and with rules that mean that campaigners, in good faith, make wide interpretations that are then found to be incorrect, due largely to the required clarity not having been given to them in the first place by government and Parliament."[19]

5.25. Lord Kennedy, called on the Government to meet with Peers to discuss these issues and clarify a number of points, including; to provide a list of the characteristics or activities required for a political party to conduct operations; to clarify what constitutes profiling with regard to the activities of political parties; and to confirm what activities of operations with reference to political activities in this exemption would be considered necessary for a political party.

5.26. Lord Ashton of Hyde for the Government, responded by referring the Information Commissioner's investigation into the data protection risks arising from the use of data analytics, including for political purposes. Noting that the Commissioner recognises that this is a complex and rapidly evolving area where organisations use a person's internet or public profile to target communications of messaging. Going on to note that the level of awareness among the public about how data is collected, shared and used through such tools is low but that what is clear is that these tools have a significant potential impact on an individual's privacy. Lord Ashton, agreed to meet with Peers and also stated that the current clause in the Bill replicates the existing wording the Data Protection Act 1998.

5.27. In the following discussion, Lord Whitty called for the issue of other organisations and political parties attempting to influence the political process to be addressed. This was supported by Baroness Jay of Paddington who together with Lady Hamwee called for involvement of the Electoral Commission. Lord McNally flagged that it would be useful to have the ICO's study before the Bill becomes law and that "There is a massive problem coming down the road concerning how data are used in the political process." Noting that, the two small amendments "are an iceberg in terms of the problems that lie beneath them". Lord Lucas, went on to point out that:

[19] House of Lords, Committee day 3, column 1816, https://goo.gl/wygmFa

"We are getting into a situation where political parties are addressing personal messages to individual voters and saying different things to voters. This is not apparent; there must be ways to control it. We will have to give some considerable thought to it, so I see the virtue of the amendments"[20]

5.28. Lord Ashton of Hyde accepted that this is the tip of an iceberg, but indicated that this is about data protection and there are other avenues to raise a lot of the points made and indicated that the ICO's report is expected before Christmas.

5.29. In a letter to the Lords following day 3 of Committee, the Government confirmed that in relation to the definition of political activities, it is for each Controller to determine what processing activities are necessary in the circumstances of the case.[21]

There are a number of reasons as to why this condition should be removed from the Data Protection Bill:

5.30. Contrary to the Government statement at Committee Stage, paragraph 18 does not replicate the DPA exemption: there is a subtle but important change in wording from "information consisting of political opinions" to "information revealing political opinions", which widens the scope to personal data revealing political opinions.

5.31. Developments in technology enable political parties to process personal data in a manner and on a scale, that was not possible when the DPA was enacted. This has been acknowledged by the Government and Peers during Committee stage and is recognised by the ICO's investigation.

5.32. The broad condition in paragraph 18, goes beyond what is set out in recital 56 of GDPR which provides that "Where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be

[20] Committee Day 3, para 1820, available at: https://goo.gl/LStr3v
[21] Letter of 16 November 2017 from Lord Ashton of Hyde, available at http://data.parliament.uk/DepositedPapers/Files/DEP2017-0707/Data_protection_bill_committee_Day_3.pdf

permitted for reasons of public interest, provided that appropriate safeguards are in place." Neither the wording of the condition in paragraph 18 nor the explanatory notes explain why the operation of a democratic system in the UK requires that political parties compile personal data on people's political opinions. The word 'revealing' and the non-defined broad scope of 'political activities', in paragraph 18, together with the threshold of 'substantial damage or substantial distress', go beyond processing required for electoral activities in a democratic system.

5.33. There are already sufficient conditions for processing in the GDPR and the Bill, that political parties can rely on for processing personal data of individuals. If the processing involves non- sensitive (or non-special category) personal data, such as names and contact details then parties can seek to rely on consent (Art 6.1(a) of GDPR) or legitimate interests (Art 6.1(f)) of GDPR). If it is political opinions of individuals, then the GDPR provides alternate conditions, including explicit consent (Art 9.2 (a) of GDPR) or processing is of the political opinions of members/ former members or those in regular contact with the party, and carried out in the course of the party's legitimate activities, with appropriate safeguards (Art 9.2(d) of GDPR). As far as we are aware, neither the Government nor political parties have provided an explanation of the necessary activities of political parties that cannot be justified through another exemption.

5.34. Political parties should rely on other conditions, such as explicit consent, before processing personal data revealing political opinions. The onus should be on political parties to explain in clear terms, to the public, how they process personal data revealing political opinions and why this condition is necessary. Only with transparency around the current and envisaged processing of political opinions by political parties, can a thorough proportionality and impact assessment be carried out around this condition.

5.35. In light of the above reasons, Privacy International's preferred outcome is that paragraph 18 should be removed from the Bill for the reasons set out above. Alternatively, amendments must be made to ensure that the scope of the condition is proportionate and adequate safeguards are established.

5.36. Paragraph 4 of Schedule 2 - Immigration exemption

5.37. The immigration exemption is new in the Bill and there was no direct equivalent under the DPA 1998. This is a broad and wide-ranging exemption which is open to abuse and interference with human rights. This exemption should be removed altogether as there are other exemptions within the Bill that the immigration authorities can seek to rely on for the processing of personal data in accordance with their statutory duties/ functions. Such a broad ranging exemption may also impact on an adequacy decision from the European Commission going forward.

5.38. At Committee stage, Lord Clement Jones and Baroness Hamwee sought to remove this clause and many peers, Baroness Jones of Mouslecoomb, Lord Lucas and Lord Kennedy, raised their grave concerns with this exemption.[22] The Government's response failed to address these concerns and offer any reasonable justification for the inclusion in the Bill of this new and wide-ranging exemption to the rights of data subjects.

5.39. Concerns about this exemption have been raised by other commentators and we support other civil society organisations who are also pushing for the removal of this exemption. In particular, we would refer to Liberty's detailed briefing[23].

5.40. Exemption for Processing by intelligence services (Part 4)

5.41. The UK Intelligence Services must comply with the UK's human rights obligations and any interference with human rights such as the right to privacy and the right to freedom of expression must meet the requirements of being in accordance with the law, necessary and proportionate for the pursuant of a legitimate aim. The wide conditions for processing and broad exemptions in the Bill set out below, do not meet these standards. Furthermore, there is a risk that these provisions could impact on an adequacy decision from the European Commission post Brexit given that factors looked in determining adequacy, as set out in Article 45 of GDPR, include respect for human rights, legislation concerning public

[22] House of Lords, Committee day 3, column 1980, available at https://goo.gl/9KSpCk

[23] https://www.liberty-human-rights.org.uk/sites/default/files/Libertys%20Abridged%20Briefing%20on%20the%20Immigration%20Control%20Exemption%20in%20the%20Data%20Protection%20Bill%202017.pdf

security, defence and national security and the access of public authorities to personal data.

5.42. Schedule 9: Conditions for processing under Part 4
Schedule 9 to the Bill sets out the conditions for processing personal data that apply to the Intelligence Services. Of particular concerns are:

5.43. Paragraph 5(e) of Schedule 9 permits processing for the exercise of any other functions of a public nature exercise in the public interest by a person. The scope of Part 4 of the Bill is limited to the processing of personal data by the intelligence services as defined in clause 80(2) of the Bill, therefore there is no demonstrable justification for including this broad provision as a condition for processing, where provision is already made for processing in the exercise of statutory functions.

5.44. Paragraph 6 of Schedule 9 permits the processing of personal data when it is in the interests of the controller or the third party or parties to whom the data is disclosed. Under Parts 2 and 3 of the Bill, public authorities and competent authorities are unable to rely on a legitimate interest condition for processing personal data. Therefore, this provision should also be removed to require intelligence services to comply with the same standards. There exist provisions for processing which the intelligence agencies can rely upon and we see no reason why the intelligence services should be permitted to process personal data out of their statutory remit. During Committee Stage, Baroness Hamwee laid an amendment to remove this condition. In response, Lord Young of Cockburn, stated that "In the case of the intelligence services, their legitimate interests are dictated by their statutory functions, including safeguarding national security and preventing and detecting serious crime… this is a condition currently provided for in Schedule 2 to the Data Protection Act 1998, so it may not surprise noble Lords that we could not support an amendment that would preclude the intelligence services from processing personal data in pursuance of their vital functions" This response fails to acknowledge that (i) that paragraph 5 of Schedule 9 already provides a condition for the intelligence services to process personal data necessary for the exercise of their statutory functions; and (ii) that whilst the legitimate interest condition was in the DPA 1998, it is no longer available to public authorities under the GDPR or to competent authorities in Part 3 of the Bill, under the Law Enforcement Directive.

