PRIVACY INTERNATIONAL

Briefing on the Data Protection Bill for the Committee Stage in the House of Lords

Privacy International's briefing (Law Enforcement and Intelligence Services)

November 2017

Briefing on the Data Protection Bill [HL] for Committee Stage in the House of Lords

Proposed draft amendments and comments

Law Enforcement and Intelligence Services Processing

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:

Anna Fielder
Senior Policy Adviser
Chair Emeritus
020 3422 4321
anna@privacyinternational.org

Tomaso Falchetta
Advocacy and Policy Team Lead
020 3422 4321
tomasof@privacyinternational.org

Table of Contents

INTRODUCTION **4**

PART 3: LAW ENFORCEMENT PROCESSING **5**

Clause 28: Meaning of "competent authority" **5**

Clause 33(6) & (7): Regulation making power re conditions for processing **5**

Clause 47: Right not to be subject to automated decision-making **6**

Clause 77: National security certificates – Law enforcement processing **9**

PART 4: INTELLIGENCE SERVICES PROCESSING **13**

Clause 84: Regulation making power re conditions for processing **13**

Clause 94: Right not to be subject to automated decision-making **13**

Clause 107: Transfers of personal data outside the United Kingdom **14**

Clause 108: National Security Exemption – Intelligence services processing **18**

Clause 109: National security certificate – Intelligence services processing **19**

Schedule 9: Conditions for processing under Part 4 ..... **21**

Schedule 11: Exemptions under Part 4 ..... **22**

Annex A **24**

Track changed version of clause 77: national security certificate for law enforcement processing 24

Annex B **26**

Rights that are exempted by national security certificates for law enforcement. 26

Annex C **28**

Track changed version of clauses 108 and 109: national security certificates for intelligence services processing 28

Annex D **31**

Rights that are exempted by national security certificates for intelligence services processing 31

Annex E **32**

UK police predictive policing plans based on responses to FOIA requests by Privacy International 32

Annex F **39**

INTRODUCTION

This briefing covers Part 3 (law enforcement processing) and Part 4 (intelligence services processing) of the Data Protection Bill.

Privacy International has also prepared:

- A briefing on the Data Protection Bill for the second reading in the House of Lords (available at http://bit.ly/2zxLDZX)

- A briefing on the Data Protection Bill for Committee State in the House of Lord covering General Processing (available at http://bit.ly/2Abc7ku)

The proposed draft amendments and comments in this briefing should be read in conjunction with these other briefings.

Privacy International's main concerns regarding Part 3 and 4 of the Bill (although they tie in with concerns elsewhere in the Bill) relate to:

- Delegated Powers
- Automated decision-making
- National Security Certificates
- Intelligence Agencies, cross-border data transfers (in Part 4)

.

PART 3: LAW ENFORCEMENT PROCESSING

Part 3 of the Data Protection Bill makes provision about the processing of personal data by competent authorities, as defined in the Bill, for law enforcement purposes and implements the EU Law Enforcement Directive**.**

Clause 28: Meaning of "competent authority"

Provide a full list of the meaning of "competent authority"

Amendment

Page 17, lines 28 – 29, delete subsection (1)(b)

(1) In this Part, "competent authority" means –
   a. A person specified in Schedule 7
   ~~b. Any other person if and to the extent that the person has statutory functions for any of the law enforcement purposes.~~

Rationale

Clarity is required as to who falls within the meaning of "competent authority". Subsection 28(1)(b) does not provide clarity as it is unclear what statutes will have to be considered to determine who falls under this provision. Schedule 7 appears to provide an exhaustive list of competent authorities and includes also provisions for some persons or entities under contract or under enactments, in paragraphs 35 to 38. If any specific entities are missing, they should be added to that list as an exhaustive list in Schedule 7 is a remedy to this potential for lack of clarity and transparency.

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.

Amendment

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"

Rationale

Regulation making powers bypass effective parliamentary scrutiny.

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.

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.

Clause 33(6) provides the Secretary of State with the power to add, vary or omit these conditions. This bypasses effective parliamentary scrutiny. This has been highlighted as an issue by the Delegated Powers and Regulatory Reform Committee,[1] which found that:

"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."

The proposed amendment seeks to remove this delegated power so that any changes to conditions would be made by primary legislation, amending the Bill. An alternative, amendment is also proposed that would make any regulations subject to the super-affirmative procedure under section 18 of the Legislative and Regulatory Reform Act 2006, which would mean that there was a statutory duty to consult and the Minister must have regard to representations made.

Automated decision-making authorized by law: safeguards

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[2].

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

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

Amendment

[1] Delegated Powers and Regulatory Reform Committee 6th Report of Session 2017-19 - published 24 October 2017, in particular paras 52 – 58, available at: http://bit.ly/2iCjXMO

[2] See also Privacy International's briefing (General Processing), re clause 13 which contains a full background related to automated processing, pages 16 – 22 http://bit.ly/2Abc7ku

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."

