PRIVACY INTERNATIONAL

Privacy International's submission on the Data Protection Bill to the Joint Committee on Human Rights

November 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

Summary

The Data Protection Bill introduced to the House of Lords in September 2017, requires close scrutiny to ensure that human rights are protected.

The right to privacy (and data protection) is enshrined in UK law, including the rights under the European Convention on Human Rights, protected through the Human Rights Act 1998 and in other international obligations of the UK. The right to privacy is intrinsically linked with other human rights, including freedom of expression.

This briefing outlines the human rights context of this Bill and sets out in detail why certain provisions of the Bill must be amended in order to be compatible with human rights, in particular the principles of **legality**, **necessity** and **proportionality**.

The provisions of particular concern from a human rights perspective (especially Article 8 of the European Convention on Human Rights), expanded upon in this briefing cover the following areas:

- **Delegated Powers**
- **Representation of Data Subjects**
- **Conditions for and exemptions from processing of personal data**
- **Automated Decision-Making**
- **National Security Certificates**
- **Intelligence services, cross-border transfers**

The provisions require to be amended to ensure clarity and foreseeability in the law, introduce and strengthen safeguards and protect the rights of data subjects.

Privacy International's proposed amendments are gathered together in Annex A to this briefing. [1]

[1] See also, 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).

1 Introduction

1.1 Privacy is a fundamental right, essential to autonomy and the protection of human dignity, serving as the foundation upon which many other human rights are built. Privacy enables us to create barriers and manage boundaries to protect ourselves from unwarranted interference in our lives, which allows us to negotiate who we are and how we want to interact with the world around us. Privacy helps us establish boundaries to limit who has access to our bodies, places and things, as well as our communications and our information. The rules that protect privacy give us the ability to assert our rights in the face of significant power imbalances. As a result, privacy is an essential way we seek to protect ourselves and society against arbitrary and unjustified use of power, by reducing what can be known about us and done to us, while protecting us from others who may wish to exert control. Privacy is essential to who we are as human beings, and we make decisions about it every single day. It gives us a space to be ourselves without judgement, allows us to think freely without discrimination, and is an important element of giving us control over who knows what about us.

1.2 Individuals, as citizens and consumers need to have the means to exercise their right to privacy and protect themselves and their information from abuse. This is particularly the case when it comes to our personal information. Data protection is about safeguarding the fundamental right to privacy, which is enshrined in international and regional laws and conventions.

1.3 The Committee will be familiar with the relevant International and Regional treaties which articulate that the UK must respect the human right to privacy and in turn data protection:

The European Convention of Human Rights (Article 8)

> *"1. Everyone has the right to respect for his private and family life, his home and correspondence.*
>
> *2. There shall be no interference by a public authority with the exercise of this right except such as in the accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

The European Charter of Fundamental Rights (Articles 7 and 8)

> *"7. Everyone has the right to respect for his or her private and family life, home and communications.*

8. (1) Everyone has the right to the protection of personal data concerning him or her; (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified; (3) Compliance with these rules shall be subject to control by an independent authority."

The Universal Declaration of Human Rights (Article 12)

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of law against such interference or attacks."

The International Covenant on Civil and Political Rights (Article 17)

"1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks."

Organization for Economic Cooperation and Development (OECD) Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Part 1: General (23 September 1980)

"2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a risk to privacy and individual liberties...

6. These Guidelines should be regarded as minimum standards which can be supplemented by additional measures for the protection of privacy and individual liberties, which may impact transborder flows of personal data."

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Article 1: Object and Purpose (28 January 1981)

"The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")."

Convention on the Rights of the Child, Article 16 (20 November 1989)

"1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honour and reputation.

2. The child has the right to the protection of the law against such interference or attacks."

International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, Article 14 (18 December 1990)

"No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy, family, correspondence or other communications, or to unlawful attacks on his or her honour and reputation. Each migrant worker and member of his or her family shall have the right to the protection of the law against such interference or attacks."

Convention on the Rights of Persons with Disabilities, Article 22: Respect for Privacy (13 December 2006)

"1. No person with disabilities, regardless of place of residence or living arrangements, shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence or other types of communication or to unlawful attacks on his or her honour and reputation. Persons with disabilities have the right to the protection of the law against such interference or attacks.

2. States Parties shall protect the privacy of personal, health and rehabilitation information of persons with disabilities on an equal basis with others."

1.4 Furthermore, the right to privacy and data protection is intrinsically linked to other human rights such as:

- The right to freedom of expression
- The right to a fair trial
- The right to an effective remedy
- The right not to be discriminated against
- The right to freedom of thought, conscience and religion
- The right to freedom of assembly and association
- The right to peaceful enjoyment of possessions
- The right to free elections

2 Delegated powers

2.1 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 and damaging democratic accountability. These regulations permit the executive to interfere with the right to privacy without appropriate safeguards. The wide-ranging power of these regulation making powers place and their so called 'Henry VIII clause' nature, have been heavily criticised by both the Delegated Power and Regulatory Reform Committee and the House of Lords Constitutional Committee.

2.2 The conditions (legal basis) for processing personal data (especially special categories of personal data) and any exemptions to the rights and obligations under the Bill (and GDPR) should be clearly set out on the face of the Data Protection 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.

2.3 In order to comply with the UK's human rights obligations, these conditions and exemptions which permit the processing of personal data (and therefore an interference with an individual's right to privacy) and any changes to them, must be in accordance with the law, necessary and proportionate. These regulation making powers create uncertainty regarding the legal framework for processing personal data and this in turn impacts on the accessibility and foreseeability of the law governing interference with the right to privacy. Furthermore, the lack of effective parliamentary scrutiny heightens the risk that the provisions in the regulations will not meet the requirement of being necessary and proportionate to achieve a legitimate aim in a democratic society.

2.4 The impact of the delegated powers on parliamentary sovereignty in turn impacts on the rule of law and the respect and realisation of human rights in the UK.

2.5 For these reasons, the regulation making powers of concern in the Bill must be removed, narrowed and as a very minimum include an assessment of the impact on the rights of individuals and be subject to adequate consultation.

2.6 The regulation making powers in the Bill that cause most concern are described below, together with the concerns of the parliamentary committees. The proposed amendments are in Annex A to this briefing.

2.7 **Part 2 - General Processing**

2.8 **Clause 9(6): Regulation making power to add, vary or omit conditions or safeguards for the processing of special categories of personal data**

2.9 Article 9.1 of GDPR prohibits the processing of special categories of personal data (previously 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 (28) for processing special categories of personal data in Schedule 1.

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

2.11 ***Constitutional Committee:*** ***"****This is a very broad Henry VIII power, potentially affecting all of the conditions and safeguards in schedule 1…"*

2.12 ***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 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."*

2.13 **Clause 15: Power to make wide ranging exemptions to GDPR application**

2.14 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.

2.15 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.

2.16 ***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."*

2.17 ***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"*

2.18 **Part 3 - Law Enforcement Processing**

2.19 **Clause 33: Power to amend conditions for processing personal data**

2.20 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.

2.21 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 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.

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

2.23 ***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)."*

2.24 **Part 4 - Intelligence Services Processing**

2.25 **Clause 84(3): Power to amend conditions for processing personal data**

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

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

2.28 **Clause 111: Power to make further exemptions**

2.29 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 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.

2.30 ***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.*

2.31 ***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 Representation (Article 80(2) of GDPR)

3.1 In order to protect and uphold the right to privacy (as enshrined in Article 8 of ECHR), individuals need effective remedies when their right is infringed.

3.2 The Bill does not provide for qualified non-profit organisations to pursue data protection infringements of their own accord, as provided by the EU General Data Protection Regulation (GDPR) in its article 80(2). We, along with UK digital rights and consumer organisations strongly recommend that the Bill is amended to include this provision.

3.3 We have proposed a new clause at Clause 173 of the Bill to include rights in Article 80(2) of GDPR. These amendments would enable qualified NGOs to take up collective actions on behalf of consumers and citizens affected by data breaches and other activities which breach the provisions of GDPR and the Bill and may cause them financial or other detriment and of which they may not be aware/ be in a position to take action on their own.

3.4 Such empowerment is provided for on an optional basis in GDPR (Article 80(2)) and we are proposing that these rights are incorporated into the provisions of the Data Protection Bill, to seek to ensure that those that breach their data protection obligations are held to account and improve their practices. Such powers of collective redress are vitally important since personal data has become such an essential part of the national and global economy, while the imbalance of power and the information asymmetry makes it particularly difficult for individuals to claim their rights effectively. Furthermore, many breaches of data protection law affect thousands rather than single individuals, so collective redress actions are more efficient in such circumstances, as illustrated by many such successful actions carried out by NGOs in countries around Europe, based both on consumer protection and data protection legislation.

4 Conditions for processing personal data / exemptions

4.1 The Bill contains conditions for processing and exemptions to data protection obligations that are wide-ranging, poorly defined and where no justification is provided as to the legitimate aim pursued. Given that the conditions for processing and exemptions justify an interference with the right to privacy (and other rights such as freedom of expression and free elections) it is imperative that these interferences are in accordance with the law, necessary and proportionate.

4.2 These concerns cover:

- Ambiguity of the term public interest in the Bill (throughout the Bill)
- Processing by political parties of special category personal data (para 17 of Sch 1 to the Bill)
- An exemption for processing personal data for effective immigration purposes (para 4 of Sch 2 to the Bill)
- Conditions and exemptions provided to the UK Intelligence Services (Part 4 of the Bill)

4.3 There is no definition in the Bill of what constitutes "substantial public interest" when processing special categories/ sensitive personal information, or why the conditions for processing set out in the Bill such information constitute such interest. This will result in lack of adequate safeguards to protect such sensitive data in all cases and we are concerned that these provisions provide for conditions which interfere with the right to privacy and are not accessible and foreseeable and also not necessary and proportionate. This concept should more clearly explained/ defined through statutory guidance and narrowly interpreted.

4.4 In particular we are concerned about the specific condition which permits political parties to process personal data revealing political opinions and the implications this has both in terms of the right to privacy and freedom of expression and free elections. This specific condition should be removed/ or explained and narrowed.

4.5 The conditions for processing and exemptions in the Bill should be clear, necessary and proportionate. This is not demonstrated in terms of the immigration exemption in Part 2 of the Bill or certain conditions and exemptions in Part 4 of the Bill, covering processing by the Intelligence Services.

4.6 **Meaning of public interest**

4.6.1 The term 'public interest' is used throughout the Data Protection Bill and is key to applying many of its provisions.[2] These are set out in a table below. 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). 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.

4.6.2 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.