5.45. Schedule 11: Exemptions under Part 4

Schedule 11 to the Bill sets out exemptions to the obligations of the Intelligence Services under Part 4 of the Bill. Of particular concerns are:

5.46. Paragraph 1 of Schedule 11 sets out the provisions "the listed provisions" from which the intelligence services are exempt on the basis of the exemptions in Schedule 11. The provisions of paragraph 1(a) are overly broad. There is no justification for almost completely exempting bodies from the data protection principles in Chapter 2 of Part 4. The processing of personal data by the intelligence services in the exemptions in Schedule 11 should still be required to be purpose limited, adequate, relevant, not excessive, accurate, up to date, kept for no longer that necessary and processed in a manner that includes taking appropriate security measures as regards risk that arise from processing personal data.

5.47. Paragraphs 10, 12, 13 and 14 of Schedule 11 are just some of the exemptions to Part 4. The exemption provided by the listed provisions in paragraph 1 of Schedule 11 are broad and wide ranging and provide a full exemption to the rights of data subjects and almost entirely to the data protection principles. The exemptions for negotiations, exam marks, research and statistics and archiving in the public interest should be removed and at the very least qualified further. It is not explained why the intelligence services needs such exemptions and it appears that they have just be carried over from the provisions of the DPA 1998.

6. Automated decision-making

6.1. Profiling and other forms of decision-making without meaningful human intervention should be subject to very strict limitations. The Bill provides insufficient safeguards in this respect.

6.2. Our world is one in which more and more of what we do is traceable, where aggregated data can reveal a lot about a person and where we see ever increasingly sophisticated means of processing data.

6.3. Profiling, which may be relied upon to make automated decisions, refers to a form of programmed processing of data, using algorithms, to derive, infer, predict or evaluate certain attributes, demographic information, behaviour or even the identity of a person. Profiling can involve the creation, discovering or construction of knowledge from large sets of data. In turn created profiles can be used to make decisions.

6.4. With technological advancements automated processes look set to play an increasing role in decision-making. Decision-making can have significant and lasting implications for an individual and their human rights.

6.5. The profiling of individuals can inform automated decision-making and therefore concerns around profiling must be taken into account when considering the need for safeguards in relation to automated decision-making: profiling itself can automate inferences and predictions by relying on an expanding pool of data sources, such as data about behaviour, location and contacts, as well as increasingly advanced data processing, such as machine learning.

6.6. To ensure data protection legislation can address the technological challenges that exist now and that lie ahead, we must ensure that profiling and automated decisions it informs are legal, fair and not discriminatory, and that data subjects can exercise their rights effectively.

6.7. When considering the input that may be used in decision-making, profiling can infer or predict highly sensitive details from seemingly uninteresting data, leading to detailed and comprehensive profiles that may or may not be accurate or fair.

6.8. The reliance on computational algorithms and machine learning may pose a number of challenges, including with regards to opacity and auditability of the processing of data as well as accountability for decisions which impact individuals' human rights. One way to tackle this is to strengthen safeguards regarding automated decision-making authorised by law.

6.9. Automated decision-making, informed by profiling practices, is widespread and central to the way we experience products and services: recommender systems rely on fine-grained profiles of what

we might next want to read, watch, or listen to; dating apps rank possible partners according to our predicted mutual interest in each other; social media feeds are automatically personalised to match our presumed interest; and online ads are targeted to show what we might want to buy at a time when we are most likely to be perceptive.

6.10. At the same time, however, it poses three closely related risks:

6.11. **Privacy invasive:** By virtue of generating new or unknown information, it is often highly privacy invasive. It challenges common views about consent and purpose limitation, and also raises issues around control, not just over personal data, but also identity. Data subjects may be unaware of the kinds of inferences and predictions that can be revealed[24] and used in automated decision-making.

6.12. **Biased:** Since derived, inferred or predicted profiles may be inaccurate, or otherwise systematically biased, profiling may also lead to individuals being misclassified or misjudged. When profiling is used to inform or feed into automated decisions that affect individuals, the outcome of such decisions may result in harm with the potential to affect the enjoyment of human rights.

6.13. **Discriminatory:** There is a risk that this can be used to the detriment of those who are already discriminated and marginalised. Even if data controllers can take measures to avoid processing sensitive data in automated processing, trivial information can have similar results to sensitive data being processed. In racially segregated cities, for instance, postcodes may be a proxy for race. Without explicitly identifying a data subject's race, profiling may therefore nonetheless identify attributes, or other information that would nonetheless lead to discriminatory outcomes, if they were to be used to inform or make a decision.

6.14. In March 2017, the United Nations Human Rights Council, noted with concern "that automatic processing of personal data for individual profiling may lead to discrimination or decisions that

[24] The Royal Society, 2017, Machine learning: the power and promise of computers that learn by example. Royal Society. Available from https://royalsociety.org/~/media/policy/projects/machine-learning/publications/machine-learning-report.pdf [Accessed 1st August 2017]

otherwise have the potential to affect the enjoyment of human rights, including economic, social and cultural rights."[25]

6.15. We recommend the Bill to be amended to include further concrete safeguards and protect human rights. It will mean amending the following clauses: 13 (Part 2, general processing); 47 (Part 3, law enforcement); and 94 (Part 4, intelligence services.)

6.16. Clause 13 (General Processing): Automated decision-making authorised by law

6.17. Amendments are suggested to Clause 13 in order to:

- Clarify the meaning of decision "based solely on automated processing";
- Strengthen safeguards regarding automated decision-making authorised by law;
- Ensure full right to challenge and redress regarding automated decision-making authorised by law.

6.18. Clarify the meaning of decision "based solely on automated processing"

6.19. Automated decision rights in the Bill are able to be triggered for decisions with legal effects or similarly significant effect, but only if these decisions are based solely on automated processing. If decisions involve a "human-in-the-loop" they can avoid decisions being subject to the safeguards, even if the human is just agreeing with the system.

6.20. As a matter of fact, all systems that exercise automated processing or decision-making are designed, operated and maintained by humans, whose involvement inevitably influences the outcomes and decisions made. Furthermore, human influence is embedded into software: the outcomes and decisions made by algorithms, for instance, are shaped by human decisions about training data (i.e. what data to feed the computer to 'train' it), semantics, criteria choices etc.

[25] U.N. Human Rights Council Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/HRC/34/7, 23 Mar. 2017.

6.21. As noted in the recently published draft guidelines on profiling by the Working Party 29 (i.e. the body representing all national data protection authorities in the EU, including the ICO which led on the consultation of this document), the: "controller cannot avoid the Article 22 provisions by fabricating human involvement. For example, if someone routinely applies automatically generated profiles to individuals without any actual influence on the result, this would still be a decision based solely on automated processing. To qualify as human intervention, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision. As part of the analysis, they should consider all the available input and output data."[26]

6.22. At Committee stage, Lord Ashton acknowledged that human intervention must be meaningful. Indicating that in the Government's view that is the meaning that the phrase "based solely on automated processing" implies, stating that the test is what type of processing the decision having legal or significant effects is based on and that:

6.23. "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."

6.24. However, as the Bill stands this is not clear. The term "solely" when given its plain and ordinary meaning, means "Not involving anyone or anything else"[27], this does not presume even token human involvement and therefore to ensure clarity and these provisions are implied as intended, the definition must be amended. To echo Lord Clement-Jones at Committee stage, the interpretation of "solely" needs to be on the face of the Bill.

6.25. We recommend defining decisions as "solely" based on automated processing where there is no "meaningful human input".

[26] http://ec.europa.eu/newsroom/document.cfm?doc_id=47742

[27] Definition of solely in Oxford English Dictionary, available at: https://en.oxforddictionaries.com/definition/solely

6.26. Strengthen safeguards regarding automated decision-making authorised by law

6.27. The provision of meaningful information about the logic involved as well as the significance and legal consequences of such processing is fundamental to allow transparency of automated decision making and ensure accountability and the rights of data subjects, including having sufficient information in order to challenge such decisions. There is no rationale for omitting it in this section.

6.28. This amendment aims to ensure a right to explanation in an automated-decision, in line with the Government's own Explanatory Notes (para 115)[28] and Recital 71 of the EU GDPR, which states: "In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision".