Rationale

The right in Article 11 Automated Individual Decision Making, of the Law Enforcement Directive, is very similar to that in Article 22 of GDPR.[3] 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, who 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.*" [4]

For the purposes of clarity of obligations imposed on controllers under Part 3, it is important that this explanation is included in the Bill. There is no rationale for omitting it in this section.

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

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

Amendment

Page 28, line 19, after "by law" add the following:
", subject to subsection ()"

Page 28, line 19, add new sub clause**:**

---

[3] Article 11 Law Enforcement Directive: 1. Member States shall provide for a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, to be prohibited unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller. 2. Decisions referred to in paragraph 1 of this Article shall not be based on special categories of personal data referred to in Article 10, unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place. 3. Profiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in Article 10 shall be prohibited, in accordance with Union law.

[4] Article 29 Working Party Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679, wp251, available at http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

"() 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."

Rationale

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

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[5] (see Annex E for details on current predictive policing plans.)

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."

Rationale

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

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.

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

[5] See https://www.privacyinternational.org/de/583

this section, particularly as there are growing concerns about the risks surrounding the use of automated decision making, including profiling, by the police.

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.

Clause 77: National security certificates – Law enforcement processing

Making national security certificates more transparent and accountable

Amendments

See full track changed amendment in Annex A below and provisions which are exempted in Annex B.

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).

Rationale

The national security exemption provisions contained in Part 3 for Law Enforcement processing to a large extent mirror the extremely wide exemption from the Data Protection Act 1998 where a national security certificate has been made. The provision allows exemption from fundamental data subject rights.

The provisions in Part 3 appear to broaden 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 the sub-sub sections, then this permits that a ‘national security certificate’ may relate to:

(a) Avoid obstructing an official or legal inquiry, investigation or procedure;
(b) Avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
(c) Protect public security;
(d) Protection national security;
(e) Protect the rights and freedoms of others.

It is therefore imperative that in referencing a restriction for clauses 42, 43, 46 and 66 they not only refer to the subsection but also the sub-sub section i.e. 42(**4**)**(d)**, 43(4)**(d)**, 46(3)**(d)** and 66(7)**(d)**. A failure to do so would significantly extend the power to exempt from data protection provisions beyond what is justifiable for genuine national security reasons.

The provision in §77(2)(b) undermines the ability to ensure effective oversight and safeguards. 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’. This should be removed completely as a wholly unacceptable provision.

National security certificates have never been subject to any oversight, review, critique by Parliament or any other statutory body. Certificates are timeless in nature and can be imposed prospectively and retrospectively. We propose the deletion of the phrase “or at any time was” in clause 77(3) to remove the retrospective nature. We propose limiting them to 6 months and deleting clause 77(4) which permits it to have prospective effect without checks. 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.

To address the current opaque nature of national security certificate we propose that all certificates are laid before Parliament and publicly accessible. We encourage Parliament to publish all current and extant certificates.

There is no independent oversight of this regime. We propose that a certificate must be ordered by a Judicial Commissioner, rather than the Minister simply signing it through. A fundamental and basic safeguard is to introduce a procedure for a Minister of the Crown to apply to a Judicial Commissioner for a certificate. The Judicial Commissioner must review the Minister's conclusions as to necessity and proportionality. To ensure oversight and safeguards are effective, sufficient detail is required in the certificate application. We have proposed such amendments that remove, for example clauses permitting general descriptions, and new clauses.

The removal of the ability to rely on 'general descriptions' appears to then necessitate the deletion of clauses 7 to 9. With a more democratic system in place this further requires the deletion of clauses 10 and 11 which are in provisions which should be acceptable and which are redundant if a proper oversight system is in place.

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.

The Data Protection Bill presents an opportune moment to reform this opaque and undemocratic regime. It may be necessary for further provisions to be made in respect of Judicial Commissioner involvement. We leave this to Parliament to consider and note that an oversight role can be performed by the Investigatory Powers Commissioner.

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"

Rationale: Our concerns regarding delegated powers are already highlighted in relation to Part 3 of the Bill. This amendment is proposed for the same reasons. The concerns with these regulation making powers were also highlighted by the House of Lords Delegated Powers and Regulatory Reform Committee.

"Schedule 10 makes equivalent provision in respect of the conditions applicable to sensitive processing under Part 4 of the Bill which applies to the intelligence services. 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"

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

Amendment

Page 54, line 26, add after "law": "unless the decision affects an individual's rights under the Human Rights Act 1998"

Rationale

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

Intelligence Agencies 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[6] . In the course of Privacy International's litigation before the Investigatory Powers Tribunal[7], 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[8]

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

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

Amendment

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."**

Rationale

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." (http://ec.europa.eu/newsroom/document.cfm?doc_id=47742)

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.

Clause 107: Transfers of personal data outside the United Kingdom

Safeguard transfer of personal data to third countries by UK intelligence agencies

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.

[6] https://www.privacyinternational.org/node/315
[7] Privacy International v Secretary of State for Foreign & Commonwealth Affairs & Ors [2016] UKIPTrib 15_110-CH Bulk Personal Datasets and Bulk Communications Data.
[8] https://www.privacyinternational.org/node/1532

Amendment

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

Rationale

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

Domestic legislation governing intelligence sharing is inadequate.[9] 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.

