Briefing on Clauses 28-30: National Security Exemptions and Joint Processing Notices for law enforcement

Data Protection and Digital Information Bill

House of Lords

Committee Stage

March 2024

For further information contact

Ellen Lefley, Lawyer, elefley@justice.org.uk

JUSTICE, 2nd Floor Lincoln House, 296-302 High Holborn, London, WC1V 7JH

email: admin@justice.org.uk website: www.justice.org.uk

Introduction

1. JUSTICE is a cross-party law reform and human rights organisation working to strengthen the justice system. It is the UK section of the International Commission of Jurists. Our vision is of fair, accessible and efficient legal processes in which the individual's rights are protected and which reflect the country's international reputation for upholding and promoting the rule of law.

2. The briefing addresses Clauses 28-30 of the Data Protection and Digital Information Bill ("**the Bill**"). These Clauses are concerned with the data protection obligations of competent authorities when they are processing data for law enforcement purposes (eg police forces) and exemptions from those rights and obligations to protect national security.

Summary

3. Clauses 28-30 weaken the data protection obligations, principles and rights bind law enforcement authorities when processing the data of victims, suspects and witnesses in circumstances of national security.

4. JUSTICE does not dispute the legitimacy and necessity of specialist national security data provisions. However, new reductions to data protection in the name of national security must be proportionate given the highly sensitive data from victims, suspects and witnesses of crime processed and controlled by law enforcement. Therefore, JUSTICE supports probing whether these clauses are sufficiently proportionate and accountable in achieving the national security aim.

5. **JUSTICE therefore supports Peers probing whether national security can be secured by law enforcement without such wholesale exemption from data principles, obligations and rights as is provided in clauses 28-30; and/or whether such extremely broad exemptions should be subject to increased oversight. To that effect, we support the amendments 135A-135E tabled by Lord Clement-Jones.**

The current regime

6. Currently, under the Data Protection Act 2018 ("**DPA 2018**"), competent authorities can restrict some data protection rights for the purpose of safeguarding national security when processing data for law enforcement purposes.

7. This is contained within Part 3 of the DPA 2018, and is distinct from Part 2 – for general processing – and Part 4 – for intelligence services. The decisive factor is the purpose of

the data processing: if it is for a law enforcement purpose – i.e. the prevention, investigation detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security – then authorities must follow the rules in Part 3 DPA 2018.

8. On a case-by-case basis, competent authorities can currently restrict rights themselves for law enforcement purposes:

    a) the rights restriction must be both **necessary and proportionate** to protect national security – it cannot be simply precautionary or convenient for law enforcement; and

    b) only four rights are capable of being restricted:[1]

        i) the right for the individual to be informed of personal data processing;

        ii) their right of access to that personal data;

        iii) their right to rectification, erasure and restriction of processing; and

        iv) their right to be notified of a personal data breach.

9. Ministers of the Crown can also issue a national security exemption certificate, which is conclusive evidence that restrictions are a "necessary and proportionate" measure to protect national security.[2] Again they are limited to the four rights listed above.

10. The certificate is appealable to the Upper Tribunal by a person directly affected if there were no reasonable grounds for it being issued, applying judicial review principles.

Changes to be imposed by Clause 28

11. Clause 28 amends the national security exemptions for law enforcement processing. It does so in three ways:

    a) It replaces the phrase "when necessary and proportionate" to protect national security, with "when required to safeguard national security";

    b) It significantly expands the number of rights and obligations from which competent law enforcement authorities can be exempted for reasons of national security; and

    c) It permits national security certificates issued to simply state that exemption from *all* the eligible rights and obligations is required.

[1] Ss 44(4), 45(4), 48(3) & 68(7) DPA 2018
[2] S.79 DPA 2018

12. The appeal provisions against certificates remain the same.

13. The new expanded list of rights and obligations from which competent authorities can be exempted can be found in draft section 78A at Clause 28. It includes:

    a) Compliance with the six data protection principles, except for lawfulness.

    b) The rights already capable of being restricted (above) as well as the general right not to be subject to automated decision making, and the safeguards which apply when lawful automated decision making does take place.

    c) The vast majority of oversight of the Information Commissioner, including:

        i) Obligation to notify them of a breach, eg in the event of unlawful processing,

        ii) The Information Commissioner's general powers to investigate, correct, authorise and advise. This includes the commissioner's power on their own initiative to issue an opinion to Parliament, the government or other institutions and bodies as well as to the public on any issue,

        iii) The Information Commissioner's powers to issue information, assessment and enforcement notices,

        iv) The Information Commissioner's entry and inspection powers, including their power to inspect when in accordance with international obligations.

    d) Requirements for transfers to third countries or international organisations.

    e) Liability for statutory data offences, including the offence of altering, destroying or concealing information to prevent it being disclosed to the data subject when exercising their right of access (which can be restricted in any event, so this particularly relates to law enforcement being able to, in addition, falsify information with immunity).