4.6.3 Clause 7 of the Bill, detracts from these safeguards by providing 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.

4.6.4 Processing of personal data constitutes an interference with individual's right to privacy and the protection of their personal data, it also has the potential to interfere with other rights such as the right to freedom of expression. Therefore, in accordance with human rights obligations it is essential that any such interference is in accordance with the law, these include the UK's obligations under the Human Rights Act 1998/ European Convention on Human Rights.

[2] 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.

4.6.5 The European Court of Human Rights has identified that the requirement that any interference with private life must be in "*accordance with the law*" under Article 8(2) will only be met where three conditions are satisfied: (i) the measure must have some basis in domestic law (ii) the domestic law must be compatible with the rule of law, i.e. the law must have a sufficient quality such as to be accessible and foreseeable to affected persons and (iii) there must be adequate and effective guarantees against abuse (*Klass*, §§43-44 and 50; *Malone*, §66; *Weber*, §84; *Gillan and Quinton v UK* (2010) 50 EHRR 45, §§76-77).

4.6.6 In relation to quality of law, in the case of T*elegraaf Media Nederland Landelijke Media BV and others v Netherlands* ("Telegraaf Media"), App. No. 39315/06, 22 November 2012 (at §90),the Court clarified that for the law to be accessible to the person(s) concerned, it "must indicate the scope of any ... discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference". See also, Weber, §§93-95 and 145; Segerstedt-Wiberg and Others v. Sweden, no. 62332/00, §76, ECHR 2006-VII; Liberty, §§62-63; Kennedy, §152.

4.6.7 Further clarification on the scope of "public interest" and "substantial public interest" in the Bill is required. Guidance is needed on how these terms are to be interpreted when applying the provisions of the Bill. The application of a public interest test or substantial public interest test, will to an extent be dependent on the particular circumstances of the processing. However, 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 to 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.

4.6.8 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. 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.

4.6.9 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.

4.6.10 Care would need to be taken that the Code adequately accounted for freedom of expression and freedom of the press.

4.7 Conditions for processing special categories of personal data - Political Parties

4.7.1 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*;"

4.7.2 Neither the Bill nor the explanatory notes explain how the conditions in Part 2 of Schedule 1 meet the requirements of Article (9)(2)(g). Of particular concern is paragraph 17 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. This can include, but is not restricted to, campaigning, fundraising, political surveys and case-work. Whilst a variation of this condition was included in a statutory instrument to the Data Protection Act 1998, technology and data processing in the political arena has 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 information about the political opinions of an individual (primarily through profiling).

4.7.3 It is essential that consideration is given to the way in which this condition for processing can interfere with the right to privacy and freedom of expression, particularly in lights of technological developments and the granularity of processing of personal data. 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 any chilling effect on the right to freedom of expression and impact on the right to free elections that could entail.

4.7.4 **Developments in profiling practices and human rights concerns**

4.7.5 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.

4.7.6 This is well documented in the US for example, where the Republican National Committee provides all Republican candidates with free access to a database that includes data on 200 million voters and includes over 7 trillion micro targeting data points. Political campaigners have moved towards knowing individuals' deepest secrets through gathering thousands of pieces of scattered information about them. Sensitive information, such as political beliefs, can be revealed from completely unrelated data using profiling. The fact that commercial data, public records, and all sorts of derived information, or Facebook likes, are used for political campaigning would come as a surprise to most people.

4.7.7 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.[3] 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.[4]

4.7.8 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.

4.7.9 A fundamental reason why in a democracy (unlike in the recent party Congress voting in China) 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.

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

- Consistency with the DPA is not a justification for including a condition for processing in the Bill. The DPA is not a gold standard of data protection and many of its provisions have not received sufficient scrutiny regarding their impact on privacy, in the almost 20 years since the legislation was enacted.

[3] 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

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

- Paragraph 17 has not been copied explicitly from the DPA, 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.

- 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. Concerns with these practices (profiling) and their implications for the democratic political process, together with the lack of public scrutiny are set out above.

- The broad condition in paragraph 17, 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 permitted for reasons of public interest, provided that appropriate safeguards are in place." Neither the wording of the condition in paragraph 17 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 17, together with the threshold of 'substantial damage or substantial distress', go beyond processing that required for electoral activities in a democratic system.

- 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-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).

- The condition in paragraph 17(1) of Schedule 1 to the Bill, does not meet the requirements of Article 9(2) derogation of GDPR. The condition is not demonstrably in the substantial public interest and it is not proportionate. This condition would legitimise and give a legal basis to, the practices described above, involving the granular scrutiny of personal data that for the concerns set out above is not in the substantial public interest. 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.

4.7.11 For the reasons identified above, there are significant concerns as to the prejudice to the fundamental rights and interests of individuals (right to privacy, freedom of expression and free elections) caused by processing under this condition. No justification has been provided as to the legitimate aim pursued and on this basis the condition should be removed from the Bill.

4.7.12 Privacy International's position is that paragraph 17 should be removed from the Bill for the reasons set out above. However, on the basis that explanation and justification are provided by Government and political parties to demonstrate the legitimate aim that this condition pursues, then amendments must be made to seek to ensure that the scope of the condition is proportionate and adequate safeguards are established.

4.7.13 The details of such amendments are for Parliament to decide, however suggested amendments are:

- that the word 'revealing' is removed;

- that 'political activities' is exhaustively defined and limited in scope;

- that 'substantial' is removed from the threshold in paragraph 17(2) and processing under this condition (paragraph 17(1)) should be prohibited where it is likely to cause damage or distress;

- that at the point of informing data subjects of the processing in accordance with Articles 13 or 14 of GDPR, political parties clearly inform individuals of their right to opt-out (paragraph 17(3) and make this right easy to exercise.

4.8 Immigration exemption

4.8.1 The immigration exemption is new in the Bill and there was no direct equivalent under the Data Protection Act 1998. This is a broad and wide-ranging exemption which is open to abuse and interference with human rights. This exemption should be removed all together 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. 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.

4.9 Intelligence Service Processing

4.9.1 The UK Intelligence Services, must comply with the UK's human rights obligations and any interference by the UK with human rights, (the right to privacy, the right to freedom of expression etc.), must meet the requirements of in accordance with the law, necessary and proportionate. The wide conditions for processing and broad exemptions in the Bill set out below, do not meet these standards.

4.9.2 Schedule 9: Conditions for processing under Part 4

4.9.3 Schedule 9 to the Bill sets out the conditions for processing personal data that apply to the Intelligence Services.

4.9.4 **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.

4.9.5 **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 with their statutory remit.

4.9.6 Schedule 11: Exemptions under Part 4

4.9.7 Schedule 11 to the Bill sets out exemptions to the obligations of the Intelligence Services under Part 4 of the Bill.

4.9.8 **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.

4.9.9 **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 Data Protection Act 1998.

5 Automated decision-making

5.1 Profiling and other forms of decision-making without human intervention should be subject to very strict limitations. The Bill provides insufficient safeguards for automated decision making. We recommend the Bill to be amended to include further concrete safeguards and protect human rights.

5.2 With technological advancements automated processes looks set to play an increasing role in decision-making. Decision-making can have significant and lasting implications for an individual and their human rights. When a decision is automated, questions arise as to how to protect from inbuilt bias and discrimination, how to ensure that a decision meets the thresholds of necessary and proportionate and how to manage accountability. 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 otherwise have the potential to affect the enjoyment of human rights, including economic, social and cultural rights***."[5]

5.3 It is essential to the protection of human rights that automated decision-making is limited and that where it is permitted adequate safeguards, including a right to redress, are in place.

5.4 **Clause 13: Automated decision-making authorised by law**

5.5 Amendments are suggested 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.

[5] 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, para.2

5.6 **Automated decision-making and profiling**

5.6.1 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 with regards to automated decision-making.

5.6.2 The profiling of individuals can inform automated decision-making and therefore cannot be isolated from considerations around 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.

5.6.3 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.

5.6.4 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.

5.6.5 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.

5.6.6 The reliance on computational algorithms and machine learning (see Annex E for more details and examples), 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.

5.6.7 **When is automated decision-making harmful?**

5.6.8 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.

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

- 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[6] and used in automated decision-making.

- 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.

- 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] 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]

5.6.10 In this context, the Bill is an opportunity to ensure rights are protected and safeguards exists.

5.7 General Processing (Part 2)

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

5.8.1 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.

5.8.2 Proprietary software, such as the COMPAS risk assessment that was sanctioned by the Wisconsin Supreme Court in 2016[7], calculates a score predicting the likelihood of committing a future crime. Even if final decisions are made by a judge, the software's automated decisions can be decisive, especially if judges rely on them exclusively or haven't been warned about their risks, including that the software produced inaccurate, illegal, discriminatory or unfair decisions.

5.8.3 This is particularly concerning in the context of automation bias, i.e. the propensity for humans to favour suggestions from automated systems over contradictory information made without automation, even if correct.[8] As a result, decisions that are formally attributed to humans but are *de facto* determined by an automated data-processing operation should clearly fall within the applicability of the provision.

5.8.4 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. For Clause 13 in the Bill to be applicable, "solely" cannot exclude any form of human involvement.

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

---

[7] Citron, D., 2016, (Un)Fairness of Risk Scores in Criminal Sentencing. Forbes. Available from: https://www.forbes.com/sites/daniellecitron/2016/07/13/unfairness-of-risk-scores-in-criminal- sentencing/#6074794b4ad2. [Accessed 1st August 2017]

[8] See for instance Skitka, L.J., Mosier, K.L. and Burdick, M., 1999. Does automation bias decision-making?. International Journal of Human-Computer Studies, 51(5), pp.991-1006.

5.8.6 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."[9]

5.8.7 For the purposes of clarity of obligations imposed on controllers, it is important that this explanation is included in the Bill.

5.8.8 We note the suggestion of the ICO, issued in a Feedback request on profiling and automated decision-making, that an effect is already significant if it has "*some consequence that is more than trivial and potentially has an unfavourable outcome*".[10]

5.9 Strengthen safeguards regarding automated decision-making authorised by law

5.9.1 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.

5.9.2 This amendment to ensure a right to explanation is an automated-decision safeguard, in line with the Government's own Explanatory Notes (para 115)[11] and Recital 71 of the EU GDPR:

---

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

[10] Information Commissioner's Office, 2017. Feedback request – profiling and automated decision- making. ICO. Available from https://ico.org.uk/about-the-ico/consultations/feedback-request-profiling-and-automated-decision-making/

[11] 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.

"The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention.

Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her.

However, decision-making based on such processing, including profiling, should be allowed where expressly authorized by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent.

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****".*

5.9.3 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).) Such provisions are also essential in the case of automated decision-making authorised by law.