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."[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*."[11]

Clause 107 continued

Amendment(s)

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)

[9] Privacy International v Secretary of State for Foreign & Commonwealth Affairs & Ors [2016] UKIPTrib 15_110-CH
[10] Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, U.N. Human Rights Committee, U.N. Doc. CCPR/C/GBR/ CO/7, para. 24 (17 Aug. 2015).
[11] Szabó and Vissy v. Hungary, App. No. 37138/14, European Court of Human Rights, Judgment, para. 78 (12 Jan. 2016).

(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).

(6) 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 of 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.

Rationale:

As it currently stands, Clause 107 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.

In the context of Privacy International's litigation on bulk data,[12] 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.

In separate litigation[13] 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."*[14]. 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.

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.

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 should have a lower standards that that applicable to law enforcement's transfers.

---

[12] Privacy International v Secretary of State for Foreign & Commonwealth Affairs & Ors [2016] UKIPTrib 15_110-CH Bulk Personal Datasets and Bulk Communications Data.

[13] 10 Human Rights Organisations v The United Kingdom, Application Number: 24960/15.

[14] David Anderson, Q.C., A Question of Trust, Report of the Investigatory Power Review, para 7.66.

Clause 108: National Security Exemption – Intelligence services processing

Restricting the scope of the national security exemption

A track changed edit of this clause is at Annex C. The provisions which it exempts are in Annex D.

Amendment

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.

Rationale

It is unacceptable that in the context of Intelligence Services Processing it is permissible to exempt the requirement in 94(1) that "The controller may not take a decision significantly affecting a data subject that is based solely on automated processing of personal data relating to the data subject." This must be an exception to the exemptions permitted by a national security certificate.

We do not accept that the intelligence agencies should be permitted to be exempt from oversight. Instead of exempting intelligence services through a national security certificate, we suggest in the alternative that it is simply clarified that oversight functions in relation to the intelligence agencies rest with the Investigatory Powers Commissioner which already has oversight of the agencies and can carry out the equivalent functions that would have been done by the Information Commissioners' Office.

We are concerned at the breadth of the other exemptions permitted under clause 108 and suggest Parliament scrutinise what provisions are necessary and proportionate.

Clause 109: National security certificate – Intelligence services processing

Making national security certificates more transparent and accountable

A track changed edit of this clause is at Annex C

Amendment

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:
- **a. approved by a Judicial Commissioner,**
- **b. laid before Parliament,**
- **c. 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. 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 sub section 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).

Rationale

We rely on the reasons we have set out in relation to Clause 77. In addition we note the following. There currently exist national security certificates signed in 2001 by Jack Straw and David Blunkett which were disclosed in the course of successful litigation brought by Privacy International which found that bulk personal data set and bulk communications data regimes were unlawful for over a decade (see attached).

These disclosed national security certificates appear to cover all work carried out by the intelligence agencies. In addition to internal functions related for example to employment, they cover:

GCHQ:

Personal data processed in the performance of the functions described in section 3 of the Intelligence Services Act 1994 or personal data processed in accordance with section 4(2)(a) Intelligence Services Act.

Security Service:

> Personal data processing in performance of the functions of the Security Service escribed in section 1 of the Security Services Act 1989 as amended by the Security Service Act 1996…
>
> **Secret Intelligence Service**
>
> Personal data processed in performance of the functions of SIS described in section 1 of the Intelligence Services Act 1994 or in accordance with section 2 of the ISA.

This raises the question as to the purpose of Part 4 in reality, if the practice is to exempt all data protection safeguards. This not only has a bearing on questions concerning effective oversight from the perspective of data protection safeguards, but further raises the specter of an adequacy decision. If the Intelligence Agencies in effect, have a blanket exemption from all data protection legislation, how is this justified, and what data protection safeguards can and do exist in relation to their processing of personal data.

We therefore suggest in addition to our proposed amendments, and in reliance upon the rationale above, that scrutiny is given to which activities, if any, which have now been disclosed as a result of Privacy International's litigation and the Investigatory Powers Act 2016, are in fact subject to data protection legislation. Given the broad nature of certificates, it may also be of use to Parliament to gain an understanding of what processes and procedures exist to determine which activities are exempt, or whether it is in fact exemption by default.

It is of utmost importance and relevance to a decision on adequacy whether Part 4 has little real application to the broad range of processing carried out by the intelligence agencies.

The evidence to date supports our view that little if any of the processing carried out by the Intelligence Agencies would fall within Part 4, and we welcome discussion in this respect.

We note with concern the proposed exemptions to 94(1) in relation to automated decision making.

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

Amendment

Page 171, line 37

Leave out subsection 5(e).

Rationale

We understand that 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.

Remove legitimate interest condition from UKIS

Amendment

Page 171, line 39

Leave out subsection (5)

Rationale

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 without their statutory remit.

Schedule 11: Exemptions under Part 4

Restrict the conditions for processing under Part 4

Amendment

Page 173, line 34

Leave our paragraph 1

Rationale

The listed provisions 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.