14. These wider exemptions mirror those available under Part 4 to Intelligence Services at section 110 DPA 2018, as well as those available for general processing under Part 2 at section 26 DPA 2018. The latter applies, for example, if a company has national security concerns about its customers, or an organisation has national security concerns about its members. The exemptions allow such processors – often acting in a private capacity – to derogate from data protection rules as above when required to act on those national security concerns.

15. However, currently, when it is a competent authority and they are processing data for law enforcement purposes, they must meet a higher standard of protection for the personal

data of witnesses, victims and suspects, in circumstances of national security. Clause 28 therefore seeks to remove that higher protection.

Changes to be imposed by Clause 29 and 30

16. These clauses introduce a new joint processing regime to empower law enforcement competent authorities and intelligence services to jointly process personal data under Part 4 DPA 2018 governing the intelligence services' data processing, instead of those competent authorities being governed by Part 3.

17. In addition to wider national security exemptions than those for law enforcement, Part 4 also consists of fewer obligations. For example, Part 4 intelligence service processing does not require:

    - data protection officers to be designated;
    - logging and records of processing activities;
    - data protection impact assessments;
    - consultation with the Commissioner in the creation of high risk filing systems.

18. The designation notice regime is set out in Clause 29, inserting new sections 82A to 82E into the DPA 2018. It can be summarised as follows:

    - The joint processing would be enabled through a "designation notice", applied for by the competent authority.
    - The Secretary of State considers the application, and issues when he "considers that designation of the processing is required for the purposes of safeguarding".
    - Before giving a designation notice, the Secretary of State must consult with the Information Commissioner, and they may also consult with other relevant public or regulatory bodies as appropriate.
    - The Secretary of State must provide a copy of the designation notice to the Commissioner and the Commissioner must make available to the public a record of that designation notice whilst it is in force, with the assumption of transparency.
    - A designation notice must be reviewed at least annually by the Secretary of State, and may be withdrawn by the Secretary of State at any time, following

a review and when some or all of the processing to which the notice applies is no longer required for the purposes of safeguarding national security.

- Notices cease to be in force after a period of 5 years or a shorter period if specified in the notice issued by the Secretary of State.
- An appeal lies to the tribunal by a person who is directly affected by the notice, if there were no reasonable grounds to issue it, applying judicial review principles.

Government explanations for Clauses 28-30

19. The reasons given by the Government for clauses 28-30 have been brief. The explanatory notes and the human rights memorandum both explain that clause 28 increases national security exemptions to ensure consistency with the other regimes in Parts 2 and 4.[3] The new joint processing regime is "*to simplify data protection considerations by enabling a single set of data protection rules to apply to joint processing activity by the police and intelligence services, which is judged to have significant operational benefits, enabling closer working in efforts to detect and combat national security threats.*"[4]

20. In Public Bill Committee, Sir John Whittingdale explained that "*Clauses [28-30] are essentially designed to enable better joined-up working between the intelligence services and law enforcement*."[5] The evidence cited was "*reports on events such as the Manchester and Fishmongers' Hall terrorist incidents have demonstrated that better joined-up working between the intelligence services and law enforcement is in the public interest to safeguard national security. A current barrier to such effective joint working is that only the intelligence services can operate under part 4 of the Data Protection Act, which is drafted to reflect the unique operational nature of their processing*."[6]

21. Rights and Security International gave evidence to the Public Bill Committee, questioning whether the further measures were necessary, rather than desirable, necessity and proportionality being the test for their lawfulness under Article 8 of the European Convention of Human Rights ("**ECHR**").[7] The Committee also heard concerns about the safe-