5.9.4 It has been suggested that subject access rights as per Article 15 (1) (h) of the GDPR are sufficient. This is not however the case, as that Article specifically refers to the right to have the information regarding automated-decision making, including profiling and the logic involved referred to in Article 22(1) and (4); **therefore Article 22 (b) which exempts automated decision-making authorised by Member State law is not included in this provision.** To ensure effective safeguards as suggested by Recital 71 of GDPR, the protection must be in Clause 13 itself, to provide for meaningful information about the logic involved as well as the significance and legal consequences of such processing.

5.9.5 Provision of meaningful information may be a step towards addressing concerns about the extent to which automated decisions rely on data that has been derived or predicted through profiling. Whilst not within the scope of the proposed amendment, guidance could require information to include:

- What data will be used as input;
- What categories of information data controllers intend to derive or predict;
- How regularly input data is updated;
- Whether the actions of others affect how data subjects are profiled;
- The presence of algorithms;
- What kinds of measures the data controller will take to address and eliminate bias, inaccuracies and discrimination. Since misidentification, misclassification and misjudgement are an inevitable risk associated to profiling, controllers should also notify the data subject about these risks and their right to access and rectification.

5.10 **Ensure full right to redress**

5.10.1 Automated decision making, including profiling, affects data subjects in a variety of ways. The potential harms caused by profiling have been confirmed by the United Nations Human Rights Council. 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.

5.10.2 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"*

5.10.3 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.

5.10.4 Further, guidelines should be provided on adequate forms of redress for irregularities that come to light as a result of the exercise of these rights, in particular with regards to "meaningful information" "logic of processing" and "envisaged consequences".

5.11 Law Enforcement (Part 3)

5.11.1 Automated decision-making authorized by law: safeguards

5.11.2 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, as a potential miscarriage of justice can scar an individual and impact his or her wellbeing for life. The Bill provides insufficient safeguards for automated decision- making authorised by law. We recommend that the Bill be amended to include further concrete safeguards.

5.11.3 Clause 47: Clarify the meaning of decision "based solely on automated processing"

5.11.4 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 general processing provisions, it is important that this explanation is included in the Bill. There is no rationale for omitting it in this section.

5.11.5 Clause 47: Ensure automated-decision making does not apply to a decision affecting individual's human rights.

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

5.11.7 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.[12]

5.11.8 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.

[12] 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

5.11.9 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.

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

5.11.11 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.

5.12 Intelligence services (Part 4)

5.12.1 **Clause 94: Ensure automated-decision making does not apply to decisions affecting individual's human rights.**

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

5.12.3 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.

5.12.4 **Clause 94: Clarify the meaning of decision "based solely on automated processing"**

5.12.5 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.

5.12.6 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.

6 National Security Certificates

6.1 These provisions are contained in Part 2 (clauses 24, 25, 26), Part 3 (clause 77) and Part 4 (108, 109) of the Bill.

6.2 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. The technological advancements have rendered safeguards protecting the right to privacy obsolete. There has been a surge in legal discourse surrounding the necessary safeguards and oversight mechanisms with respect to both governmental and corporate entities. The General Data Protection Regulation and the Law Enforcement Directive and in turn the UK Data Protection Bill are one mechanism intended to redress the power imbalance between data controllers and data subjects.

6.3 However, in replicating and expanding the opaque and undemocratic national security regime, originally in section 28 of the Data Protection Act 1998, the processing of personal data outside the safeguards and oversight of the Data Protection Bill plainly amounts to a serious interference with Article 8 rights of privacy. This national security 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, transparency and oversight.

6.4 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."[13]

6.5 We note and have commented below on the replies of The Minister of State, Home Office (Baroness Williams of Trafford) to questions raised in committee stage with regard to national security certificates. No sufficient justification has been provided as to why basic safeguards should not be implemented.

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

6.6 In addition, the forceful resistance of the government is cause for concern. The highly secretive and opaque nature of this regime together with broad and unchecked exemptions to the data protection principles; the rights of data subjects; the responsibilities of data controllers and processors; and to safeguards for transfers of personal data to third countries and international organisations undermines public trust in effective data protection principles. Such sweeping powers may be unlawful under Article 8 ECHR and are unlikely to be acceptable to the European Union.

6.7 If the scope of certain principles and rights need to be limited for national security, this must be scrutinised by the Human Rights Committee to determine for each of Parts 2, 3 and 4 of the Bill which rights and principles it is permissible to exempt. However, we see no justification as to why this also requires an absence of safeguards.

6.8 The European Union demands the utmost respect for data protection, including within the context of national security. The European Parliament in their Report on the US NSA surveillance programme noted:

"5. … that several governments claim that these mass surveillance programmes are necessary to combat terrorism; strongly denounces terrorism, but strongly believes that the fight against terrorism can never be a justification for untargeted, secret, or even illegal mass surveillance programmes; takes the view that such programmes are incompatible with the principles of necessity and proportionality in a democratic society;

Recalls the EU's firm belief in the need to strike the right balance between security measures and the protection of civil liberties and fundamental rights, while ensuring the utmost respect for privacy and data protection; [14]

22. Calls on the EU Member States, and in particular those participating in the so-called '9- eyes' and '14-eyes' programmes', to comprehensively evaluate, and revise where necessary, their national legislation and practices governing the activities of the intelligence services so as to ensure that they are subject to parliamentary and judicial oversight and public scrutiny, that they respect the principles of legality, necessity, proportionality, due process, user notification and transparency, including by reference to the UN compilation of good practices and the recommendations of the Venice Commission, and that they are in line with the standards of the European Convention on Human Rights and comply with Member States' fundamental rights obligations, in particular as regards data protection, privacy, and the presumption of innocence."

[14] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, Main Findings, 2013/2188(INI) (21 February 2014)

6.9 In the Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, U.N. Doc. A/HRC/23/40 (17 April 2013) it was noted that:

"95. States should ensure that communications data collected by corporate actors in the provision of communications services meets the highest standards of data protection."

6.10 In *Digital Rights Ireland Ltd v. Minister of Communications, Marine and Natural Resources et al. (C-293/12); Kärntner Landesregierung and others (C-594/12), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (8 April 2014)* it was stated:

40. Nor is that retention of data such as to adversely affect the essence of the fundamental right to the protection of personal data enshrined in Article 8 of the Charter, because Article 7 of Directive 2006/24 provides, in relation to data protection and data security, that, without prejudice to the provisions adopted pursuant to Directives 95/46 and 2002/58, certain principles of data protection and data security must be respected by providers of publicly available electronic communications services or of public communications networks. According to those principles, Member States are to ensure that appropriate technical and organisational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data...

54. Consequently, the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data.

55. The need for such safeguards is all the greater where, as laid down in Directive 2006/24, personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data.

6.11 In considering the human rights implications of national security certificates we have set out below:

A. Questions as to who can benefit from a national security certificate

B. Why these provisions are lacking in clarity, accessibility and foreseeability which creates a risk of arbitrariness

C. Lack of adequate safeguards and our proposed safeguards.

D. Lack of effective oversight.

E. Lack of effective redress.

6.12 Within each of these we have discussed where relevant the statements of the Minister of State and our response.

6.13 By far the most relevant right engaged by the Bill is the right to respect for private life, family life, home and correspondence in Article 8 ECHR. The right to privacy is also protected by Article 17 of the International Covenant on Civil and Political Rights and Article 7 of the EU Charter of Fundamental Rights (which applies within the field of application of EU law, including data protection).

6.14 Any interferences with the right to respect for privacy must satisfy three requirements: they must be (1) in accordance with the law (which requires not only a clear legal basis but also sufficient specificity in the definition of the powers to provide effective guarantees against the risk of arbitrariness); (2) necessary in pursuit of a legitimate aim and (3) proportionate. The adequacy of safeguards against possible abuse is also relevant to any assessment of the proportionality of any interference with privacy.

6.15 The EU Charter of Fundamental Rights also contains a distinct right to the protection of personal data (Article 8 EUCFR).

6.16 **A. Who can benefit from a national security certificate?**

6.17 In order to assess the human rights implications of national security certificates, it is necessary to understand to whom they apply.

6.18 National Security Certificates can be found in Parts 2, 3 and 4 of the Bill. This underlines the fact that this regime does not only apply to the intelligence agencies and law enforcement.

6.19 Clauses 24, 25 and 26 of the draft Bill do not apply to law enforcement or intelligence agency processing of data. This begs the obvious question, which companies benefit from the national security certificates regimes and do not have to comply with the data protection act safeguards?

6.20 Baroness Hamwee questioned:

"What processing is outside the scope of EU law, and so would fall within Part 2 and not within Parts 3 and 4, the parts of the Bill on law enforcement and the intelligence services?"[15]

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

6.21 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 General Data Protection Regulations ("GDPR"). However, once we leave the European Union, the 'applied GDPR' will 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.

6.22 Not knowing to whom these provisions (clauses 24, 25, 26) may apply nor having available those certificates currently in existence, makes it impossible to evaluate the necessity, proportionality and risk posed by these provisions. In turn, as the Committee evaluates these proposals, it undermines the ability to effectively debate whether organisations, which are not law enforcement or intelligence agencies should, as a matter of principle, be able to exempt fundamental data protection safeguards.

6.23 We have raised in our amendments to Clauses 24, 25 and 26 whether it is acceptable to ever allow entities who are neither law enforcement nor intelligence services to exempt data protection safeguards. In order to make clear and apparent to the Committee the full breadth as to what Clause 24 exempts we have set this out in Annex B. We note that this includes:

- 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

6.24 As noted by Baroness Hamwee at committee stage:

6.25 *"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."*[16]

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

6.26 *"Clause 77(5) gives individual the right to appeal against a national security certificate, but individuals will not know that they have been subject to such a national security certificate if the certificate itself takes away the specific rights which would require a controller or a processor to inform individuals that there was such a restriction in effect against them. The whole point of a right to access personal information and, on the basis of that, the right to appeal against a restriction, does not seem to us to work. The amendment provides for informing the data subject that he is a subject to a certificate."*[17]

6.27 If it is considered that there should be permitted certain exemptions from data protection provisions in the Bill, these should be restricted only to what is necessary and proportionate. In line with this we have proposed the deletion of Clause 24 and modification of Clause 25 with respect to seeking exemptions from aspects of the Bill for national security purposes.

6.28 We note that The Minister of State, Home Office (Baroness Williams of Trafford) in Committee stage stated:

"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."

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

6.30 In relation to Part 2 The Minister of State, Home Office (Baroness Williams of Trafford) further commented at Committee stage that:

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

"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."