6.29. The obligation to provide information about the logic involved in the automated decision is already contained in the GDPR (Article 13(2)(f), Article 14(2)(g) (Information to be provided to the data subject) and Article 15(1)(h) (Right of access by the data subject).) These rights, to information about the existence of automated decision-making and to be provided with meaningful information about the logic involved as well as the significance and the envisaged consequences of such processing, are extremely important. However, there is a risk that this right which applies to Article 22(1) and (4) of GDPR, does not extend to decisions under Article 22(2)(b) automated decision-making authorised by law (provided for in clause 13 of the Bill). This is not just a regulatory burden as suggested by Lord Ashton at Committee Stage, it is essential to ensure that when a 'significant' decision is to be made individuals are provided with meaningful information.

6.30. Ensure full right to redress

[28] "115. The GDPR does not set out what suitable safeguards are, though recital 71 suggests they should include: - provision of specific information to the data subject; and - right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after an assessment, and an opportunity to challenge the decision."

6.31. Automated decision making, including profiling, affects data subjects in a variety of ways. Given this potential negative impact, data subjects must be expressly given the right to challenge automated decisions, when done in accordance with this clause of the Bill.

6.32. Article 22(2)(b) of the GDPR requires member states to establish "suitable measures to safeguard the data subject's rights and freedom and legitimate interest". Article 23 (3), and related recital 71 (see above), further requires the data controller to "...implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision"

6.33. A right to effective remedy is definitely among the fundamental safeguards required: this is a separate right to redress than the remedies in the GDPR and the Enforcement section of the Bill, which only cover an infringement of the data subject rights as set out in the legislation. So, the Bill needs to specifically refer to a right to challenge and redress in cases, for example, where a decision is discriminatory with consequences that prejudice the rights and freedoms of the data subject.

6.34. Clause 47 (Law Enforcement): Automated decision-making authorized by law: safeguards

6.35. Profiling and other forms of decision-making without human intervention should be subject to very strict limitations. This is particularly important in the law enforcement sector, because of the risk for miscarriage of justice and for violations of an individual's' human rights. The Bill provides insufficient safeguards for automated decision- making authorised by law. We recommend that the Bill be amended to include further concrete safeguards.

6.36. Amendments are suggested to Clause 47 in order to:

- Clarify the meaning of decision "based solely on automated processing";
- Ensure automated-decision making does not apply to a decision affecting individual's human rights;
- Strengthen safeguards regarding automated individual decision-making.

6.37. **Clarify the meaning of decision "based solely on automated processing"**

6.38. The right in Article 11 covering Automated Individual Decision Making in the Law Enforcement Directive, is very similar to that in Article 22 of GDPR. For the purposes of clarity of obligations imposed on controllers under Part 3, and for the reasons provided in relation to the related Clause 13, it is important that this explanation is included in the Bill. There is no rationale for omitting it in this section.

6.39. **Ensure automated-decision making does not apply to a decision affecting individual's human rights.**

6.40. This amendment aims to clarify that automated individual decision-making must not apply to decisions that affect individual's human rights.

6.41. This is fundamental to ensure the Bill addresses the current (and planned) reliance of police forces to technologies (such as facial recognition, social media monitoring, etc.) which collect vast amount of personal data and use opaque algorithms to profile and predict crime and make decisions about individuals.[29]

6.42. **New Clause (after Clause 47) - Strengthen safeguards regarding automated individual decision-making**

6.43. The obligation to provide information about the logic involved in the automated decision is already contained in the GDPR (Article 13(2)(f), Article 14(2)(g) and Article 15(1)(h).) However, these provisions are not replicated in the Law Enforcement Directive.

6.44. This information is fundamental to allow transparency of automated decision making and ensure accountability and the rights of data subjects, including having sufficient information in order to challenge such decisions. There is no rationale for omitting it in this section, particularly as there are growing concerns about the risks

[29] For details on current predictive policing plans, see Annex E of Privacy International's briefing on Parts 3 and 4 of the DP Bill, available at: https://privacyinternational.org/sites/default/files/17%2011%2008%20PI%20briefing%20on%20Committee%20Stage%20DPB%20HL%20Parts%203%20and%204.pdf

surrounding the use of automated decision making, including profiling, by the police.

6.45. The proposed new clause replicates Clause 96 of Part 4 of the Bill related to processing by intelligence services. This clause in turn incorporates Council of Europe Convention 108.

6.46. Introducing this clause would give data subjects additional fundamental safeguards. As such it would be compatible with the EU Law Enforcement Directive which states in Article 1(3) that the directive "shall not preclude Member States from providing higher safeguards" than those contained in the Directive.

6.47. Clause 94 - Intelligence services (Part 4)

6.48. **Ensure automated-decision making does not apply to decisions affecting individual's human rights.**

6.49. The Intelligence Services have developed significant capacity to collect and analyse vast amounts of personal data and apply automated decision-making technologies which affect individuals' human rights. For example, Squeaky Dolphin – the programme developed by the Government Communications Headquarters (GCHQ), collects and analyses data from social networks. In the course of Privacy International's litigation before the Investigatory Powers Tribunal, the UK Government disclosed documents which revealed that the UK intelligence agencies hold databases of social media data of potentially millions of people, with lack of any effective oversight on the use of such data, including in the access provided to such databases to third parties.

6.50. Privacy International proposes an amendment to clarify that automated individual decision-making must not apply to decisions that affect individuals' human rights.

6.51. **Clarify the meaning of decision "based solely on automated processing"**

6.52. The rationale set out above in relation to general processing and law enforcement processing, applies equally to the intelligence services in the context of automated-decision making.

6.53. For the purposes of clarity of obligations imposed on controllers, it is important that this explanation is included in Part 4 of the Bill. There is no rationale for omitting it in this section.

7. National Security Certificates

7.1. Privacy International is very concerned by the seemingly unchecked powers to exempt a broad range of data controllers from the obligations under the Bill, on national security (and defence) grounds. These provisions are contained in **Part 2 (Clauses 24, 25, 26), Part 3 (Clause 77) and Part 4 (Clauses 108, 109) of the Bill.**

7.2. The 21st century has brought with it rapid development in the technological capacities of Governments and corporate entities to intercept, extract, filter, store, analyse and disseminate the communications of whole populations. The costs of retaining data have decreased drastically and continue to do so every year, and the means of analysing the information have improved exponentially due to developments in automated machine learning and algorithmic designs. These technological advancements have raised significant challenges to maintain adequate level of protection, safeguards and oversight, particularly when data is processed in the name of national security. The GDPR and the Law Enforcement Directive and in turn this Bill are all mechanisms intended to redress the power imbalance between data controllers and data subjects and avoid unfettered powers to process personal data.

7.3. The reasons given by The Minister of State, Home Office (Baroness Williams of Trafford) in Committee stage seeking to dismiss the need to reform the national security exemption scheme contained in the DPA[30] were inadequate and do not stand up to scrutiny.

7.4. Consistency with the DPA is not a justification for replicating and expanding national security certificates. The DPA is not a gold standard of data protection and many of its provisions have not

[30] "Amendments 124C, 124D, 124E, 124F, 124P and 148E seek to restrict the scope of the national security exemption provided for in Parts 2 and 4 of the Bill. I remind the Committee that Section 28 of the Data Protection Act 1998 contains a broad exemption from the provisions of that Act if the exemption is required for the purpose of safeguarding national security. Indeed, Section 28 provides for an exemption on such grounds from, among other things, all the data protection principles, all the rights of data subjects and all the enforcement provisions. Although we have adopted a more nuanced approach in the Bill, it none the less broadly replicates the provisions in the 1998 Act, which have stood the test of time. Crucially, under the Bill—as under the 1998 Act—the exception can be relied upon only when it is necessary to do so to protect national security; it is not a blanket exception."

received sufficient scrutiny regarding their impact on privacy, in the almost 20 years since the legislation was enacted.

7.5. In fact, in replicating and expanding the opaque and undemocratic national security regime, originally in section 28 of the DPA, the national security exemption regime not only undermines the right to privacy, it is likely to be a significant challenge to securing a positive decision by the European Commission to grant adequacy to the UK post Brexit (see GDPR Article 45, 2(a)). It its current form the regime is deficient in basic principles of legality including clarity, accessibility and transparency and lacking in basic safeguards and oversight.

7.6. As noted by Baroness Hamwee at committee stage: "there are very broad exemptions in Clause 24 and Privacy International even says that the clause has the potential to undermine an adequacy decision."[31]

7.7. Privacy International has concerns about the following aspects of the national security certificate regime proposed in the Bill.