[3] Explanatory Notes, p12; Human Rights Memorandum, p12
[4] ibid
[5] Data Protection and Digital Information Bill, Public Bill Committee, PBC (Bill 265) 2022 – 2023, Fifth sitting, 18 May 2023, Col 177
[6] Data Protection and Digital Information Bill, Public Bill Committee, PBC (Bill 265) 2022 – 2023, Fourth Sitting 16 May 2023, Col 171
[7] Data Protection and Digital Information Bill, Public Bill Committee, PBC (Bill 265) 2022 – 2023, Second Sitting 10 May 2023, Col 70 onwards

guards and oversight available in the provisions, considering but voting down an amendment to Clause 29 to increase the oversight of the Information Commissioner over designation notices (to make them subject to an application to, rather than just consultation of, the Information Commissioner, tabled by Stephanie Peacock MP).[8]

Purpose of the current Part 3 regime within DPA 2018

22. It is helpful to consider why the Part 3 national security exemptions are different in the first place. During the passing of the DPA 2018, the different regimes in Part 2, Part 3 and Part 4 were justified because general purpose processing, law enforcement processing, and intelligence services data processing were "*three very different situations*."[9]

23. National security exemptions for law enforcement, tighter than those available to general processors, were described as being "*carefully constructed*". The Government stated these carefully constructed provisions would "*ensure that investigations, prosecutions and public safety are not compromised*" while ensuring "*[p]eople will always have the right to ensure that the data held about them is fair and accurate, and consistent with the data protection principles*."[10]

24. The Government also highlighted the importance of maintaining consistency and transnational interoperability with law enforcement agencies and judicial cooperation in criminal matters when it introduced Part 3 in the 2018 Act, which implemented the EU Law Enforcement Directive 2016/680. "*The Bill does not just implement the recent directive on law enforcement data protection; it ensures that there is a single domestic and transnational regime for the processing of personal data for law enforcement purposes across the whole of the law enforcement sector.*"[11]

25. This reflected the purpose of the Directive, which was to ensure "*a consistent and high level of protection of the personal data of natural persons and [to] facilitate[e] the exchange of personal data between competent authorities of Members States [which] is crucial in order to ensure effective judicial cooperation in criminal matters and police cooperation*."[12]

[8] Data Protection and Digital Information Bill, Public Bill Committee, PBC (Bill 265) 2022 – 2023, Fifth sitting, 18 May 2023, Col 177
[9] Lord Ashton of Hyde (Parliamentary Under-Secretary of State, Department for Digital, Culture, Media and Sport), Data Protection Bill, Lords second reading (10 Oct 2017), Vol 785 Col 125
[10] Ibid, Col 126
[11] ibid
[12] EU Law Enforcement Directive 2016/680, recital 7

JUSTICE's analysis and concerns

9. JUSTICE does not dispute the need for necessary and proportionate interference with privacy for the purposes of national security. Protecting national security is of clear importance, is a core function of the State, and is an established legitimate derogation of the right to privacy under Article 8 ECHR. Whilst the majority of law enforcement data processing will not concern national security, some might, and necessary and proportionate exemptions should exist.

10. However, that has long been the case, and certainly was when the law enforcement processing regime in Part 3 DPA 2018 was introduced. That regime was "*carefully constructed*", and allows for significant derogations from data rights, such as the right to information and access. This was deemed proportionate to the need for law enforcement to be able to process data when national security was involved, with a reduced level of transparency to the data subject, whilst maintaining a high standard of data protection.

11. This Bill significantly undermines the high standards set by that 2018 regime just 6 years ago. While that regime sought to, understandably, limit transparency to the data subject, these Clauses will impact obligations and principles which will apply to that data subject's data processing behind closed doors. It marks a significant departure, therefore, from the high standards of data protection required of law enforcement in the processing of personal data of witnesses, victims and suspects.

Illustration of impact

A victim may be trafficked by a group who are a suspected national security threat. Currently, a competent authority processing for law enforcement purposes, eg a police force, could restrict the victim's data rights such as her right to be informed and to access her data, if necessary and proportionate to safeguard national security. ***Behind closed doors, however, police would still currently have to abide by the data protection principles and make sure her data is limited, accurate, etc.***

However, clause 28 would mean none of the principles except lawfulness would apply, if the police force, or a Minister of the Crown in an exemption notice, considered it was "required" to safeguard national security. This would mean:

- *It would relieve them from the obligation to ensure her data is accurate;*
- *They would not have to ensure her data was processed for a specified, explicit and legitimate purpose; or that it was adequate, relevant and not excessive;*

- *They could make decisions about her using solely automated methods, with no meaningful human intervention, and there would not need to be any notice, opportunity for human intervention or opportunity to contest the decision; and*
- *They could even falsify her data or conceal it with immunity (usually a statutory offence).*

Notwithstanding the above, other obligations on police forces still apply currently – for example the obligations to have data protection officers, conduct impact assessments, and consult the Information Commissioner in relation to any high-risk filing system. However, if the police force were to be subject to a designation notice under clauses 29 and 30, these obligations would be removed.