6.31 We are confused why in relation to Part 2, which is general processing not law enforcement or intelligence services processing, The Minister of State gives an example where an individual is subject of a covert investigation. 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.

6.32 We submit that for each of Parts 2, 3 and 4 the government must provide justifications for each of the exemptions they seek. The Government clearly should rely on separate justifications as they apply to general processing, law enforcement and intelligence services processing. Parliament cannot and should not approve such broad exemptions without specific justification. In addition, we do not see why this abrogates a need for safeguards and specification.

6.33 **B. Lacking in clarity, accessibility and foreseeability**

6.34 The regime providing for national security certificates operates on a legal basis that lacks in clarity, precision and comprehension. We note this in respect of the defence purposes exemption; lack of parliamentary scrutiny to date; retrospective and prospective nature of certificates; and the expansion in Part 3 beyond national security reasons.

6.35 Any interference with Article 8 must be *"in accordance with the law"* (see Article 8(2) ECHR). This requires more than merely that the interference be lawful as a matter of English law: it must also be *"compatible with the rules of law": Gillan v United Kingdom (2010) 50 EHRR 45 at §76.* There must be *"a measure of legal protection against arbitrary interferences by public authorities",* and public rules must indicate *"with sufficient clarity"* the scope of any discretion conferred and the manner of its exercise: *Gillan* at §77.

6.36 U.N. Human Rights, General Comment No. 16: Article 17 (Right to Privacy), U.N. Doc. HRI/GEN/1/Rev.1 at 21 (8 April 1988)

"10. The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law."

6.37 U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/69/166 (18 December 2014)

"Noting in particular that surveillance of digital communications must be consistent with international human rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and non- discriminatory and that any interference with the right to privacy must not be arbitrary or unlawful, bearing in mind what is reasonable to the pursuance of legitimate aims, and recalling that States that are parties to the International Covenant on Civil and Political Rights must undertake the necessary steps to adopt laws or other measures as may be necessary to give effect to the rights recognized in the Covenant."

6.38 Concluding observations on the fifth periodic report of France, Human Rights Committee, U.N. Doc. CCPR/C/FRA/CO/5 (17 August 2015):

"12. ...Specifically, measures should be taken to guarantee that any interference in persons' private lives should be in conformity with the principles of legality, proportionality and necessity. The State party should ensure that the collection and use of data on communications take place on the basis of specific and legitimate objectives and that the exact circumstances in which such interference may be authorized and the categories of persons likely to be placed under surveillance are set out in detail."

6.39 *Taylor-Sabori v. The United Kingdom, App. No. 47114/99, European Court of Human Rights, Judgment (22 October 2002)*

"18. The Court notes that it is not disputed that the surveillance carried out by the police in the present case amounted to an interference with the applicant's rights under Article 8 § 1 of the Convention. It recalls that the phrase "in accordance with the law" not only requires compliance with domestic law but also relates to the quality of that law, requiring it to be compatible with the rule of law.

6.40 *Malone v. The United Kingdom*, App. No. 8691/79, European Court of Human Rights, Judgment (2 August 1984)

"70. The issue to be determined is therefore whether, under domestic law, the essential elements of the power to intercept communications were laid down with reasonable precision in accessible legal rules that sufficiently indicated the scope and manner of exercise of the discretion conferred on the relevant authorities...

79. ...in its present state the law in England and Wales governing interception of communications for police purposes is somewhat obscure and open to differing interpretations... on the evidence before the Court, it cannot be said with any reasonable certainty what elements of the powers to intercept are incorporated in legal rules and what elements remain within the discretion of the executive. In view of the attendant obscurity and uncertainty as to the state of the law in this essential respect, the Court cannot but reach a similar conclusion to that of the Commission. In the opinion of the Court, the law of England and Wales does not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities. To that extent, the minimum degree of legal protection to which citizens are entitled under the rule of law in a democratic society is lacking."

6.41 Part 2, Chapter 3, of the Bill introduces a new **defence purposes exemption.** This is an expansion of the Data Protection Act 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.'

6.42 Baroness Hamwee asked the Government in committee stage:

"What are "defence purposes"? That phrase does not feature in the interpretation clause of the Bill. The Explanatory Notes, in referring to the 1998 Act, refer to the section about national security. Is defence not a national security matter? [18]

6.43 In response, The Minister of State, Home Office (Baroness Williams of Trafford) stated:

"*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.*

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

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."

6.44 Whilst the Minister states that the term 'combat effectiveness' is no longer adequate, we question why it is Schedule 11 of the Bill (exemptions to Part 4 of the Bill):

Schedule 11
7) The listed provisions do not apply to personal data to the extent that the application of the listed provisions would be likely to prejudice the combat effectiveness of any of the armed forces of the Crown.

6.45 We further note that in the Data Protection Act 1998, the exemptions for combat effectiveness are limited to subject information provisions:

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.

6.46 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)

6.47 The Bill therefore expands the exemptions applicable to combat effectiveness of the armed forces considerably (see Annex B). We are concerned at what appears to be 'mission creep' and an unjustified expansion of an exemption from fundamental data protection principles and safeguards, particularly given the lack of justification from the government.

6.48 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.

6.49 If the Minister of State is serious about ensuring that *"these provisions do not give carte blanche",* then there needs to be a limit on the exemptions upon which entities which fall under Part 2 can rely and justification for each of those exemptions that are sought to be included in Clause 24. This is in addition to the safeguards we propose for the actual application for a certificate.

6.50 There is a marked **absence of public Parliamentary or independent scrutiny** of national security certificates since the Data Protection Act 1998 came into force.

6.51 The only certificates we are aware that have been published result from litigation by Privacy International in relation to bulk personal datasets and bulk communications data. In addition in relation to Transport for London.

6.52 Lord Kennedy of Southwark stated in committee stage 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."*[19]

6.53 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."[20]

6.54 We note that the Minister of State, Home Office (Baroness Williams of Trafford) reported at committee stage that:

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

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

"I firmly believe that it is in the UK's national interest to recognise that there may sometimes be a conflict between the individual's right to have their personal data protected and the defence of the realm, and to make appropriate provision in the Bill to this end. 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****."*

6.55 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 certificates in existence and extant 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.

6.56 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 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.

6.57 The **timeless nature** of national security certificates means that they cannot be foreseen or predicted. The timeless nature of the Certificates is illustrated by Privacy International's ongoing litigation in relation to bulk personal datasets and bulk communications data where certificates signed in 2001 covered bulk surveillance activities that commenced five years later. The Minister questions what purpose would be served by a requirement that they be subject to time limitation, to name but a few reasons:

- Effective oversight;
- Sufficient safeguards to prevent the executive abusing its powers and undermining the ability of the legislature to hold it to account;
- Prevent against abuse;

6.58 National security certificates are both **retrospective and prospective.** The timeless nature has been addressed above. The retrospective nature of certificates is clearly troubling and it would be useful to understand how often this power has been used. With the upcoming deadline for GDPR, it should be expected that all entities, organisations and government departments, the police and intelligence agencies should be up to date and prioritising data protection. We can see no justification for maintaining the retrospective power to impose national security certificates. If there are examples or justifications, the government must clarify.

6.59 The provisions in Part 3, relating to law enforcement processing, go **beyond the scope of national security certificates.** Subsection (4) of Clause 77 attempts to broaden the basis upon which a certificate may relate beyond national security. Unless the provision is explicitly restricted to national security by referencing (4)(d) then national security is expanded to 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.

6.60 We propose the imperative amendment to reference 42(4)(d), 43(4)(d), 46(3)(d) and 66(7)(d).

6.61 **C. Lack adequate safeguards**

6.62 There is an issue of whether the legal framework in fact contains adequate safeguards. It is not sufficient for the Minister to state that the Data Protection Act 1998 has "stood the test of time" nor that it "works well". It is not sufficient that a power is capable of being exercised proportionately. What the national legislation must do is publicly to ensure that there are sufficient binding rules as to prevent arbitrary use of power and ensure that sufficient mandatory safeguards are in place to ensure that a power is exercised proportionately.

6.63 See the judgment of Lord Reed in *R (T) v Chief Constable of Greater Manchester* [2004] UKSC 35, [2014] 3 WLR 96 at §114:

"Determination of whether the collection and use by the state of personal data was necessary in a particular case involves an assessment of the relevancy and sufficiency of the reasons given by the national authorities. In making that assessment, in a context where the aim pursued is likely to be the protection of national security or public safety, or the prevention of disorder or crime, the court allows a margin of appreciation to the national authorities, recognising that they are often in the best position to determine the necessity for the interference. As i have explained, the court's focus tends to be on whether there were adequate safeguards against abuse, since the existence of such safeguards should ensure that the national authorities have addressed the issue of the necessity for the interference in a manner which is capable of satisfying the requirements of the Convention. In other words, in order for the interference to be "in accordance with the law", there must be safeguards which have the effect of enabling the proportionality of the interference to be adequately examined. Whether the interference in a given case was in fact proportionate is a separate question."

6.64 The case law of the European Court of Human Rights is clear that the minimum safeguards should be set out in law in order to avoid abuses of power.

6.65 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. It is clear on the face of this provision found in in Clause 25(1), 77(1), 109(1) (Parts 2, 3 and 4) is deficient. Basic safeguards are required.

6.66 This was raised by Baroness Hamwee at committee stage who 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."[21]

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

6.67 We note that the government are wholly resistant to any form of safeguards and oversight. We have noted our concerns that this will impact on an adequacy decision and we recommend the Committee consider whether a proportionate and necessary provision for safeguards and oversight is not more desirable than and a negative decision on adequacy. We rely on what we have said with respect to the Data Protection Act 1998 not being a gold standard. We are concerned at the forceful resistance by the government to oversight which they believe is:

"Wholly unnecessary, unjustified and disproportionate departure from a scheme which has been relied on under the Data Protection Act 1998 for many years and which works well."

6.68 With respect, the opacity of the regime means that there is a distinct paucity of evidence that it is working well. Further, 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. In our submission, section 28 of the Data Protection Act 1998 does not work well and it is time for it to be amended in line with our regimes relating to national security which contain basic safeguards against abuse.

6.69 Finally, the Minister makes no acknowledgment of the dynamically different times we live in with respect to data processing. We have referred to this above. To rely on a scheme that is outdated is to rely on a scheme not fit for the digital age.

6.70 U.N. Human Rights Council Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/HRC/28/L.27 (24 March 2015)

"Recognizing the need to further discuss and analyse, on the basis of international human rights law, issues relating to the promotion and protection of the right to privacy in the digital age, procedural safeguards, effective domestic oversight and remedies, the impact of surveillance on the right to privacy and other human rights, as well as the need to examine the principles of non-arbitrariness and lawfulness, and the relevance of necessity and proportionality assessments in relation to surveillance practices...