7.8. Some relate to specific parts of the Bill, notably:

- General processing:
  - Lack of clarity on who would benefit from a national security certificate under Part 2 (**Clauses 24, 25 and 26**);
  - Lack of clarity of the scope of the defence purpose exemption (**Clause 26**);
- Law enforcement processing:
  - Broad scope of national security certificate for law enforcement in in Part 3 (**Clause 77**);
- Intelligence agencies:
  - Lack of effective oversight for intelligence agencies in Part 4 (**Clause 108**.)

7.9. **Cross cutting issues:** Some are general in nature and cut across parts 2, 3 and 4 of the Bill (**Clauses 25, 77, 108 and 109**)

- Lack of publicly available information on the national security certificate;
- Timeless and retrospective nature of the national security certificates;

[31] https://hansard.parliament.uk/lords/2017-11-15/debates/9DC4D211-3573-4D97-82DB-92B75547B506/DataProtectionBill(HL)

- Lack adequate safeguards and authorisation.

7.10. General processing

7.11. Clauses 24, 25, and 26 (General Processing): lack of clarity on who would benefit from a national security certificate

7.12. Clauses 24, 25 and 26 of the draft Bill do not apply to law enforcement or intelligence agency processing of data, which are covered in Part 3 and 4 respectively.

7.13. Clauses 24, 25, and 26 lie in the so-called 'applied GDPR (Part 2 Chapter 3) being processing which falls 'outside the scope of EU law.' Until Brexit, processing that falls within the scope of EU law will be covered by the GDPR. However, once we leave the European Union, there is an indication that the 'applied GDPR' may become the source of our data protection rights, and thus include for all general processing the ability to rely upon national security certificates and exempt data protection safeguards.

7.14. This begs the obvious question, which organisations or companies benefit from the national security certificates regimes and do not have to comply with the data protection act safeguards?

7.15. In response, the Minister of State gave an example where an individual is subject of a covert investigation.[32] We are unsure what covert investigations would be carried out by private companies or other entities and why this would not fall under Parts 3 and 4.

7.16. We question whether it is acceptable to ever allow entities who are neither law enforcement (processing for law enforcement purposes under Part 3) nor intelligence services (under part 4) to be exempt from data protection safeguards on national security grounds.

[32] The Minister of State, Home Office (Baroness Williams of Trafford) commented at Committee stage that: "The need for a wide-ranging exemption applies equally under Part 2 of the Bill. Again, a couple of examples will serve to illustrate this. Amendment 124C would mean that a controller processing data under the applied GDPR scheme could not be exempted from the first data protection principle as it relates to transparency. This principle goes hand in hand with the rights of data subjects. It cannot be right that a data subject should be made aware of a controller providing information to, say, the Security Service where there are national security concerns, for example because the individual is the subject of a covert investigation." [ADD HANSARD SOURCE]

7.17. Even if so, we question the breadth of possible exemptions that can be granted under Clause 24. We note that the provisions permit exemption from:
- Lawfulness, fairness and transparency;
- Notification of a personal data breach to the supervisory authority;
- Transfer of personal data to third countries;
- Remedies, liability and penalties;
- Representation of data subjects.

7.18. Lord Kennedy of Southwark stated in Committee stage with respect of Clause 24: "I feel the clause as presently worded it too vague, and that cannot be a good thing when dealing with these serious matters."[33]

7.19. And Baroness Hamwee also noted: "For us, we are not convinced that the clause does not undermine the data protection principles - fairness, transparency and so on - and the remedies, such as notification to the commissioner and penalties."[34]

7.20. Privacy International agrees with these concerns and suggest amendments to **Clauses 24, 25 and 26** to limit the scope of the exemptions.

7.21. **Clause 26 (General processing): Lack of clarity of the scope of the defence purpose exemption**

7.22. Clause 26 in Part 2, Chapter 3, of the Bill introduces a new defence purposes exemption. This is an expansion of the DPA 1998. In the Bill and explanatory notes, it is not explained, defined, or elaborated as to what the purpose of this addition is and what it covers. The Department of Culture, Media and Sport who are responsible for the Bill have been unable to provide us with anything other than a vague definition that it relates to 'defence activities.'

7.23. In response to a request for clarification in committee stage, the Minister of State, Home Office (Baroness Williams of Trafford)

[33] https://hansard.parliament.uk/lords/2017-11-15/debates/9DC4D211-3573-4D97-82DB-92B75547B506/DataProtectionBill(HL)
[34] https://hansard.parliament.uk/lords/2017-11-15/debates/9DC4D211-3573-4D97-82DB-92B75547B506/DataProtectionBill(HL)

indicated that this applies to the armed forces, explaining that this is necessary to capture activities which go beyond "combat effectiveness" wording under the DPA.[35]

7.24. Whilst the Minister states that the term 'combat effectiveness' is no longer adequate, we note that "combat effectiveness" is included in Schedule 11 of the Bill (exemptions to Part 4 of the Bill.)

7.25. We further note that in the Data Protection Act 1998, the exemption for combat effectiveness is limited to subject information provisions, which essentially constitute the fairness principle and the right of subject access.[36]

7.26. The clause in the Bill therefore expands the exemption applicable to 'combat effectiveness' of the armed forces considerably. We are concerned at what appears to be 'mission creep' and an unjustified expansion of an exemption from fundamental data protection

[35] "Amendments 124A, 124M and 124N relate to the exemption in Clause 24 for defence purposes. Amendments 124A and 124N seek to reinstate wording used in the Data Protection Act 1998 which used the term "combat effectiveness". While it may have been appropriate for the 1998 Act to refer to "combat effectiveness", the term no longer adequately captures the wide range of vital activities that the Armed Forces now undertake in support of the longer-term security of the British islands and their interests abroad and the central role of personal data, sometimes special categories of personal data, in those activities. I think that is what the noble Lord was requiring me to explain. Such a limitation would not cover wider defence activities which defence staff are engaged in, for example, defence diplomacy, intelligence handling or sensitive administration activities. Indeed, the purpose of many of these activities is precisely to avoid traditional forms of combat. Yet without adequate provision in the Bill, each of the activities I have listed could be compromised or obstructed by a sufficiently determined data subject, putting the security, capability and effectiveness of British service personnel and the civilian staff who support them at risk.
Let me be absolutely clear at this stage: these provisions do not give carte blanche to defence controllers. Rights and obligations must be considered on a case-by-case basis. Only where a specific right or obligation is found to be incompatible with a specific processing activity being undertaken for defence purposes can that right or obligation be set aside. In every other circumstance, personal data will be processed in accordance with GDPR standards." Committee Day 4, column 2049, available at: https://goo.gl/pC7D7U

[36] Schedule 7, section 37 Armed forces:"2. Personal data are exempt from the subject information provisions in any case to the extent to which the application of those provisions would be likely to prejudice the combat effectiveness of any of the armed forces of the Crown."
Part IV s.27 of the DPA states:
"(2) In this Part "the subject information provisions" means—(a) the first data protection principle to the extent to which it requires compliance with paragraph 2 of Part II of Schedule 1, and (b) section 7 (Rights of Data Subjects and Others).

principles and safeguards, particularly given the lack of justification from the government.

7.27. Whilst we acknowledge that there may be a requirement to limit certain data protection provisions such as data subject access rights in specified circumstances, this does not justify the wholesale abrogation of safeguards in the Bill.

7.28. Law Enforcement processing

7.29. Clause 77 - Broad scope of national security certificate for law enforcement

7.30. The provisions in Part 3, relating to law enforcement processing, go beyond the scope of national security certificates. Clause 77 read together with Clauses 42, 43, 46, 66 attempts to broaden the basis upon which a certificate may relate beyond national security.

7.31. These clauses permit national security certificates to be granted for a wider range of issues that relate to:

- Avoid obstructing an official or legal inquiry, investigation or procedure.
- Avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- Protect public security;
- Protection of national security;
- Protect the rights and freedoms of others.

7.32. We propose amendments to Clause 77 to ensure national security certificates, so that they can only relate to national security. This is done simply by making reference to paragraph (d) in 42(4)(d),43(4)(d), 46(3)(d) and 66(7)(d) to address this concern.

7.33. Intelligence agencies processing

7.34. Clause 108 (intelligence agencies): Lack of effective oversight for intelligence agencies

7.35. Clause 108(2)(c) - (e) of the Bill removes the oversight function of the Information Commissioner.

7.36. During Committee, the Minister of State explained the rationale of why the exemption "needs to be drawn as widely as it is" on the ground that "it may be necessary for an intelligence service to apply this exemption in cases of extreme sensitivity or where the commissioner requested sensitive data but was unable to provide sufficient assurances that it would be held securely enough to protect the information" as well as if "disclosure would be damaging to national security because, say, it would reveal the identity of a covert human intelligence source."[37]

7.37. Rather than remove the oversight role, provided for in Clause 106 (Part 4), Part 5, Schedule 13 and Part 6, Privacy International suggests that this oversight role is instead undertaken by the Investigatory Powers Commissioner (IPCO) who has responsibility for oversight of national security provisions and thus is well-placed to carry out this function without any risks to the agencies.