Amendment

Page 175,

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

Rationale

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.

Annex A

Track changed version of clause 77: national security certificate for law enforcement processing

77 National security: certificates by the Minister

(1) A Minister of the Crown **must apply to a Judicial Commissioner for a certificate,** ~~may issue a certificate certifying,~~ for the purpose of section 42(4)**(d)**, 43(5)**(d)**, 46(3)**(d)** or 66(7)**(d)**, **if he or she believes** that a restriction is a necessary and proportionate measure to protect national security.

[New Clause

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.]**

(2) An application for a ~~The~~ certificate ~~may~~ **must** –

a. **Identify which** ~~Relate to a~~ specific restriction (described in the certificate) ~~which~~ a controller ~~has~~ **seeks to** impose~~d~~ or is proposing to impose under section 42(4)**(d),** 43(4)**(d)**, 46(3) or 66(7), ~~or~~ **and**

~~b. Identify any restriction to which it relates by means of a general description.~~

c. **Identify the personal data to which it applies by means of a detailed description, and**

d. **Provide a justification for both (a) and (c).**

[New Clause

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:

- **(d) Whether the certificate is necessary on relevant grounds, and**
- **(e) Whether the conduct that would be authorised by the certificate is proportionate to what is sought to be achieved by that conduct, and**
- **(f) Whether it is necessary and proportionate to exempt all provisions specified in the certificate.]**

~~(3) Subject to subsection (6), a certificate issued under subsection (1) is conclusive evidence that the specific restriction or (as the case may be) any restriction falling within the general description is, or at any time was, a necessary and proportionate measure to protect national security~~

~~(4) A certificate issued under subsection (1) may be expressed to have prospective effect.~~

New clauses

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.

(5) 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.

(6) If, on an appeal under subsection (4), the Tribunal finds that, applying the principles applied by a court on an application for judicial review, **it was not necessary or proportionate to issue** the Minister did not have reasonable grounds for issuing a certificate, the Tribunal may –

1. Allow the appeal, and
2. Quash the certificate.

~~(7) Where in any proceedings under or by virtue of this Act, it is claimed by a controller that a restriction falls within a general description in a certificate issued under subsection (1), any other party to the proceedings may appeal to the Tribunal on the ground that the restriction does not fall within that description.~~

~~(8) But, subject to any determination under subsection (9), the restriction is to be conclusively presumed to fall within the general description.~~

~~(9) On an appeal under subsection (7), the Tribunal may determine that the certificate does not so apply.~~

~~(10) A document purporting to be a certificate under subsection (1) is to be — (a) received in evidence, and (b) deemed to be such a certificate unless the contrary is proved.~~

~~(11) A document which purports to be certified by or on behalf of a Minister of the Crown as a true copy of a certificate issued by that Minister under subsection (1) is — (a) (b) in any legal proceedings, evidence of that certificate, and in any legal proceedings in Scotland, sufficient evidence of that certificate.~~

(12) The power conferred by subsection (1) on a Minister of the Crown is exercisable only by—

(a) a Minister who is a member of the Cabinet, or (b) the Attorney General or the Advocate General for Scotland.

~~(13) No power conferred by any provision of Part 6 may be exercised in relation to the imposition of — (a) a specific restriction in a certificate under subsection (1), or (b) a restriction falling within a general description in such a certificate.~~

Annex B

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 –

a. Avoid obstructing an official or legal inquiry, investigation or procedure;
b. Avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
c. Protect public security;
d. Protect national security;
e. 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 –

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

a. Avoid obstructing an official or legal inquiry, investigation or procedure;
b. Avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
c. Protect public security;
d. Protect national security;
e. 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 –

a. Avoid obstructing an official or legal inquiry, investigation or procedure;
b. Avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
c. Protect public security;
d. Protect national security;
e. 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 -

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

Annex C

Track changed version of clauses 108 and 109: national security certificates for intelligence services processing

108 National Security

(1) A provision mentioned in subsection (2) does not apply to personal data to which this Part applies if exemption from the provision is required for the purpose of safeguarding national security.

(2) The provisions are –

a. Chapter 2(the Data Protection Principles), except section 84(1)(a) and (2) and Schedules 9 and 10;

b. Chapter 3 (rights of data subjects) **except section 94(1);**

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

~~d. 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;~~

~~e. In Part 6~~

~~i. Sections 137 to 147 and Schedule 15 (Commissioner's notices and powers of entry and inspection);~~

~~ii. Sections 161 to 163 (offences relating to personal data)~~

~~iii. Sections 164 to 166 (provision relating to the special purposes)~~

[Insert new clauses

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 agencies processing

(1) ~~Subject to subsection (3), a~~ **A** ~~certificate signed by a~~ Minister of the Crown **must apply to a Judicial Commissioner for a certificate, if exemptions are sought** ~~certifying that exemption~~ from **specified** ~~all or any of the~~ provisions mentioned in section 108(2) ~~is~~, ~~**or at any time was**~~, ~~required~~ for the purpose of safeguarding national security in respect of any personal data ~~is conclusive evidence of that fact~~.