Noting that the rapid pace of technological development enables individuals all over the world to use new information and communications technology and at the same time enhances the capacity of governments, companies and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights, in particular the right to privacy, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, and its therefore an issue of increasing concern."

6.71 We suggest that the approach of the Minister to basic safeguards is irresponsible, not solely in relation to data subject rights but in respect to an adequacy decision. We believe that it leaves the scheme wide open to a challenge not just on adequacy but further on the basis of lawfulness.

6.72 The Minister complains that the amendments will create inconsistency. We have proposed safeguards to apply to Parts 2, 3 and 4. The Bill itself differs for each Part with respect to the provisions exempted.

6.73 The Minister states that:

"It is important to recognise that these certificates are already subject to judicial oversight, given that they may be appealed to the Upper Tribunal."

6.74 With respect, it is difficult to see how on any basis this can be viewed as effective judicial oversight and certainly we submit would not be accepted as adequate in accordance with Article 8 ECHR. It is dependent upon an individual bringing litigation (note our comments on redress), and the judge will not be considering the necessity and proportionality of the certificate per se. Instead the judge will be considering it in the context of the litigation. Further, it is post-facto oversight at the very best and is not comprehensive of all certificates.

6.75 The Minister refers to the current safeguards.

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

6.76 We are at a loss as to what these are, aside from very broad powers for Ministers to make certificates which, lack any standards of process or form, where there is no oversight, and certificates are timeless, prospective and retrospective. We have not been provided with any detail as to internal safeguards which we maintain would not be sufficient in any event, which are applicable to:

- Companies and organisations;
- Armed forces;
- Law enforcement;
- Intelligence agencies.

6.77 We see no reason not to improve the current regime and the argument that it would create inconsistency or may be difficulty could equally have applied in relation to changes that were introduced by the Investigatory Powers Act 2016. 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.

6.78 In relation to timing we note the Minister states:

"Amendment 148D would provide that the national security exemption provided for in Clause 108, which allows exemption from specified provision in Part 4 of the Bill, can be relied on only if a Minister of the Crown has signed a certificate under Clause 109. A certificate signed by a Minister certifies that the need for reliance on an exemption is conclusive evidence of that fact. It is not a prerequisite for the reliance on an exemption; to make it so would be operationally damaging. It would introduce delays that would be likely to significantly hamper, if not wholly frustrate, proper processing. Clearly, if processing was dependent on the issuing of a ministerial certificate, it could not proceed without one—by which time a threat that could have been identified by the processing may have crystallised into actual damage to national security."

6.79 If we are to understand the statement correctly, the Minister is stating that a certificate does not even need to be signed by the Minister. We find this shocking. Further we believe that arguments in relation to operational efficiency and urgent procedures were discussed at length during the course of the Investigatory Powers Act. If there are provisions for obtaining warrants in relation to powers exercised under the Investigatory Powers Act, including in urgent situations, which can be subject to oversight and safeguards, we fail to see how the Minister can maintain the above position with respect to national security certificates.

6.80 In relation to Parts 2, 3 and 4 we have proposed consistent safeguards as follows:

6.80.1 **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."

6.80.2 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'.

6.80.3 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****. 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."*

I hope that this has given the Committee a flavour of why the national security exemption has been framed in the way that it has. As I have indicated, the Bill's provisions clearly derive from a similar provision in the existing Data Protection Act and are subject to the same important qualification: namely, that an exemption may be applied in a given case only where it is required for the purpose of safeguarding national security.

6.80.4 In light of this, we do not see why there should be any objection firstly to the proposal that an application for a certificate to identify the personal data to which it applies and secondly to identify the provisions it seeks to exempt.

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

6.80.6 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.

6.80.7 The decision to issue the certificate **must be approved** by the Judicial Commissioner;

6.80.8 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.

6.80.9 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. There should be a clear limit on the duration of certificates. Interception warrants under s8(4) of the Regulation of Investigatory Powers Act 2000 (RIPA), should be limited to the relevant period, by virtue of s9(1)(a) and 9(6)(ab) of RIPA a standard warrant endorsed under the hand of the Secretary of State on national security grounds lasts for 6 months. Although not directly analogous, this period should be replicated for national security certificates under the Bill without the ability to have rolling warrants that in practice continue indefinitely, a defect of the RIPA regime.

6.81 The Minister of State, Home Office (Baroness Williams of Trafford) states that

"She also asked about the timelessness of these certificates. They 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."

6.82 We disagree. For the same reason that warrants are time limited, this allows for effective safeguards and oversight. Timeless certificates allow for abuse. 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.

6.83 If we consider that national security certificates can be relied upon <u>not only</u> 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.

6.84 We further question how reliable the statement by the Minister can be, that this is not a carte blanche, and that rights and obligations are considered on a case-by-case basis, if there is no requirement for certificates to be on a case-by-case basis nor for them to be renewed. This in effect means that there is no oversight whatsoever. All that is required is an extremely broad certificate, as we have seen for the intelligence agencies, to cover all their statutory powers. We have seen no evidence of the case-by-case consideration. As we have stated above, internal procedures within a company, law enforcement or agency are not effective oversight.

6.85 We note that Clause 26 removes the requirement for **'security of processing'**. There is no justification for exempting Article 32 GDPR (security of processing) and we suggesting removing Clause 26(2) and (3) and modifying Clause 26(4) to refer to additional provisions to Article 32.

6.86 The Minister for State commented at committee stage that it was **necessary to allow the intelligence agencies to unlawfully obtain personal data**.

"In relation to the offence of unlawfully obtaining personal data, much intelligence work involves obtaining and then disclosing personal data without the consent of the controller. For example, if GCHQ intercepts personal data held on a foreign terrorist group's computer, the data controller is the terrorist group. Without the national security exemption, the operation, although authorised by law, would be unlawful as the data controller has not consented. Similarly, reidentification of de-identified personal data may be a valuable source of intelligence if it can be reidentified. For example, an intelligence service may obtain from a computer a copy of a list of members of a terrorist group who are identified using code names, and from other sources the service believes that it can tie the code names to real identities."

6.87 We do not accept that the right way to resolve the apparent issues is to exempt the data protection safeguards. Consent is not the only process/ condition by which data processing is lawful. The Bill includes provisions/ conditions such as public interest, under which this could fall under. We submit, with all due respect, the reference merely to consent is a red herring.

6.88 The Information Commissioner's Office has published a number of blogs explaining GDPR and busting some of the myths of GDPR. One such myth is that you must have consent if you want to process personal data.

"The rules around consent only apply if you are relying on consent as your basis to process personal data.

So let's be clear. Consent is one way to comply with the GDPR, but it's not the only way

Headlines about consent often lack context or understanding about all the different lawful bases businesses and organisations will have for processing personal information under the GDPR.

Not only has this created confusion, it's left no room to discuss the other lawful bases organisations can consider using under the new legislation.

For processing to be lawful under the GDPR, you need to identify a lawful basis before you start."[22]

6.89 **D. Lack of effective oversight**

6.90 There currently exists no oversight in respect of national security certificates. There has never been any review or critique by Parliament or any other statutory body.

6.91 Clause 108(2)(c) - (e) of the Bill removes the oversight function of the Information Commissioner. Rather than remove the oversight role, provided for in Chapter 4, section 106, Part 5, Schedule 13 and Part 6, this oversight role should instead be 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. We have proposed a new clause to this effect.

6.92 We note the Minister of State referred to this at the committee stage stating:

It may assist the Committee if I provide a couple of examples, first in the context of Part 4, of why the exemption needs to be drawn as widely as it is. Clause 108 includes an exemption from Clauses 137 to 147 relating to information, assessment and enforcement notices issued by the Information Commissioner. 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."***

[22] https://iconewsblog.org.uk/2017/08/16/consent-is-not-the-silver-bullet-for-gdpr-compliance/

To take another example which touches on Amendment 124D, it is wholly appropriate to be able to limit the obligation on controllers under article 33 of the applied GDPR to disclose information to the Information Commissioner where the disclosure would be damaging to national security because, say, it would reveal the identity of a covert human intelligence source. As is the case under Part 4, this exemption would be applied so as to restrict the information provided to the commissioner, not to remove entirely the obligation to report appropriate details of the breach.

6.93 We submit that our amendment, to provide for oversight by the IPCO, will address concerns about extreme sensitivity or secure protection, given their role.

6.94 We support the statement of Baroness Hamwee that appeal rights are not a sufficient substitute for effective oversight:

"Finally, I do not think that the right of appeal provides the same protection as applying oversight from the very start of the process. We have had that debate many times, but I shall leave it there for now. There is quite a lot to read, so I am grateful to the Minister for replying at such length."

6.95 *Maximillian Schrems v. Data Protection Commissioner* (C-362/14), Court of Justice of the European Union, Grand Chamber, Judgment (6 October 2015)

"39. It is apparent from Article 1 of Directive 95/46 and recitals 2 and 10 in its preamble that that directive seeks to ensure not only effective and complete protection of the fundamental rights and freedoms of natural persons, in particular the fundamental right to respect for private life with regard to the processing of personal data, but also a high level of protection of those fundamental rights and freedoms…

40. As regards the powers available to the national supervisory authorities in respect of transfers of personal data to third countries, it should be noted that Article 28(1) of Directive 95/46 requires Member States to set up one or more public authorities responsible for monitoring, with complete independence, compliance with EU rules on the protection of individuals with regard to the processing of such data. In addition, that requirement derives from the primary law of the European Union, in particular Article 8(3) of the Charter and Article 16(2) TFEU.

41. The guarantee of the independence of national supervisory authorities is intended to ensure the effectiveness and reliability of the monitoring of compliance with the provisions concerning protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim. It was established in order to strengthen the protection of individuals and bodies affected by the decisions of those authorities. The establishment in Member States of independent supervisory authorities is therefore, as stated in recital 62 in the preamble to Directive 95/46, an essential component of the protection of individuals with regard to the processing of personal data.

42. In order to guarantee that protection, the national supervisory authorities must, in particular, ensure a fair balance between, on the one hand, observance of the fundamental right to privacy and, on the other hand, the interests requiring free movement of personal data.

43. The national supervisory authorities have a wide range of powers for that purpose. Those powers, listed on a non-exhaustive basis in Article 28(3) of Directive 95/46, constitute necessary means to perform their duties, as stated in recital 63 in the preamble to the directive. Thus, those authorities possess, in particular, investigative powers, such as the power to collect all the information necessary for the performance of their supervisory duties, effective powers of intervention, such as that of imposing a temporary or definitive ban on processing of data, and the power to engage in legal proceedings."