7.38. Cross cutting concerns

7.39. Clauses 25, 77 and 109 - Lack of publicly available information on the national security certificate

7.40. The regime providing for national security certificates operates on a legal basis that lacks in clarity, precision and comprehension.

7.41. There is a marked absence of public Parliamentary or independent scrutiny of national security certificates since the DPA came into force.

7.42. The only certificates Privacy International is aware that have been published resulted from litigation by Privacy International in relation to Transport for London and separately in relation to bulk personal datasets and bulk communications data and cover GCHQ, MI5 and MI6.

7.43. Baroness Hamwee stated in committee stage: "Those who know about these things say that they do not know what certificates exist under the current regime, so they do not know what entities may benefit from Clauses 24 to 26."[38]

[37] Committee Day 4, column 2049, available at: https://goo.gl/pC7D7U
[38] https://hansard.parliament.uk/lords/2017-11-15/debates/9DC4D211-3573-4D97-82DB-92B75547B506/DataProtectionBill(HL)

7.44. The Minister of State, Home Office (Baroness Williams of Trafford), replied: "I think that the noble Baroness, Lady Hamwee, asked about the publication of security certificates. National security certificates are public in nature, given that they may be subject to legal challenge. They are not secret and in the past they have been supplied if requested. A number are already published online and we will explore how we can make information about national security certificates issued under the Bill more accessible in future."

7.45. Whilst we welcome the statements that the government will explore how they can make information about national security certificates more accessible in the future, they have failed to publish all existing certificates to inform the debate. This must be done without delay. Aside from those that have been published by Privacy International as a result of our litigation, we are not aware what certificates the Minister believes are published.

7.46. We do not accept it is accurate to describe national security certificates as 'public' if the only way they become public is as a result of a legal challenge. Privacy International has experienced great difficulty and resistance from the government in seeking to obtain disclosure in the course of its litigation. It should not be presumed that obtaining disclosure of certificates as a result of litigation is a simple matter. Issues regarding national security certificates in the Bill and the need for transparency and a presumption of placing certificates in the public domain are also raised by the Information Commissioner.[39]

7.47. To address the current opaque nature of national security certificate we propose that all certificates are laid before Parliament and publicly accessible. We suggest amendments to **Clauses 25, 77 and 109** to address this concern in relation to general processing, law enforcement and intelligence services respectively.

7.48. **Clauses 25, 77, 108 and 109 - Timeless nature of the national security certificates**

7.49. The timeless nature of the certificates is illustrated by Privacy International's ongoing litigation in relation to bulk personal

[39] https://ico.org.uk/media/about-the-ico/documents/2172658/dp-bill-lords-briefing-committee-stage-combined-annex-20171030.pdf

datasets and bulk communications data where certificates signed in 2001 covered bulk surveillance activities that commenced five years later, and thus cannot have formed part of the consideration by the Minister as to what activities would be covered by a national security certificate. This undermines the ability for the involvement of a Minister to be seen as any form of safeguard.

7.50. The Minister of State, Home Office (Baroness Williams of Trafford) stated that these certificates "are general and prospective in nature, and arguably no purpose would be served by a requirement that they be subject to a time limitation. For example, in so far as a ministerial certificate allows the intelligence services to apply a "neither confirm nor deny" response to a subject access request, any certificate will inevitably require such a provision."[40]

7.51. Privacy International believes that for the same reason that warrants for interceptions or other surveillance are time limited, so should national security certificates under this Bill: this allows for effective safeguards and oversight. Instead timeless certificates allow for abuse. As the provisions stand, they allow data controllers and processors to continue to rely on certificates for activities that were not considered by the Minister of State when the certificate was signed, as we have noted in relation to our litigation with respect to bulk personal datasets and bulk communications data. These regimes collect enormous amounts of data on everyone in the UK. The certificates relied upon to exempt Bulk Personal Datasets from the data protection regime, were signed before the Bulk Personal Datasets regime came into practice. They were signed in 2001, yet Bulk Personal Datasets were not collected, retained and processed until around 2005.

7.52. If we consider that national security certificates can be relied upon not only by the intelligence agencies, but also law enforcement, the armed forces and unknown entities under Part 2, the idea that certificates can be timeless, despite developments in technology, is of grave concern.

7.53. For the above reasons, we recommend that **Clauses 25, 77, 108 and 109** in the Bill are amended so that:

[40] Committee Day 4, column 2049, available at: https://goo.gl/pC7D7U

7.54. It should not be permitted for the certificate to be retrospective and the statement "or at any time was" required must be removed;

7.55. It should not be permitted for the certificate to have prospective effect. The certificate should be time limited for 6 months and an extension can be sought upon application to the Judicial Commissioner.

7.56. **Clauses 25, 77, and 109 - Lack adequate safeguards and authorisation**

7.57. Privacy International believes that the legal framework proposed for national security certificates lacks adequate safeguards, particularly in relation to authorisation and oversight.

7.58. Under the current provisions a certificate signed by a Minister of the Crown certifying an exemption of all or any provisions is or at any time was required, is conclusive evidence of the fact (see Clauses 25(1), 77(1), 109(1)).

7.59. Adequate safeguards are required as noted by some Peers at Committee stage.[41]

7.60. We regret that the government has been wholly resistant to any such safeguards and oversight. The Minister responded: "I hope that noble Lords will recognise and accept that the national security exemption and certification provisions provided for in Clauses 24 and 25 maintain precisely the same safeguards that currently apply, which are clearly understood and work well. There is no weakening

[41] Baroness Hamwee at committee stage stated:

"I note that under Clause 25(2)(a) a certificate may identify data, "by means of a general description". A certificate from a Minister is conclusive evidence that the exemption is, or was, required for a purpose of safeguarding national security, so is "general description" adequate in this context?

Amendment 124L proposed a new Clause 25 and is put forward against the backdrop that national security certificates have not been subject to immediate, direct oversight. When parliamentary committees consider them, they are possibly tangential and post hoc. Crucially, certificates are open-ended in time. There may be an appeal but the proposed new clause would allow for an application to a judicial commissioner, who must consider the Minister's request as to necessity and proportionality … applying these to each and every provision from which exemption is sought."

https://hansard.parliament.uk/lords/2017-11-15/debates/9DC4D211-3573-4D97-82DB-92B75547B506/DataProtectionBill(HL)

of a data subject's rights or of the requirements that must be met before an exemption can be relied on."

7.61. This response is not sufficient to allay the concerns expressed. First, the opacity of the regime means that there is a distinct paucity of evidence that it is working well. Second, we question whether it works well for the data subject or the data controller. The aims of GDPR are to address the power imbalance and information asymmetry that has resulted from the current regime. Maintaining it is not the answer. Third it fails to acknowledge the different times we live in with respect to data processing. To rely on a scheme that is outdated is to rely on a scheme not fit for the digital age.

7.62. We see no reason not to seek to improve the current regime and the argument that it would create inconsistency or may be difficult could equally have applied in relation to changes that were introduced by the Investigatory Powers Act 2016, where basic safeguards including independent judicial authorisation were proposed and supported by the Government.

7.63. Whilst we maintain our concerns regarding the Investigatory Powers Act which we have raised on numerous occasions, arguably the changes required to improve the national security certificates regime are far less onerous than the mechanisms required by the Investigatory Powers Act.

7.64. In relation to Clauses 25, 77 and 109 in Parts 2, 3 and 4 respectively, we have proposed consistent safeguards as follows:

7.65. **Introduce a procedure for a Minister of the Crown to apply to a Judicial Commissioner for a certificate**. "A Minister of the Crown must apply to a Judicial Commissioner for a certificate, if exemptions are sought from specified provisions … for the purpose of safeguards national security in respect of personal data."

7.66. **To ensure oversight and safeguards are effective, sufficient detail is required in the certificate application.** The Minister must refer to "specific" provisions rather than "all or any" provisions. Each of the provisions in Parts 2, 3 and 4 should require specification of the sections which the certificate seeks to exempt and provide justification for seeking to exempt the personal data to which it applies and the provisions it seeks to exempt. It is impossible to

ensure the power is only exercised where necessary and proportionate if it is possible to identify 'any restriction' to which a certificate relates by means of a 'general description'.