[New clauses

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.

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.]

(2) **An application for a** certificate ~~under subsection (1)—~~

a. **Must** ~~may~~ identify the personal data to which it applies by means of a ~~general~~ **detailed** description, and

~~(b) may be expressed to have prospective effect.~~

[new clauses:

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.

(3) Any person **who believes they are** directly **or are indirectly** affected by the issuing of a certificate under subsection (1)

a. may appeal to the Tribunal against the certificate

b. rely upon section 173 of this Act.

(4) If on an appeal under subsection (3), the Tribunal finds that~~, applying the principles applied by a court on an application for judicial review~~, **it was not necessary or proportionate to issue** ~~the Minister did not have reasonable grounds for issuing~~ the certificate, the Tribunal may—

(a) allow the appeal, and

(b) quash the certificate.

~~(5) Where, in any proceedings under or by virtue of this Act, it is claimed by a controller that a certificate under subsection (1) which identifies the personal data to which it applies by means of a general description applies to any personal data,~~

another party to the proceedings may appeal to the Tribunal on the ground that the certificate does not apply to the personal data in question.

(6) But, subject to any determination under subsection (7), the certificate is to be conclusively presumed so to apply.

(7) On an appeal under subsection (5), the Tribunal may determine that the certificate does not so apply.

(8) A document purporting to be a certificate under subsection (1) is to be —

(a) received in evidence, and

(b) deemed to be such a certificate unless the contrary is proved.

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

Annex E

UK police predictive policing plans based on responses to FOIA requests by Privacy International

This Annex expands on the rationale given for the amendment of Clause 47 (see page 3) which aims to ensure that the Bill addresses the current and planned reliance of police forces on 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. By way of example of the technologies currently being considered or used by the UK police, we set out here the information one one key area of data-driven policing which has seen a rapid rise in popularity. This is based on information we hold as a result of Freedom of Information Act request in relation to predictive policing. If you seek copies of the relevant response we can provide them.

Predictive policing is an algorithm-based approach to policing based on the assumption that certain algorithms and machine learning can help predict where and when crimes will happen. Her Majesty's Inspectorate of Constabulary has defined predictive policing as:

> "Methods used by police forces to use and analyse data to predict future patterns of crime and vulnerable areas." It also offers a definition of "preventative policing": "Methods used by police forces to pre-empt crime and to prevent it happening. These can range from working with other partners and agencies to using predictions about where crimes may occur to decide where to place visible resources."

An investigation carried out by online-publication ProPublica exposed bias of algorithms used in predictive policing, and that regardless of the crimes they have committed, people of colour are disproportionately wrongly assigned a high risk score, while white people are disproportionately more likely to be granted a low risks score.[15]

Use of predpol

Predpol was the first company to sell predictive policing software. The use of predictive policing in the UK was first publicised in 2013 when media organisations including the International Business Times publicized the potential use of the PredPol program in the UK, which allows police to feed in crime data, from which it calculates and highlights 250-yard zones of particular risk[16]. This technology has attracted controversy and concerns that it is biased and discriminatory[17] if for example the data that it relies upon is not neutral.

---

[15] https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing
[16] http://www.ibtimes.co.uk/predictive-policing-predpol-future-crime-509891
[17] https://www.economist.com/news/briefing/21582042-it-getting-easier-foresee-wrongdoing-and-spot-likely-wrongdoers-dont-even-think-about-it

The IBTimes identified a number of UK police forces and stated that:

> *"Forces in Greater Manchester, Kent, the West Midlands and West Yorkshire that trialed the software have reported encouraging results. In Trafford, a borough of Manchester, police using the software witnessed a drop in burglary rates of 26% between May 2010 and May 2011, compared with a 9% reduction across the city as a whole.*
>
> *Now the Metropolitan Police in London is to use the technology with police commissioner Sir Bernard Hogan-Howe reportedly strongly supportive of the scheme."*

Privacy International questioned these forces in relation to their use of the company PredPol's predictive policing software[18], and received the following responses:

> ***Greater Manchester:***
>
> *07.11.16*
> *GMP were approached by declined. Of note, however, GMP's Trafford division had its own method not linked to PredPol.*
> http://www.ucl.ac.uk/jdi/events/int-CIA-conf/ICIAC11_Slides/ICIAC11_5A_VJones
>
> As part of the trial GMP 'provided a small data set of sanitized crime data of the same type that is publicly available on the crime map (Home Office open source) to allow PredPol to demonstrate local data within the PredPol software as part of their initial approach to GMP. They state that no reviews of the technology were conducted. A decision not to proceed with PredPol was taken without any test or trial.
>
> ***Kent:***
>
> On 28.11.2017 Kent police stated:
> *"Kent Police is currently using Predpol technology and is on an ongoing contract. Data has been supplied to researches to test the application of PredPol technology.*
>
> *The attached appendices provide reports drafted since 1 January 2014 relating to Predpol. For appendix 1, 'PredPol operational review', the introduction states "The full report will be published at the next Performance Committee on 16 April 2014". Please note that it was later decided that this report was not necessary and as such was not created. For appendix 2, the third paragraph makes reference to 'Table 1', however please note that no such table was created."*

---

http://uk.businessinsider.com/predictive-policing-discriminatory-police-crime-2016-10

[18] http://www.predpol.com/

We asked Kent again in 2017 about use of predictive policing technology. We are still awaiting a response.