6.96 U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/69/166 (18 December 2014)

"4. Calls upon all States... (d) To establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data..."

6.97 European Commission For Democracy Through Law (Venice Commission), Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies, Study No. 719/2013 CDL- AD(2015)006 (7 April 2015)

"22. Parliamentary accountability. There are a number of reasons why parliamentary supervision of strategic surveillance is problematic. First, the technical sophistication of signals intelligence makes it difficult for parliamentarians to supervise without the aid of technical experts. Second, the general problem of parliamentarians finding sufficient time for oversight along with all their other duties is particularly acute as regards strategic surveillance, where for controlling the dynamic process of refining the selectors (as opposed to a post-hoc scrutiny), some form of standing body is necessary. Thirdly, the high degree of network cooperation between certain signals intelligence agencies means an added reluctance to admit in parliamentary oversight, which can thus affect not simply one's own agencies, but also those of one's allies. In some states the doctrine of parliamentary privilege means that parliamentary committees cannot be security-screened, adding to an already-existing fear of leaks. The other, crucial, factor is that strategic surveillance involves an interference with individual rights. Supervision of such measures has traditionally been a matter for the judiciary. The constitutional principle of separation of powers can make it problematic for a parliamentary body to play such a quasi-judicial role.

23. A decision to use particular selectors, resembles, at least in some ways, a decision to authorize targeted surveillance. As such, it can be taken by a judicial body. As the decision involves considerable policy elements, knowledge of intelligence techniques and foreign policy are also desirable. Finding a group of people who combine all three types of competence is not easy, even for a large state. Thus, it is easier to create a hybrid body of judges and other experts. As regards follow-up (oversight) it is necessary to oversee decisions made by automated systems for deleting irrelevant data, as well as decisions by human analysts to keep the personal information collected, and to transfer it to other domestic and foreign agencies. This type of oversight is of a "data protection" character, most suitably assigned to an independent, expert administrative body. Neither of these types of decision is "political" in nature. What, by contrast, is more "political" is the prior decision taken, that somebody, or something, is of sufficient importance to national security to need intelligence about. This is the type of decision which would benefit from a (closed) discussion in a political body, where different spectrums of opinion are represented. Another type of policy-oriented issue is deciding the general rules regarding who, and under what circumstances, signals intelligence can be exchanged with other signals intelligence organisations. A third is making a general evaluation of the overall effectiveness and efficacy of signals intelligence measures. A fourth role for a political body is to engage in a continuous dialogue with whatever expert oversight body is established.

24. Judicial authorization. A system of authorization needs to be complemented by some form of follow-up control that conditions are being complied with. This is necessary both because the process of refining selectors is dynamic and highly technical and because judges do not tend to see the results of the signals intelligence operations as these seldom lead to prosecutions. Thus the safeguards applying to a subsequent criminal trial do not become applicable."

6.98 **F. Effective redress**

6.99 In our proposed amendments the right to challenge a certificate has been modified to include those who believe they are directly or indirectly affected. Given the highly secretive nature of certificates it is logical to include these amendments.

6.100 Clause 108(3) of the Bill must be amended to allow those who 'believe they are' affected by the issuing of a certificate to appeal to the Tribunal against the certificate.

6.101 **Conclusion**

6.102 For the reasons we have set out, there is clear engagement with Article 8 ECHR and the may further be engagement with Article 6 ECHR given the nature of this regime.

6.103 We note specifically in relation to Part 4, intelligence services processing that the certificates disclosed in the course of Privacy International's litigation exempt the agencies from performance of their functions. This raises the question as to the purpose of Part 4 in reality, if the practice is to exempt all data protection safeguards. If the agencies have a blanket exemption, how is this justified. The evidence to date supports our view that little if any of the processing carried out by the Intelligence Services would fall within Part 4, and we welcome discussion in this respect.

6.104 We have suggested for each of the rights and safeguards each of Parts 2, 3 and 4 separately seek to exempt, their must by scrutiny and the government must provide detailed justification in order to see these on the statute book.

6.105 This is a key and opportune moment for the Committee to scrutinise national security certificate regime and report upon the fundamental safeguards that are required to protect human rights.

7 Intelligence agencies, cross border transfers.

7.1 The transfer of data must be subject to adequate safeguards. In relation to general processing these are set out in Chapter V of GDPR. Safeguards should also be in place for intelligence services and criteria have been articulated by the European Court of Human Rights in the case of *Weber & Saravia v. Germany.* Any interference with Article 8 must be *"in accordance with the law"* (see Article 8(2)). This requires more than merely that the interference be lawful as a matter of English law: it must also be *"compatible with the rule of law"*: Gillan v United Kingdom (2010) 50 EHRR 45 at §76. There must be *"a measure of legal protection against arbitrary interferences by public authorities"* and public rules must indicate *"with sufficient clarity"* the scope of any discretion conferred and the manner of its exercise: *Gillan* at §77.

7.2 In Weber & Saravia v Germany (2008) 46 EHRR SE5, the ECtHR held at §§93-94:

"The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures … Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the execution or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference."

7.3 In *Weber* the Court at §95 referred to the minimum safeguards in order to avoid abuses of power, including the need for safeguards on sharing:

"In its case law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: … the precautions to be taken when communicating the data to other parties."

7.4 The Bill provides for almost unfettered powers for cross-border transfers of personal data by intelligence agencies without appropriate levels of protection; we recommend that rules for such transfers are brought into line with those required in the Bill for law enforcement purposes.

7.5 We propose at Clause 107 that it is specified that transfer is "provided by law".

7.6 The interference with privacy posed by intelligence sharing is equivalent to that posed by direct state surveillance.

7.7 Domestic legislation governing intelligence sharing is inadequate. We note in respect of bulk data, there are no restrains in primary legislation on the sharing of bulk data:

7.7.1 Section 19 of the Counter Terrorism Act 2008 permits sharing and onward disclosure and the use of material obtained for one purpose for another. Sharing of information pursuant to section 19 of the 208 Act does not require any warrant or other external authorisation, regardless of the private or sensitive nature of the information. There is no requirement for oversight of a decision to share information under section 19.

7.7.2 For intercept material, the basic safeguards in section 15(2) and (3) of RIPA limiting the number of persons to whom the material is disclosed, the extent of copying and arrangements for destruction may be disapplied by the Secretary of State. The Secretary of State may decide to retain such requirements *"to such extent (if any) as the Secretary of State thinks fit" (section 15(7)(a) RIPA).*

7.7.3 In relation to bulk communications data, nothing in section 94 Telecommunications Act 1984 imposes any restriction on sharing.

7.8 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.

7.9 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."

7.10 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*."

7.11 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.

7.12 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.

7.13 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 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.

7.14 The UK legal regime on intelligence sharing lacks the required minimum safeguards. The provision in this Bill fails to bring it to conformity with standards complying with human rights law.

7.15 The proposed amendments bring the transfer of personal data to third parties under Part IV in line with provisions under Part III (Law Enforcement.) There is no rationale to justify transfers by intelligence agencies having lower safeguards than those applicable to law enforcement's transfers.

8 Data Retention

8.1 We note that it has been raised in amendments that:

> *"Amendment 137EA in the name of the noble Lord, Lord Kennedy, and articulated by the noble Lord, Lord Stevenson, seeks to set in statute the retention period for personal data derived from ANPR cameras. ANPR is an important tool used by the police and others for the prevention and detection of crime. I understand that the National Police Chiefs' Council has recently changed its policy on the retention of ANPR records, reducing the retention period from two years to 12 months. The new policy requires all data not related to a specific case to be deleted after 12 months. This will be reflected in revised national ANPR standards. We know that the Information Commissioner had concerns about the retention of ANPR records and we welcome the decision by the NPCC in this regard."*[23]

8.2 Whilst we are concerned about the retention policies of the police with respect to ANPR, this amendment fails to take into account the plethora of data current acquired, collected, retained and processed by the police.

8.3 We are further concerned that to try and include retention periods for only certain organisations in the Bill means that it would never be comprehensive and periods may be found in other previous or subsequent legislation. We suggest that it may be useful for the ICO to dedicate resources to collating statutory requirements. In relation to the police we suggest that specific consultation and legislation is required to address the scope and variety of retained data to ensure minimum retention and enforce deletion.

8.4 We are concerned however that the data protection principle to only keep data as long as necessary is not useful in respect of practical guidance for the police. We would suggest that the Committee recommend the ICO carries out an investigation into the types of data held by the police, and provides guidance on retention and deletion.

8.5 In relation to new technology used by the police we have previously highlighted the practice of mobile phone extraction and called for a warrant to be imposed for this practice. We have further set out the use of predictive policing to date based on FOIA requests. [24]

---

[23] https://www.theyworkforyou.com/lords/?id=2017-11-15a.2080.0

[24] 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

Annex A: Proposed draft amendments (in chronological order)

PART 2 - GENERAL PROCESSING

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

Page 5, line 6, remove "includes" and insert "refers to"

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

Page 6, line 1, leave out "varying or omitting conditions or"

Schedule 1: Paragraph 17 - remove condition for political parties

Page 118, line 10, remove paragraph 17

Clause 13: Automated decision-making authorised by law

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

Page 7, line 11, 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 26 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 39, 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 35, 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 125, line 40, leave out paragraph 4

Clause 24: national security and defence exemption

Page 14, line 35 to page 15, line 32, leave out clause 24

Clause 25: National security: certificate

Page 15, line 34, delete "Subject to subsection (3), a certificate signed by"

Page 15, line 35, 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 35, delete "certifying that exemption"

Page 15, line 35, insert after "from" the word "specified"

Page 15, line 35, delete the words "all or any of the"

Page 15, line 35 – 36 delete the words "listed in section 24(2) is, or at any time was, required"

Page 15, line 37, delete the words "conclusive evidence of that fact"

Page 15, line 37, insert new subsections:

(2) The decision to issue the certificate must be:

a. approved by a Judicial Commissioner,

b. Laid before Parliament,

c. 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 15, line 38, insert before "A certificate" the words "An application for"

Page 15, line 39, delete the word "may"

Page 15, line 39, insert before the word "identify", the word "Must"

Page 15, line 39, delete the word "general"

Page 15, line 39, insert after the words "means of a" the word "detailed"

Page 15, line 41, insert new subsections in clause 24(2) which states:

a. ...

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

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

d. ...

Page 15, line 41, delete the subsection (2(b)) which states "may be expressed as having prospective effect."