7.67. **An application for a certificate must identify the personal data to which it applies by means of a detailed description of the data**. At the very least it must identify the category of data. It is unacceptable in the current provisions that the requirements are that the Minister 'may' identify personal data with a 'general' description. The Minister of State, Home Office (Baroness Williams of Trafford) appears to endorse this approach when referencing the armed forces, where she states that: "Let me be absolutely clear at this stage: these provisions do not give carte blanche to defence controllers. Rights and obligations must be considered on a case-by-case basis."

7.68. **The Judicial Commissioner must review the Minister's conclusions** as to whether the certificate is necessary on relevant grounds and whether the conduct that would be authorised by the certificate is proportionate to what is sought to be achieved by that conduct; whether it is necessary and proportionate to exempt all provisions specified in the certificate.

7.69. **The decision to issue the certificate must be approved by the Judicial Commissioner**. Where a Judicial Commissioner refuses to approve a Minister's application for a certificate the Judicial Commissioner must give the Minister of the Crown reasons in writing for the refusal. Where a Judicial Commissioner refuses to approve a Minister's application for a certificate the Minister may apply for a review.

7.70. **The right to challenge** a certificate must include those who believe they are directly or indirectly affected.

8. Intelligence agencies - cross border transfers

8.1. Clause 107 (Intelligence agencies): Transfer to personal data outside the UK

8.2. The Bill provides for almost unfettered powers for cross-border transfers of personal data by intelligence agencies without appropriate levels of protection.

8.3. Domestic legislation governing sharing of data by intelligence agencies to third countries is inadequate. Under Article 45 of GDPR, rules for the onward transfer of personal data to another third country are an important factor for a determination of adequacy, which will be relevant to the UK post Brexit.

8.4. As it currently stands, Clause 107 of the Bill provides almost unfettered powers to transfer personal data outside of the United Kingdom by intelligence agencies. The only condition – namely that such transfers are necessary and proportionate for the purposes of the controller's statutory functions or for other purposes as provided in the Security Services Act 1989 or Intelligence Services Act 1994 – does not provide meaningful safeguards as these purposes are significantly broad. As such this clause provides for no requirement of appropriate level of protection as demanded by Article 12 of the Council of Europe modernised "Convention 108" which this clause is said to implement.

8.5. Intelligence sharing arrangements between agencies in different countries are typically confidential and not subject to public scrutiny, often taking the form of secret memoranda of understanding directly between the relevant ministries or agencies. Non-transparent, unfettered and unaccountable intelligence sharing threatens the foundations of the human rights legal framework and the rule of law.

8.6. Article 17 of the International Covenant on Civil and Political Rights protects the right to privacy and requires that any interference with privacy complies with the three overarching principles of legality, necessity and proportionality. In reviewing the UK's implementation of the Covenant, the UN Human Rights Committee has specifically noted the need to adhere to Article 17, "including the principles of legality, proportionality and necessity," as well as the need to put in

"effective and independent oversight mechanisms over intelligence-sharing of personal data."[42]

8.7. The European Court of Human Rights has also expressed concerns regarding the practice of intelligence sharing and the need for greater regulation and oversight: "The governments' more and more widespread practice of transferring and sharing amongst themselves intelligence retrieved by virtue of secret surveillance – a practice, whose usefulness in combating international terrorism is, once again, not open to question and which concerns both exchanges between Member States of the Council of Europe and with other jurisdictions – is yet another factor in requiring particular attention when it comes to external supervision and remedial measures."[43]

8.8. In the context of Privacy International's litigation on bulk data, where the legality of transfer and sharing of data is the subject of court proceedings, it has emerged that there is little, if any, oversight in respect of the transfer of bulk data or remote access to it. It is unclear whether the use of shared data is even auditable or audited.

8.9. In separate litigation challenging UK bulk interception and UK access to data collected under US bulk surveillance programs, Privacy International submit that in relation to communicating intercepted material to other parties, under section 15(2) Regulation of Investigatory Powers Act 2000, the Secretary of State is simply required to ensure that the disclosure of section 8(4) intercepted material "is limited to the minimum that is necessary for authorised purposes." Those authorised purposes (section 15(4)) are broadly drawn and do not limit the power to disseminate intercepted material to situations where there is a reasonable suspicion that an individual has committed or is likely to commit a criminal offence or is a threat to national security. The section 15(2) limitation does not apply to dissemination of intercepted material to foreign authorities (section 15(6)). The Independent Reviewer of Terrorism has noted, in this respect, that there is "no statute or Code of Practice

[42] Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, U.N. Human Rights Committee, U.N. Doc. CCPR/C/GBR/ CO/7, para. 24 (17 Aug. 2015).

[43] Szabó and Vissy v. Hungary, App. No. 37138/14, European Court of Human Rights, Judgment, para. 78 (12 Jan. 2016).

governing how exchanges [to foreign authorities] should be authorized or take place.". We note that whilst chapter 12 of the Interception of Communications Code of Practice (as amended in January 2016) sets out some rules for requesting and handling unanalysed intercepted communications from a foreign government it does not provide adequate safeguards for transfers of personal data by UK Intelligence Services. These are minimal, focus on interception warrants under section 8(4) of RIPA and requests by the UK to foreign governments.

8.10. We propose amendments to Clause 107:

8.10.1. To specify that transfer must be "provided by law";

8.10.2. To bring the transfer of personal data to third parties under Part 4 in line with provisions under Part 3 (Law Enforcement.) There is no rationale to justify transfers by intelligence agencies having lower safeguards than those applicable to law enforcement's transfers.

Annex A: Proposed draft amendments

Amendments proposed by Privacy International, in order of appearance of the Bill.

References are to the Data Protection Bill [HL] [as amended in Committee] (available at: https://publications.parliament.uk/pa/bills/lbill/2017-2019/0074/18074.pdf)

PART 2 - GENERAL PROCESSING

Clause 7: Lawfulness of processing: public interest etc. – limit condition

Page 5, line 8, remove "includes" and insert "refers to"

Clause 9: Special categories – remove ability to vary/ omit safeguards via regulations

Page 6, line 5, leave out "varying or omitting conditions or"

Schedule 1: Paragraph 18 - remove condition for political parties

Page 121, line 6, remove paragraph 18

Clause 13: Automated decision-making authorised by law: safeguards

Clarify the meaning of decision "based solely on automated processing"

Page 7, line 16, at end insert:

"() 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."

Strengthen safeguards regarding automated decision-making authorised by law

Page 7, line 31 at end, after "and" insert:

"provide meaningful information about the logic involved as well as the significance and legal consequences of such processing; and"

Ensure full right to challenge and redress regarding automated decision-making authorised by law

Page 7, line 44, after paragraph (5), insert:

"() Data subject affected by a qualifying significant decision under this section retains the right to lodge a complaint to the Commissioner under Clause 156 and to seek compliance order by a court under Clause 158."

Clause 15: Power to make further exemptions etc. by regulations

Remove wide ranging regulation making power

Page 8, line 42, leave out clause 15 and at end insert -

"15A Power to make further exemptions etc. by amendment to the 2017 Act

The powers in Article 6(3), 23(1), 85(2), and 89 of the GDPR to legislate on the legal basis for processing, restrictions to the scope of obligations and rights, processing carried out for journalistic purposes or the purpose of academic artistic or literary expression and process for archiving purposes, together with the respective safeguards set out in those Articles, are to be exercised by means of amendments of the 2017 Act."

Schedule 2: Paragraph 4 - Remove immigration exemption

Page 129, line 18, leave out paragraph 4

Clause 24: national security and defence exemption

Page 15, line 1 to page 15, line 42, leave out clause 24

Clause 25: National security: certificate

Page 15, line 44, delete "Subject to subsection (3), a certificate signed by"

Page 15, line 45, insert after "a Minister of the Crown" the words "must apply to a Judicial Commissioner for a certificate, if exemptions are sought"

Page 15, line 45, delete "certifying that exemption"

Page 15, line 45, insert after "from" the word "specified"

Page 15, line 45, delete the words "all or any of the"

Page 15, line 45 – 46 delete the words "listed in section 24(2) is, or at any time was, required"

Page 15, line 47, delete the words "conclusive evidence of that fact"

Page 15, line 43, insert new subsections:

(2) The decision to issue the certificate must be:
approved by a Judicial Commissioner,
Laid before Parliament,
published and publicly accessible on the Cabinet Office website.

(3) In deciding whether to approve an application under subsection (1), a Judicial Commissioner must review the Minister's conclusions as to the following matters:
Whether the certificate is necessary on relevant grounds, and
Whether the conduct that would be authorised by the certificate is proportionate to what it sought to be achieved by that conduct, and
Whether it is necessary and proportionate to exempt all provisions specified in the certificate.