MET:

The MET stated in 2016 in relation to PredPol that

"The MPS have been actively exploring the use of predictive policing technology. Between May 2014 to April 2015, trials of three predictive mapping companies took place of which PredPol was one. We are not currently using PredPol.

The MPS currently use an 'in house' predictive analytical product."

They confirmed that data as supplied to researchers to test the application of PredPol technology. In response to a follow up request, the MET confirmed that two companies trialed May 2014 to April 2015 were Azavea and Palantir. The MET provided these companies with data to test their predictive analytics. Data Sharing Agreements will all three companies stipulated that all data was to be destroyed at the conclusion of the trial.

In relation to the in house product they state:

"The process was written in-house but was based on the process originally devised by Greater Manchester Police which was published on the Internet. We have since revised their process on a number of occasions in response to user feedback and some academic support. We didn't have to buy any specialist hardware or software to run the process but we did need to buy some hardware and software to produce the volume of outputs eventually requested by the business."

The MET stated they could not provide information on a review of in house practices since 'it is not held in any central location'.

West Midlands

"West Midlands Police have never been approached by the company PredPol nor other companies offering predictive policing software in the last 2 years. A while ago we did talk to the Jill Dando Institute about some research work that they were doing about hot streets, but that was probably more than 2 years ago.

Internally, WMP have done some analysis of crime and incident data around hot grids. This was doe using our in-house geographical information system and some aoristic analysis using Excel programming. For this we used internal resources."

West Yorkshire

"West Yorkshire hold no information and confirm that the article is incorrect. We do not currently, and have not previously used this technology or supplied any data."

2017 update

In 2017 a Tech UK report on Policing and the Internet of Things states:

> *"The vast amounts of data now generated online creates vast opportunities to anticipate risk, and predictive policing is already being trialled. Indeed, the Met police disclosed in December 2016 that they have actively been exploring the use of predictive policing, with trials of three predictive mapping companies between May 2014 and April 2015."*
>
> *"Advanced use of data - bringing together and analysing information from a number of sources - could help the police better prioritise resources and protect officers. Visualisation systems now exist that allow forces to minority and integrate a wide array of data streams, like transit maps, weather repots and crime statistics. Authorities can then look for patterns and trends."*

Privacy International decided to enquire more widely about the use of predictive policing. In response to Freedom of Information requests in 2017 further to this report we received the following responses:

Avon and Somerset

> *"Predictive analytics is utilised by the constabulary. Predictive policing / mapping software is used. We use SPSS Modeler provided by IBM. We operate the technology ourselves. Visualisation systems are used. We use Qlik Sense and Business Objects."*

British transport police:

> *"British Transport Police has not trialled predictive policing to date but it is likely to do so over the next 24 months.*
>
> *British Transport Police has software that would be capable of running predictive analytics but it is not specifically designed or currently used for this.*
>
> *The software is a generic GIS software package supplied under licence from Pitney Bowes."*

Cheshire states that it intends to trial predictive policing in the next 24 months.

Derbyshire police do not currently use predictive policing but state that this may change.

Gwent

> "*We tried, but network infrastructure problems prevented the trial for technical reasons. We do intend to trial predictive policing as soon as it becomes technically feasible.*

We are joint partners with South Wales Police in developing the software, which was also partly funded by Welsh Government. Presently, we don't own the software but we hold an option to purchase the software at a reduced prices in future. "

Lancashire state

"*Lancashire Constabulary has a selection of trained Analysts who have the capability to conduct predictive analysis to varying levels as well as crime mapping and these are dedicated roles. There will be a small number of other staff however that have these skills outside of this being a core aspect of their role. Lancashire Constabulary has been using near-repeat victimisation analysis for highlighting areas of burglary risk, there is also some staff in our corporate development team who conduct statistical forecasts of crime trends.*

Methods employed use a variety of software but nothing is badged as 'predictive software / hardware' therefore the answer to this question it no. I can advice however that for mapping purposes we use MapInfo (provided through the CDR group) and Northgate XD (provided through Northgate Public Services). We have trialled add-on's to MapInfo, but we have not adopted or commissioned any additional services. We have found that the best approach is the application of scientific analysis to the data yields results that enable appropriate directing of resources.

…we have used the Microsoft Business Intelligence power tools for improving visualisation of data in the form of dashboards and this is party of Microsoft office."

Leicestershire

"Leicestershire Police does not currently use predictive policing, however we are looking into the possibility of employing this in the future."

Merseyside

"Merseyside Police do not intend to run any trials, the Force already has such systems in place. The force use predictive policing / mapping software and hardware. Merseyside Police own and operate the software and do not use a company to provide the technology."

Northamptonshire state they have trialed predictive policing but do not use specific predictive policing software.