Page 15, after line 41, 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>

a. Chapter II of the applied GDPR (principles) –

i. Article 5 (lawful, fair and transparent processing)
ii. Article 6 (lawfulness of processing)
iii. Article 9 (processing of special categories of personal data)

b. 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. **Part 7 of this act, section 173 (representation of data subjects)**

Page 15, line 42, insert after the words "Any person" the words "who believes they are"

Page 15, line 42, insert after the word "directly" the words "or are indirectly"

Page 15, line 43, insert after the words "against the certificate" the word ", and"

Page 15, line 43, insert subjection which states "rely upon section 173 of this Act"

(1) Any person **who believes they are** directly **or are indirectly** affected by a certificate under subsection (1)
a. may appeal to the Tribunal against the certificate, and
b. rely upon section 173 of this Act.

Page 15, lines 44 – 45, delete the words "applying the principles applied by a court on an application for judicial review"

Page 15, line 45, insert after the words "judicial review" the words "it was not necessary or proportionate to issue"
Page 15, lines 45 – 46, delete the words "the Minister did not have reasonable grounds for issuing"

Page 16, lines 1 – 20, delete clauses (5), (6), (7), (8), (9).

Clause 26 National Security and defence

page 16, line 25, delete the words 'and defence'

page 16, line 30 - 31, delete the words 'or for defence purposes' page 16, 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 14, leave out paragraphs (6) and (7)

Or

Page 20, line 16:, 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 19, 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 19, after "by law" add the following: ",subject to subsection ()"

Page 28, line 19, 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 13, after Clause 48 insert the following new clause:

"( ) Right to information about decision-making
(1) Where—
(a) the controller processes personal data relating to a data subject, and
(b) 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 – Law enforcement processing

Page 44, line 36, insert after "A Minister of the Crown" the words "must apply to a Judicial Commissioner for a certificate".

Page 44, line 36, delete the words "may issue a certificate certifying"

Page 44, line 37, 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 37, 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:
(a) Approved by a Judicial Commissioner,
(b)Laid before Parliament,
(c) Published and publicly accessible on the Cabinet Office website.

Page 44, line 39 insert before the words "The certificate may" the words "An application for a"

Page 44, line 39, before the word "certificate" delete the word "The"

Page 44, line 39, after the word "certificate" delete the word "may"

Page 44, line 39, after the word "certificate" insert the word "must"

Page 44, line 40, delete the words "relate to a" and "which"

Page 44, line 40 insert before the word "relate" the words "a. Identify which"

Page 44, line 41, delete the words "has" and "imposed"

Page 44, line 41, after the words "a controller has" insert the words "seeks to"

Page 44, line 42, add in sub-subsection (d) to all references clauses to read: 42(4)**(d),** 43(4)**(d),** 46(3)**(d),** 66(7)**(d).**

Page 44, line 42, delete the word "or" and insert the word "and"

Page 45, line 1-2, delete the entire sub-clause which reads "(b) identify any restriction to which it relates by means of a general description."

Page 45, line 1, 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 2, 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:
(a) Whether the certificate is necessary on relevant grounds, and
(b) 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 3 to 6, delete entire clause 77(3)

Page 45, lines 7 to 8, delete entire clause 77(4)

Page 45, line 9, 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 9, insert after the words "Any person" the words "who believes they are"

Page 45, line 9, insert after the word "directly" the words "or are indirectly"

Page 45, line 10, before the word "may" insert "(a)" and after the word "certificate" insert the word ", and"

Page 45, line 10 after the words "against the certificate" insert "(b) rely upon section 173 of this Act."

Page 45, line 12, after the words "judicial review" insert the words "it was not necessary or proportionate to issue"

Page 45, lines 16 to 34, delete in their entirety, clauses (7), (8), (9), (10) and (11).

Page 45, lines 39 to 41, delete in its entirety, clause (13).

PART 4 - INTELLIGENCE SERVICES PROCESSING

Clause 84: Regulation making power re conditions for processing

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 171, line 37
Leave out subsection 5(e).

Remove legitimate interest condition from UKIS

Page 171, line 39
Leave out subsection (5)

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 26, 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 24, 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 - adding safeguards

Page 59, line 27, after "the transfer is" add "is provided by law and is".

Page 59, line 26, after (2) add ,(3), (4), (5) and section ().

Page 59, line 33, add new sub-clauses 107(3), (4), (5) and new section ():

(3) The transfer falls within this subsection if the transfer–
(a) is based on an adequacy decision (see section 72) (b) if not based on an adequacy decision, is based on there being appropriate safeguards (see section 73), or
(c) 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
(a) 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

(i) 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).

(ii) 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).

(iii) 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.

(iv) 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

(v) 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) –
(a) the seriousness of the circumstances leading to the request for authorisation,
(b) the purpose for which the personal data was originally transferred, and
(c) 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 Exemption – Intelligence services processing

Restricting the scope of the national security exemption

Page 60, line 3, after the words "(rights of data subjects)" add the words "except section 94(1)".

Page 60, line 4 to 15, delete all clauses 108(2)(c) to (e). Page 60, line 4 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 – Intelligence services processing

Making national security certificates more transparent and accountable

Page 60, line 17, delete 'Subject to sub-section (3) a certificate signed by a"

Page 60, line 17, insert after the words "certificate signed by" the word "A"

Page 60, line 18, before the word “certifying” insert the words “must apply to a judicial commissioner for a certificate, if exemptions are sought”

Page 60, line 18, delete the words “certifying that exemption”

Page 60, line 18, after the word “form” insert the word “specified”

Page 60, line 18, delete the words “all or any of the”

Page 60, line 19, delete the words “is, or at any time was required”

Page 60, line 20, delete the words “is conclusive evidence of that fact”.

Page 60, line 21, 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:
(a) Whether the certificate is necessary on relevant grounds, and
(b) Whether the conduct that would be authorised by the certificate is proportionate to what it sought to be achieved by that conduct, and
(c) Whether it is necessary and proportionate to exempt all provisions specified in the certificate.

Page 60, line 22, insert before the word “certificate” the words “An application for a”

Page 60, line 22, delete the words “under subsection (1)

Page 60, line 23 delete the word “may”

Page 60, line 23, insert at the start of the subsection the word “a. Must”

Page 60, line 23, delete the word “general”

Page 60, line 24, before the word “description” insert the word “detailed”

Page 60, line 25, delete the subsection which reads “b. may be expressed as having prospective effect”.

Page 60, line 25, 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 26, 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 27, 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 28 – 29 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 29 – 30 delete the words "the Minister did not have reasonable grounds for issuing"

Page 60, lines 34 to 44 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 173, line 34
Leave out paragraph 1

Page 175,
Leave out subsections (10), (12), (13), (14).

PART 5 - THE INFORMATION COMMISSIONER

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

Page 66, line 2, at end insert: "120A Public interest code

The Commissioner must prepare a code of practice which contains –

(a) Practical guidance in relation to the processing of personal data in the public interest
(b) Practical guidance in relation to the processing of personal data in the substantial public interest
(c) 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.

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

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

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

(5) 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 96, line 1, after Commissioner insert ", data subjects and persons who appear to the Commissioner to represent the interests of data subjects,"

Page 96, line 3, leave out paragraph (a)

Amendment Clause 173: Representation of data subjects

Adding rights from Article 80(2) of GDPR

Page 98, line 20, 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—

1. (a) Article 77(right to lodge a complaint with a supervisory body);
2. (b) Article 78 (right to an effective judicial remedy against a supervisory authority); and
3. (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 31, 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.”

Annex B: Clause 24: exemptions for national security and defence

A full list of what this clause exempts is set out below:

Chapter II of the applied GDPR (principles)
Article 5: lawfulness, fairness and transparency (except 5(1)(a))[25]
Article 6: Lawfulness of processing (exception 24(2)(a(ii))
Article 7: Conditions for consent
Article 8: Conditions applicable to child's consent in relation to information society services
Article 9: Processing of special categories of personal data (exception 24(2)(a)(iii))
Article 10: Processing of personal data relating to criminal convictions and offences
Article 11: Processing which does not require identification

Chapter III: Rights of the data subjects (24(2)(b))
Article 12: Transparent information, communication and modalities for the exercise of the rights of the data subject
Article 13: Information to be provided where personal data are collected from the data subject.

25

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Article 14: Information to be provided where personal data have not been obtained from the data subject.
Article 15: Right of access by the data subject
Article 16: Right to rectification
Article 17: Right to erasure
Article 18: Right to restriction on processing
Article 19: Notification obligation regarding rectification or erasure of personal data or restriction of processing.
Article 20: Right to data portability.
Article 21: Right to object
Article 22: Automated individual decision-making including profiling
Article 23: Restrictions

Chapter IV: Controller and Processor (24(2)(c)
Article 33: Notification of a personal data breach to the supervisory authority (24(2)(c)(i))
Article 34: Communication of a personal data breach to the data subject (24(2)(c)(ii))

Chapter V: Transfers of personal data to third countries or international organisations (24(2)(d)
Article 44: General principle for transfers
Article 45: Transfers on the basis of an adequacy decision

Article 46: Transfers subject to appropriate safeguards
Article 47: Binding corporate rules
Article 48: Transfers or disclosures not authorized by Union law
Article 49: Derogations for specific situations
Article 50: International cooperation for the protection of personal data

Chapter VI: Independent supervisory authorities
Article 57: Tasks (57(1)(a) and (h) (24(2)(e)) – Commissioner's duties to monitor and enforce the applied GDPR and to conduct investigations
Article 58: Powers (24(2)(ii)) – investigative, corrective, authorisation and advisory powers of Commissioner

Chapter VIII: Remedies, liability and penalties (24(2)(f))
Article 77: Right to lodge a complaint with a supervisory authority
Article 78: Right to an effective judicial remedy against a supervisory authority
Article 79: Right to an effective judicial remedy against a controller or processor
Article 80: Representation of data subjects.
Article 81: Suspension of proceedings
Article 82: Right to compensation and liability
Article 83: General conditions for imposing administrative fines (exception 24(2)(f)(i))
Article 84: Penalties (exception 24(2)(f)(ii))

Part 5 of the Data Protection Bill (The Information Commissioner)

Section 113 – general functions of the Commissioner
(3) The Commissioner's functions in relation to the processing of personal data to which the GDPR applies include—
(a) a duty to advise Parliament, the government and other institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data, and
(b) a power to issue, on the Commissioner's own initiative or on request, opinions to Parliament, the government or other institutions and bodies as well as to the public on any issue related to the protection of personal data.

(8) The following powers are exercisable only by giving an enforcement notice under section 142— (a) the Commissioner's powers under Article 58(2)(c) to (g) and (j) of the GDPR (certain corrective powers); (b) the Commissioner's powers under Article 58(2)(h) to order a certification body to withdraw, or not to issue, a certification under Articles 42 and 43 of the GDPR.