Page 16, line 1, insert before "A certificate" the words "An application for"

Page 16, line 2, delete the word "may"

Page 16, line 2, insert before the word "identify", the word "Must"

Page 16, line 2, delete the word "general"

Page 16, line 2, insert after the words "means of a" the word "detailed"

Page 16, line 4, insert new subsections in clause 24(2) which state:

...
Must specify each provision of this Act which it seeks to exempt, and

Must provide a justification for both (a) and (b).

...

Page 16, line 4, delete the subsection (2(b)) which states "may be expressed as having prospective effect."

Page 16, after line 4, insert new subsections which state:

Where a Judicial Commissioner refuses to approve a Minister's application for a certificate under this Chapter, the Judicial Commissioner must give the Minister of the Crown reasons in writing for the refusal.

Where a Judicial Commissioner refuses to approve a Minister's application for a certificate under this Chapter, the Minister may apply to the Information Commissioner for a review of the decision.

<u>It is not permissible for exemptions to be specified in relation to:</u>

Chapter II of the applied GDPR (principles) –

Article 5 (lawful, fair and transparent processing)

Article 6 (lawfulness of processing)

Article 9 (processing of special categories of personal data)

Chapter IV of the applied GDPR –

iv. Articles 24 – 32 inclusive;

v. Articles 35 – 43 inclusive;

c. Chapter VII of the applied GDPR (remedies, liabilities and penalties)

vi. Article 83 (general conditions for imposing administrative fines);

vii. Article 84 (penalties);

d. Part 5 of this Act –

viii. Section 112;

ix. Section 113 (general functions of the Commissioner), subsections (3) and (

x. Sections 114 – 117;

e. <u>Part 7 of this act, section 173 (representation of data subjects)</u>

Page 16, line 5, insert after the words "Any person" the words "who believes they are"

Page 15, line 5, insert after the word "directly" the words "or are indirectly"

Page 15, line 6, insert after the words "against the certificate" the word ", and"

Page 15, line 6, insert subsection which states "rely upon section 173 of this Act"

> Any person who believes they are directly or are indirectly affected by a certificate under subsection (1)

may appeal to the Tribunal against the certificate, and

rely upon section 173 of this Act.

Page 16, lines 7-8, delete the words "applying the principles applied by a court on an application for judicial review"

Page 16, line 8, insert after the words "judicial review" the words "it was not necessary or proportionate to issue"
Page 6, lines 7 – 8, delete the words "the Minister did not have reasonable grounds for issuing"

Page 16, lines12 - 30, delete clauses (5), (6), (7), (8), (9).

Clause 26 - National Security and defence

page 16, line 35, delete the words 'and defence'
page 16, line 41 - 42, delete the words 'or for defence purposes'
page 17, delete subsections (2) (3) (4).

PART 3 - LAW ENFORCEMENT PROCESSING

Clause 33(6) & (7): Regulation making power re conditions for processing

Restrict the scope of delegated powers to add, vary or omit conditions for processing.

Page 20, line 24, leave out paragraphs (6) and (7)

Or

Page 20, line 26, leave out "affirmative resolution procedure" and insert "super- affirmative procedure in accordance with section 18 of the Legislative and Regulatory Reform Act 2006"

Clause 47: Right not to be subject to automated decision-making

Clarify the meaning of decision "based solely on automated processing"

Page 28, line 30, add the following: "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."

Ensure automated decision-making does not apply to a decision affecting an individual's human rights

Page 28, line 30, after "by law" add the following: ", subject to subsection ()"

Page 28, line 30, add new sub clause:

"() A controller may not take a significant decision based solely on automated processing if that decision affects the rights of the data subject under the Human Rights Act 1998"

New Clause - Strengthen safeguards regarding automated individual decision-making

Page 29, line 25, after Clause 48 insert the following new clause:

"() Right to information about decision-making

Where—

the controller processes personal data relating to a data subject, and

results produced by the processing are applied to the data subject,

the data subject is entitled to obtain from the controller, on request, knowledge of the reasoning underlying the processing.

(2) Where the data subject makes a request under subsection (1), the controller must comply with the request without undue delay."

Clause 77: National security certificates: certificates by the Minister

Page 44, line 39, insert after "A Minister of the Crown" the words "must apply to a Judicial Commissioner for a certificate".

Page 44, line 39, delete the words "may issue a certificate certifying"

Page 44, line 40, insert "(d)" after 42(4), after (43(4), after 46(3) and after 66(7) so it reads 42(4)(d), 43(4)(d), 46(3)(d) or 66(7)(d),

Page 44, line 40, insert after 66(7) the words "if he or she believes".

Page 44, insert new clause after 77(1) which reads:

() The decision to issue the certificate must be:
Approved by a Judicial Commissioner,
(b)Laid before Parliament,
(c) Published and publicly accessible on the Cabinet Office website.

Page 44, line 42 insert before the words "The certificate may" the words "An application for a"

Page 44, line 42, before the word "certificate" delete the word "The"

Page 44, line 42, after the word "certificate" delete the word "may"

Page 44, line, after the word "certificate" insert the word "must"

Page 45, line 1, delete the words "relate to a" and "which"

Page 45, line 1 insert before the word "relate" the words "a. Identify which"

Page 45, line 2, delete the words "has" and "imposed"

Page 45, line 2, after the words "a controller has" insert the words "seeks to"

Page 45, line 2-3, add in sub-subsection (d) to all references clauses to read: 42(4)(d), 43(4)(d), 46(3)(d), 66(7)(d).

Page 45, line 3, delete the word "or" and insert the word "and"

Page 45, line 4-5, delete the entire sub-clause which reads "(b) identify any restriction to which it relates by means of a general description."

Page 45, line 5, insert new clauses as sub-clauses to clause 77(2):
(c) Identify the personal data to which it applied by means of a detailed description, and
(d) provide a justification for both (a) and (c).

Page 45, line 6, after clause 77(2) insert new clause: which reads:

() A certificate is valid for 6 months.

In deciding whether to approve an application under subsection (1), a Judicial Commissioner must review the Ministers' conclusions as to the following matters:

Whether the certificate is necessary on relevant grounds, and Whether the conduct that would be authorized by the certificate is proportionate to what is sought to be achieved by that conduct, and (c) Whether it is necessary and proportionate to exempt all provisions specified in the certificate.

Page 45, lines 6 to 9, delete entire clause 77(3)

Page 45, lines 10 to11, delete entire clause 77(4)

Page 45, line 12, insert new clauses before 77(5) which read:

() Where a Judicial Commissioner refuses to approve a Minister's application for a certificate under this section, the Judicial Commissioner must give the Minister of the Crown reasons in writing for the refusal.

Where a Judicial Commissioner refuses to approve a Minister's application for a certificate under this Chapter, the Judicial Commissioner must give the Minister of the Crown reasons in writing for the refusal.

Page 45, line 12, insert after the words "Any person" the words "who believes they are"

Page 45, line 12, insert after the word "directly" the words "or are indirectly"

Page 45, line 13, before the word "may" insert "(a)" and after the word "certificate" insert the word ", and"

Page 45, line 13 after the words "against the certificate" insert "(b) rely upon section 173 of this Act."

Page 45, line 15, after the words "judicial review" insert the words "it was not necessary or proportionate to issue"

Page 45, lines 19 - 36, delete in their entirety, clauses (7), (8), (9), (10) and (11).

Page 45, lines 41 - 44, delete in its entirety, clause (13).

PART 4 - INTELLIGENCE SERVICES PROCESSING

Clause 84: The first data protection principle

Restrict the scope of delegated powers to add, vary or omit conditions for processing

Page 49, line 17:

Leave out subsections (3) and (4)

Or

Page 49, line 19:

Leave out "affirmative resolution procedure" and insert "super-affirmative procedure in accordance with section 18 of the Legislative and Regulatory Reform Act 2006"

Schedule 9: Conditions for processing under Part 4

Remove the condition that allows processing for the exercise of any other functions of a public nature exercise in the public interest by a person

Page 177, line 39
Leave out subsection 5(e).

Remove the condition that allows processing necessary for the purposes of legitimate interests pursued by the controller or third party/ parties to whom the data is disclosed.

Page 178, line 1
Leave out subsection (6)

Clause 94: Right not to be subject to automated decision-making

Ensure automated-decision making does not apply to decisions affecting individual's human rights

Page 54, line 31, add after "law": "unless the decision affects an individual's rights under the Human Rights Act 1998"

Clarify the meaning of decision "based solely on automated processing"

Page 54, line 29, add the following: "() 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."