North Wales

Trialed predictive policing and use predictive policing.
IBM SPSS Modeler.

Police Scotland

"Police Scotland has recently launched a Policing 2026 strategy which aims to align the organisation's priorities and resources with the changing face of society and policing challenges we anticipate over the next 10 years. The strategy outlines our commitment to 'invest in our information' and recognises the benefits that can be gained from harnessing our data as a strategic asset. We will be undertaking some significant programs of work as we look to put the appropriate services, structures and governance in order to better manage our data as we recognise this will be the foundations with which to explore added value through the use of data. Data analytics and predictive modelling is an area Police Scotland wish to explore in the pursuit of new strategies, operating models and insight however we recognise the key enabler to this is strong data governance and this will form the initial stage of our work program.

Currently we don't have any 3rd party procured predictive analysis software and, at present, there are no plans to buy any in the next 24 months."

Staffordshire Police state:

"Staffordshire Police is currently embarking on a 3 – 5 year transformation programme within which the use of technologies as mentioned are an aspiration.

Currently however there are no planned activities around these areas. It is likely that should the force wish to trial these that they would work with their strategic IT partner Boeing Defence UK to enable this."

South Wales

"*South Wales Police have recently run a Small Business Research Initiative (SBRI) project in relation to developing a predictive policing solution. The SBRI process is run by Innovate UK and is funded R&D. As part of this process this force worked with 2 companies to develop potential solutions. The companies were Innaxys Ltd. And GPC Ltd. During the project both companies piloted their prototype solutions on a small scale. The project ended recently and the force is currently undertaking an evaluation process to determine whether it wishes to continue to a procurement state with either company.* "

Warwickshire

"Software was trialed in one policing area but was not procured. There are no plans to trial other predictive policing software as we are about to introduce other

software systems that may enhance our capability or will at least need to be considered regards interoperability."

West Yorkshire state:

"*We are currently piloting the use of predictive analytics in one locality in West Yorkshire. The software that generates the predictions is owned by the University College London. We operate the software as part of a successful Home Office Innovation Fund bid.*

Visualisation software and mobile technology is used to disseminate to end users. We use Cadcorp software for visualisation as part of wider existing licence agreement between Yorkshire Police and Cadcorp[19]. "

[19] https://www.blpd.gov.uk/foi/foicontractview.aspx?contractid=31648

Annex F

National security certificates under the DPA

National security certificates were issued under section 28 of the Data Protection Act 1998 for the Security Service (MI5), the Secret Intelligence Service (MI6) and GCHQ.

By way of example, we have included (see next page) the certificate covering the Secret Intelligence Service.

SECTION 28 DATA PROTECTION ACT 1998

CERTIFICATE OF THE SECRETARY OF STATE

---

1. **Whereas:**

(i) by section 28(1) of the Data Protection Act 1998 ("the Act") it is provided that personal data are exempt from any of the provisions of :-

(a) the data protection principles;

(b) Parts II, III and V; and

(c) section 55

of the Act if the exemption from that provision is required for the purpose of safeguarding national security;

(ii) by subsection 28(2) it is provided that a certificate signed by a Minister of the Crown certifying that the exemption from all or any of the provisions mentioned in subsection 28(1) is or at any time was required for the purpose there mentioned in respect of any personal data shall be conclusive evidence of that fact;

(iii) by subsection 28(3) it is provided that a certificate under subsection 28(2) may identify the personal data to which it applies by means of a general description and may be expressed to have prospective effect.

2. **And considering** the potentially serious adverse repercussions for the national security of the United Kingdom were the exemptions hereafter identified not available.

And for the reasons set out in my public statement issued on 10 December 2001, in summary that:

2.1 The work of the security and intelligence agencies of the Crown requires secrecy.

2.2 The general principle of neither confirming nor denying whether the Secret Intelligence Service (SIS) processes data about an individual is an essential part of that secrecy.

2.3 In dealing with subject access requests under the Data Protection Act 1998, SIS will examine each individual request to determine:

(i) whether adherence to that general principle is required for the purpose of safeguarding national security; and

(ii) in the event that such adherence is not required, whether and to what extent the non-communication of any data or any description of data is required for the purpose of safeguarding national security.

2.4 The very nature of the work of SIS requires exemption on national security grounds from those parts of the Act which would prevent it for example passing data outside the European Economic Area and which would allow access to SIS's premises by third parties.