(9) The Commissioner's powers under Articles 58(2)(i) and 83 of the GDPR (administrative fines) are exercisable only by giving a penalty notice under section 148.

Section 117 – inspection in accordance with international obligations
(1) The Commissioner may inspect personal data where the inspection is necessary in order to discharge an international obligation of the United Kingdom, subject to the restriction in subsection (2).
(2) The power is exercisable only if the personal data—
is processed wholly or partly by automated means, or
is processed otherwise than by automated means and forms part of a filing system or is intended to form part of a filing system.

(3)The power under subsection (1) includes power to inspect, operate and test equipment which is used for the processing of personal data.
(4)Before exercising the power under subsection (1), the Commissioner must by written notice inform the controller and any processor that the Commissioner intends to do so.
(5) Subsection (4) does not apply if the Commissioner considers that the case is urgent.
(6) It is an offence—
intentionally to obstruct a person exercising the power under subsection (1), or
to fail without reasonable excuse to give a person exercising that power any assistance the person may reasonably require.

Part 6 of the Data Protection Bill (Enforcement)

Sections 137 – 147
137: Enforcement notices
138: Information notices: restrictions

139: Failure to comply with an information notice
140: Assessment notices
141: Assessment notices: restrictions
142: Enforcement notices
143: Enforcement notices: supplementary
144: Enforcement notices: rectification and erasure of personal data
145: Enforcement notices: restrictions
146: Enforcement notices: cancellation and variation
147: Powers of entry and inspection

Schedule 15 – Commissioner's notices and powers of entry and inspection Part 7

Section 173 – representation of data subjects

Annex C: Rights that are exempted by national security certificates for law enforcement.

42 Information: controller's general duties

(4) The controller may restrict, wholly or partly, the provision of information to the data subject under subjection (2) to the extent that and for so long as the restriction is, having regard to the fundamental rights and legitimate interests of the data subject, a necessary and proportionate measure 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;

Protect national security;

Protect the rights and freedoms of others

43 Rights of access by the data subject

(1) A data subject is entitled to obtain from the controller –

Confirmation as to whether or not personal data concerning him or her is being processed, and

Where that is the case, access to the personal data and the information set out in subsection (2).

(2) That information is –

a. The purposes of and legal basis for the processing;

b. The categories of personal data concerned;

c. The recipients or categories of recipients to whom the personal data has been disclosed (including recipients or categories of recipients in third countries or international organisations);

d. The period for which it is envisaged that the personal data will be stored or, where that is not possible, the criteria used to determine that period; e. The existence of the data subject's rights to request from the controller –

i. Rectification of personal data (see section 44), and

ii. Erasure of personal data or the restriction of its processing (see section 45);

f. The existence of the data subject's right to lodge a complaint with the Commissioner and the contact details of the Commissioner;

g. Communication of the personal data undergoing processing and of any available information as to its origin.

(3) Where a data subject makes a request under subsection (1), the information to which the data subject is entitled must be provided in writing ...

(4) Rights of the Data Subject

The controller may restrict, wholly or partly, the rights conferred by subsection (1) to the extent that and for so long as the restriction is, having regard to the fundamental

rights and legitimate interests of the data subject, a necessary and proportionate measures 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;
Protect national security;
Protect the rights and freedoms of others.

46(3) Rights under section 44 or 45: Supplementary

(3) The controller may restrict, wholly or part, the provision of information to the data subject under subsection (1)(b)(i) to the extent that and for so long as the restriction is, having regard to the fundamental rights and legitimate interests of the data subject, a necessary and proportionate measure 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;
Protect national security;
Protect the rights and freedoms of others;

66 Communication of a personal data breach to the data subject
(7) The controller may restrict, wholly or partly, the provision of information to the data subject under subsection (1) to the extent that and for so long as the restriction is, having regard to the fundamental rights and legitimate interests of the data subject, a necessary and proportionate measure 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;
Protect national security;
Protect the rights and freedoms of others;

Annex D: Rights that are exempted by national security certificates for intelligence services processing

Chapter 2: Data Protection Principles

- Section 84 sets out the first data protection principle (requirement that processing be lawful, fair and transparent);
- Section 85 sets out the second data protection principle (requirement that the purposes of processing be specified, explicit and legitimate);
- Section 86 sets out the third data protection principle (requirement that personal data be adequate, relevant and not excessive);
- Section 87 sets out the fourth data protection principle (requirement 40 that personal data be accurate and kept up to date);

Schedules 9 and 10;

Schedule 9: Conditions for processing under Part 4
Schedule 10: conditions for sensitive processing under Part 4

Chapter 3 (rights of data subjects);

- Right to information
- Right of access
- Right of access: supplementary
- Right not to be subject to automated decision-making
- Right to intervene in automated decision-making
- Right to information about decision-making
- Right to object to processing
- Right to rectification and erasure

Chapter 4, section 106 (communication of personal data breach to the Commissioner);

In Part 5 –

i. Section 117 (inspection in accordance with international obligations)
ii. Schedule 13 (other general functions of the Commissioner), paragraphs 1(a) and (g) and 2;

In Part 6

Sections 137 to 147 and Schedule 15 (Commissioner's notices and powers of entry and inspection);
Sections 161 to 163 (offences relating to personal data)
Sections 164 to 166 (provision relating to the special purposes)

Annex E - Further background on automated decision-making

Computational algorithms and machine learning

Computational algorithms are perhaps most appropriately defined as "*a series of well-defined step-by-step operations*" performed by a computer.[26] Such step-by-step operations can be used for processes and decision-making on a very large scale. An algorithm could be designed to turn very specific input variables, such as credit card transaction information, into output variables such as a flag for fraud. If the credit card transactions follow a specific pattern, the system could automatically classify the transaction as fraudulent.

Profiling (and automated decision-making) that is based on machine learning go further than specified computational algorithms. Rather than explicitly formalising a model as a single step-by-step algorithm, machine learning trains a model implicitly. Machine learning algorithms learn from and are trained on large amounts of data. In the case of financial transactions, for instance, the designer of a machine learning system would not specify a rule which defines what kinds of transaction patterns indicate a fraudulent account. Instead, machine learning systems learn often highly non-linear correlations from data which is fed into them for training purposes (training data), which is then formalised as a model that can be queried with input data.

Purposes and practical applications

Automated decision-making may occur in a range of contexts, from targeted advertising and healthcare screenings to policing, for a variety of purposes. Examples of combining profiling and decision-making to score, rate and assess people include:

- A hiring software analyses an applicant's voice in order to identify applicants with "*energy and personality*" and evaluates "*language proficiency, fluency, critical thinking, and active listening*".[27]

- In 2016, IBM launched a tool that would help governments separate "real asylum seekers" from potential terrorists by assigning each refugee a score that would assess their likelihood to be an imposter.[28]

[26] Michael Negnevitsky, Artificial Intelligence, A guide to intelligent systems, second edition, 2005

[27] http://www.hireiqinc.com/solutions [Accessed 1st August 2017]

[28] Tucker, P., 2016, Refugee or Terrorist? OBM Thinks Is Software Has the Answer. Defense One. http://www.defenseone.com/technology/2016/01/refugee-or-terrorist-ibm-thinks-its-software-has- answer/125484/ [Accessed 1st August 2017]

- Hiring software automatically scores and sorts resumes and ranks applicants. The hiring company only considers applicants that score above a certain threshold.[29]

- The NSA reportedly uses web browsing data to predict an internet user's likely nationality, which allows the agency to distinguish between foreign and domestic communications.[30]

- In 2013, the Chicago Police Department conducted a pilot of a predictive policing program designed to reduce gun violence. The program included development of a Strategic Subjects List (SSL) of people estimated to be at highest risk of gun violence. Research found that individuals on the SSL are not more or less likely to become a victim of a homicide or a shooting, but are more likely to be arrested for shooting.[31]

- A social networking site automatically flags some names as fake and suspends the respective accounts. As a result of this automated system, a disproportionate number of minorities' names are deleted.[32]

Automated decisions, informed by profiling, may also be made based on a person's individual environment. Real-time personalisation gears information towards an individual's presumed interests. Such automated decisions can even be based on someone's predicted vulnerability to persuasion or their inferred purchasing power.

(a) Social media platforms tailor their services to their users' presumed tastes and interests, including what kinds of content, including news, users see in their news feeds, and in which order.[33]

(b) Billboards on the Tokyo Expressway—on one of Japan's busy expressways— detect and identify cars to then select and display content based on the types of cars.[34]

(c) Another study examined 16 major e-commerce sites and found search discrimination, i.e. differences in the products shown to users based on their

[29] Rosenblat, A. and Kneese, T., 2014. Networked Employment Discrimination.
[30] Cheney-Lippold, J., 2011. A new algorithmic identity: Soft biopolitics and the modulation of control. Theory, Culture & Society, 28(6), pp.164-181.
[31] Saunders, J., Hunt, P. and Hollywood, J.S., 2016. Predictions put into practice: a quasi-experimental evaluation of Chicago's predictive policing pilot. Journal of Experimental Criminology, 12(3), pp.347-371
[32] Kayyali, D., 2015, Facebook's Name Policy Strikes Again, This Time at Native Americans. EFF. https://www.eff.org/deeplinks/2015/02/facebooks-name-policy-strikes-again-time-native-americans
[33] Holm, N., 2016. Advertising and Consumer Society: A Critical Introduction. Palgrave Macmillan.
[34]https://builders.intel.com/docs/storagebuilders/deep_learning_enables_intelligent_billboard_for_dyna mic_targeted_advertising_on_tokyo_expressway.pdf [Accessed 1st August 2017]

click and purchase history as well as their operating system or browser or whether they were using a mobile device.[35]

As we move towards 'smart' environments and 'persuasive computing' automatically modified choice architectures[36] can nudge the behaviour of data subjects in the real world.[37]

[35] Hannak, A., Soeller, G., Lazer, D., Mislove, A. and Wilson, C., 2014, November. Measuring price discrimination and steering on e-commerce web sites. In Proceedings of the 2014 conference on internet measurement conference (pp. 305-318). ACM.
[36] Tene, O. and Polonetsky, J., 2012. Big data for all: Privacy and user control in the age of analytics. Nw. J. Tech. & Intell. Prop., 11, p.xxvii.
[37] Mikians, J., Gyarmati, L., Erramilli, V. and Laoutaris, N., 2012, October. Detecting price and search discrimination on the internet. In Proceedings of the 11th ACM Workshop on Hot Topics in Networks (pp. 79-84). acm.