Clause 107: Transfers of data outside the UK

Additional safeguards

Page 59, line 37, after "the transfer is" add "is provided by law and is".

Page 59, line 42, after (2) add, (3), (4), (5) and section ().

Page 60, line 1, add new sub-clauses 107(3), (4), (5) and new section ():

(3) The transfer falls within this subsection if the transfer–

is based on an adequacy decision (see section 72)

if not based on an adequacy decision, is based on there being appropriate safeguards (see section 73), or

if not based on an adequacy decision or on there being appropriate safeguards, is based on special circumstances (see section 74 as amended by subsection (5)).

(4) A transfer falls within this subsection if

The intended recipient is a person based in a third country that has (in that country) functions comparable to those of the controller or an international organisation, or

(b)The transfer meets the following conditions

The transfer is strictly necessary in a specific case for the performance of a task of the transferring controller as provided by law or for the purposes set out in subsection (2).

The transferring controller considers that the transfer of the personal data under subsection (4)(a) would be ineffective or inappropriate (for example, where the transfer could not be made in sufficient time to enable its purpose to be fulfilled).

The transferring controller informs the intended recipient of the specific purpose or purposes for which the personal data may, so far as necessary, be processed.

The transferring controller informs a controller under subsection (4)(a) of the transfer in that third country without undue delay of the transfer, unless this would be ineffective or inappropriate

The transferring controller documents any transfer and informs the Commissioner about the transfer on request.

(5) The reference to law enforcement purposes in subsection (4) of Article 74 are to be read as the purposes set out in subsection (2).

() Subsequent transfers

(1) Where personal data is transferred in accordance with section 107, the transferring controller must make it a condition of the transfer that the data is not to be further transferred to a third country or international organisation without the authorisation of the transferring controller.

(2) A transferring controller may give an authorisation under subsection (1) only where the further transfer is necessary for the purposes in subsection (2).

(3) In deciding whether to give the authorisation, the transferring controller must take into account (among any other relevant factors) –

the seriousness of the circumstances leading to the request for authorisation,

the purpose for which the personal data was originally transferred, and

the standards for the protection of personal data that apply in the third country or international organisation to which the personal data would be transferred.

Clause 108: National Security

Restricting the scope of the national security exemption

Page 60, line 10, after the words "(rights of data subjects)" add the words "except section 94(1)".

Page 60, line 11 - 23, delete all clauses 108(2)(c) to (e). Page 60, line 11 insert a new sub-clause (3) which reads:

In Chapter 4, section 106 (communication of personal data breach), the Commissioner for the purposes of the Intelligence Services processing is the Investigatory Powers Commissioner.

In Part 5, inspection in accordance with international obligations, the Commissioner for the purposes of the Intelligence Services processing is the Investigatory Powers Commissioner.

In Schedule 13, other general functions of the Commissioner, paragraphs 1(a) and (g) and 2, the Commissioner for the purposes of the Intelligence Services processing is the Investigatory Powers Commissioner.

In Part 6, Enforcement, the Commissioner for the purpose of the Intelligence Services processing is the Investigatory Powers Commissioner.

Clause 109: National security: certificate

Making national security certificates more transparent and accountable

Page 60, line 24, delete 'Subject to sub-section (3) a certificate signed by a"

Page 60, line 24, insert after the words "certificate signed by" the word "A"

Page 60, line 25, before the word "certifying" insert the words "must apply to a judicial commissioner for a certificate, if exemptions are sought"

Page 60, line 25, delete the words “certifying that exemption”

Page 60, line 25, after the word “from” insert the word “specified”

Page 60, line 25, delete the words “all or any of the”

Page 60, line 26, delete the words “is, or at any time was required”

Page 60, line 27, delete the words “is conclusive evidence of that fact”.

Page 60, line 29, after clause (1) insert new clauses:

() A certificate is valid for 6 months.

() The decision to issue the certificate must be:
approved by a Judicial Commissioner,
laid before Parliament,
published and publicly accessible on the Cabinet Office website.

() In deciding whether to approve an application under subsection (1), a Judicial Commissioner must review the Minister’s conclusions as to the following matters:

Whether the certificate is necessary on relevant grounds, and
Whether the conduct that would be authorised by the certificate is proportionate to what it sought to be achieved by that conduct, and
Whether it is necessary and proportionate to exempt all provisions specified in the certificate.

Page 60, line 29, insert before the word “certificate” the words “An application for a”

Page 60, line 29, delete the words “under subsection (1)

Page 60, line 30 delete the word “may”

Page 60, line 30, insert at the start of the subsection the word “Must”

Page 60, line 30, delete the word “general”

Page 60, line 31, before the word “description” insert the word “detailed”

Page 60, line 32, delete the subsection which reads "(b) may be expressed as having prospective effect".

Page 60, line 33, insert new clauses:
(2) …
(c) Must specify each provision of section 108(2) which it seeks to exempt, and
(d) Must provide a justification for seeking to exempt the personal data to which it applied and the provisions it seeks to exempt.

() Where a Judicial Commissioner refuses to approve a Minister's application for a certificate under this Chapter, the Judicial Commissioner must give the Minister of the Crown reasons in writing for the refusal.

() Where a Judicial Commissioner refuses to approve a Minister's application for a certificate under this Chapter, the Minister may apply to the Information Commissioner for a review of the decision.

Page 60, line 33, insert after the words "Any person" the words "who believes they are" and after the words "directly" insert the words "or are indirectly".

Page 60, line 34, create a subsection (a) for "may appeal to the Tribunal against the certificate" and insert new subsection "(b) rely upon section 173 of this Act."

Page 60, line 35 - 36 delete the words "applying the principles applied by a court on an application for judicial review" and insert the words "it was not necessary or proportionate to issue"

Page 60, lines 36 - 37 delete the words "the Minister did not have reasonable grounds for issuing"

Page 60, lines 40-44 and page 61 lines 1 – 7 delete clauses (5), (6), (7) and (8).

Clause 110 - Other exemptions

Schedule 11: Exemptions under Part 4

Restrict the conditions for processing under Part 4

Page 179, line 33
Leave out paragraph 1

Page 181,
Leave out paragraphs 10 (Negotiations), 12 (Exam scripts and marks), 13 (Research and statistics), 14 (Archiving in the public interest).

PART 5 - THE INFORMATION COMMISSIONER

New clause after clause 120 - add requirement to publish public interest code

Page 66, line 11, at end insert: "120A Public interest code

The Commissioner must prepare a code of practice which contains –

Practical guidance in relation to the processing of personal data in the public interest
Practical guidance in relation to the processing of personal data in the substantial public interest
Such other guidance as the Commissioner considers appropriate to promote an understanding of the application of the terms public interest and substantial public interest in the context of the 2017 Act.

Where a code under this section is in force, the Commissioner may prepare amendments of the code or a replacement code.

Before preparing a code or amendments under this section, the Commissioner must consult the Secretary of State and –
Data subjects
Persons who appear to the Commissioner to represent the interests of data subjects.

A code under this section may include transitional provision or savings.

In this section –
"public interest" means public interest as used in the 2017 Act and the GDPR

"substantial public interest" means substantial public interest as used in the 2017 Act and the GDPR

N.B Consequential amendments would be needed to s121 – 123 to include reference to Code published under 120A

PART 7 - SUPPLEMENTARY AND FINAL PROVISION

Clause 169: Regulations and consultation

Require public consultation re regulations

Page 95, line 36, after Commissioner insert ", data subjects and persons who appear to the Commissioner to represent the interests of data subjects,"

Page 95, line 38, leave out paragraph (a)

Amendment Clause 173: Representation of data subjects

Adding rights from Article 80(2) of GDPR

Page 98, line 16, at end insert—

"( )
In relation to the processing of personal data to which the GDPR applies, Article 80(2) of the GDPR (representation of data subjects) permits and this Act provides that a body or other organisation which meets the conditions set out in that Article has the right to lodge a complaint, or exercise the rights, independently of a data subject's mandate, under—
(an) Article 77(right to lodge a complaint with a supervisory body);
(b) Article 78 (right to an effective judicial remedy against a supervisory authority); and
(c) Article 79 (right to an effective judicial remedy against a controller or processor), of the GDPR if it considers that the rights of a data subject under the GDPR have been infringed as a result of the processing."

Page 98, line 26, at end insert –

"() The rights in subsection (2)(a) - (d) may also be exercised by a body or other organisation that meets conditions in subsections (3) and (4) independently of a data subject's authorisation."