3. **Now, therefore**, I, the Right Honourable Jack Straw MP, A Minister of the Crown and a member of the Cabinet, in exercise of the powers conferred by the said section 28(2) do issue this certificate and certify as follows:-

3.1. that any personal data processed by the SIS as described in Column 1 of Part A in the table below are and shall continue to be required to be exempt from those provisions of the Act which are set out in Column 2 of Part A;

3.2. that any personal data processed by any other person or body in the course of data processing operations (in circumstances where the data processing comprises or includes the disclosure of data by that other person or body to SIS) in the course of data processing operations carried out for, on behalf of, at the request of or with a view to assisting SIS or in relation to the functions of SIS as set out in section 1 of the Intelligence Services Act 1994, as described in Column 1 of Part B in the table below are and shall continue to be exempt from those provisions of the Act which are set out in Column 2 of Part B;

3.3. that any personal data processed by any other person or body (other than a Government department, agency or non-departmental public body) in the course of data processing operations as a consequence of its disclosure by SIS in accordance with section 2(2)(a) of the Intelligence Services Act 1994 as described in Column 1 of Part B in the table below are and shall continue to be exempt from those provisions of the Act which are set out in Column 2 of Part B;

3.4. that any personal data processed by SIS as described in Column 1 of Part C in the table below are and shall continue to be required to be exempt from those provisions of the Act which are set out in Column 2 of Part C below; and

3.5. that any personal data processed by SIS as described in Column 1 of Part D of the table below are and shall continue to be required to be exempt from those provisions of the Act as are set out in Column 2 of Part D below

all for the purpose of safeguarding national security, provided that:

(i) no personal data shall be exempt from the provisions of section 7(1)(a) of the Data Protection Act 1998 if SIS, after considering any request by a data subject for access to relevant personal data, determines that adherence to the principle of neither confirming nor denying whether SIS holds personal data about an individual is not required for the purpose of safeguarding national security;

(ii) no personal data shall be exempt from the provisions of section 7(1)(b), (c) or (d) of the Data Protection Act 1998 if SIS, after considering any request by a data subject for access to relevant personal data, determines that non-communication of such data or any description of such data is not required for the purpose of safeguarding national security.

4. **This certificate** gives notice that I require SIS, by virtue of my authority arising from section 1(1) of the Intelligence Services Act 1994, to report to me on the operation of the exemptions described in this certificate.

5. **This certificate** in all respects supersedes the Certificate of the Secretary of State in respect of SIS dated 30 July 2000, and that Certificate is hereby revoked.

PART A	
Column 1	**Column 2**
1. Personal data processed in performance of the functions of SIS described in section 1 of the Intelligence Services Act 1994 ("ISA") or in accordance with section 2 of the ISA. 2. Personal data processed in relation to the recruitment of staff of SIS and assisting with the recruitment of staff of the Security Service and GCHQ. 3. Personal data processed for the purposes of the administration of human resources in relation to former members of staff. 4. Personal data processed in relation to vetting of SIS's candidates, staff, contractors, agents and others in accordance with the government's vetting policy.	(i) Sections 7(1), 7(8), 10, 12 of Part II; (ii) Section 16(c), 16(e), 16(f), 17, 21, 22 and 24 of Part III; (iii) Part V; (iv) the first data protection principle; (v) the second data protection principle; (vi) the sixth data protection principle to the extent necessary to be consistent with the exemptions contained in this certificate; and (vii) the eighth data protection principle.

Part B	
Column 1	**Column 2**
1. Personal data processed for, on behalf of, at the request of or with a view to assisting SIS, including: • personal data processed in relation to the functions described in section 1 of the ISA; • personal data processed in relation to the recruitment of staff of SIS and assisting with the recruitment of staff of the Security Service and GCHQ; • personal data processed in relation to the vetting of SIS's candidates, staff, contractors, agents and others in accordance with the government's vetting policy. 2. Personal data processed as a consequence of disclosure by SIS in accordance with section 2(2)(a) of the ISA.	(i) Sections 7(1), 7(8), 10, 12 of Part II; (ii) Section 16(c), 16(e), 16(f), 17, 21, 22 and 24 of Part III to the extent that those provisions require any reference to SIS or data processing operations carried out by, in support of, at the request of or with a view to assisting SIS or in consequence of a lawful disclosure by SIS; (iii) Part V; (iv) section 55; (v) the first data protection principle; (vi) the second data protection principle; and (vii) the sixth data protection principle to the extent necessary to be consistent with the exemptions contained in this certificate

PART C	
Column 1	**Column 2**
1. Personal data processed by SIS for the purposes of administration of human resources in relation to serving members of staff only (except for the filing system containing confidential data as described in Part D of this table) and staff pay, tax and national security contributions. 2. Personal data processed by SIS for the purposes of maintaining CCTV coverage of Vauxhall Cross, 85 Albert Embankment, London SE1, in relation to the security and integrity of the building, crime prevention and detection and the apprehension and prosecution of offenders, to the extent that the said data do not comprise data to which Part A or Part B applies.	(i) Sections 16(1) (f), 47 and 50 and Schedule 9, and (ii) the eighth data protection principle.

Part D	
Column 1	**Column 2**
Insofar as it relates to serving members of staff, personal data processed by SIS for the purpose of maintaining and consulting a filing system containing confidential data about members of its staff whose purpose is to provide personnel officers and management with information considered necessary to make informed decisions as to the suitability of individuals for any task, appointment, postings or any other matter, with particular regard to the security implications of those decisions.	(i) Sections 7(1), 7(8), 10, 12 of Part II; (ii) Section 16(c), 16(e), 16(f), 17, 21, 22 and 24 of Part III; (iii) Part V; and (iv) the eighth data protection principle.

.....

The Right Hon Jack Straw MP

dated the 8th day of December 2001