Finally, the burden of holding the executive to account in both scenarios would be on the victim herself. *It would be extremely difficult to know whether she had, in fact, been affected by the provisions since they exempt forces from having to provide information to her. Nevertheless, the only avenue of independent scrutiny would be an appeal by her; there would be no pre-emptory oversight of the national security exemption and the Information Commissioner has a consultation role only with respect to the joint process designation notice.*

Recommendations

12. Given these significant changes, JUSTICE is concerned that the justifications for clauses 28-30 thus far has been brief and inadequate. More is needed to understand:
    1) firstly whether these new provisions are indeed necessary; and
    2) secondly, if they are, whether they are proportionate, or whether the impact on the rights of the data subject could be reduced while maintaining the national security protections.
13. In this light, JUSTICE supported the amendments of Lord Clement-Jones at 135A-135E. These amendments probe the Government's position by proposing the following:
    1) Putting "proportionality" back in to clause 28;
    2) Restricting the broad range of exemptions being introduced in clause 28 by putting the principles back in;
    3) Introducing pre-emptory oversight by a judicial commissioner for Clause 28 certificates.

4) Increasing the pre-emptory oversight of the information commissioner for designation notices at Clause 29, making his approval mandatory (as tabled by Stephanie Peacock MP in public bill committee but voted down)

1) Putting proportionality back in

14. At a minimum, JUSTICE would support amendments which probe the deletion of the word "proportionality".

15. In any event, even if the Bill were to pass in its current state, JUSTICE would consider the proper interpretation of the word "required" to be "necessary and proportionate", given the obligation for public authorities to interpret their obligations consistently with human rights law. Nevertheless, JUSTICE is concerned by the change in wording and the deletion of the word "proportionality" from the test. Indeed, if Parliament were to sanction this, there is a real risk that it would give police forces and other law enforcement agencies the impression that there was no longer a need to be proportionate.

16. Putting proportionality back in would be achieved by Amendments 135A and 135D, as follows:

Amendment 135A

Clause 28, page 48, line 35, leave out "required" and insert "necessary and proportionate"

Explanatory statement

This amendment would ensure that "proportionality" continues to be considered by competent authorities when they are deciding whether national security exemptions apply to their processing for the purposes of law enforcement.

Amendment 135D

Clause 28, page 49, line 41, leave out "required" and insert "necessary and proportionate"

Explanatory statement

This amendment would ensure that "proportionality" continues to be considered by Ministers of the Crown when they are deciding whether to issue a national security certificate for the purposes of law enforcement.

2) Putting the principles back in

17. JUSTICE considers the most notable expansion of the national security exemptions is the ability to exempt from the fundamental data protection principles, except for lawfullness. This is contrary to the assurances of Government to Parliament during the passage of the DPA 2018, when referring to Part 3 rules for law enforcement: "*[p]eople will always have the right to ensure that the data held about them is fair and accurate, and consistent with the data protection principles*."[13]

18. Relevant too is whether disapplication of principles will affect consistency and transnational interoperability with law enforcement agencies and judicial cooperation in criminal matters with the EU and its member states. Part 3 implemented the Law Enforcement Directive to ensure international consistency and cooperation, and therefore to disapply data protection principles may risk such effective cooperation.

19. JUSTICE therefore supports the probing amendment 135B:

Amendment 135B

Clause 28, page 48, line 37, leave out lines 37 and 38

Explanatory statement

This amendment probes why competent authorities need to be able to disapply the data protection principles for the purposes of safeguarding national security, given the assurances given during the Data Protection Act 2018 by Government that data held by law enforcement would always abide by the data protection principles.

3) Pre-emptory oversight by a judicial commissioner for Clause 28 certificates

20. During the DPA 2018's Parliamentary passage, there was much debate over the Part 2 national security exemption for general processing at section 26, and the national security certificates at section 27. MPs and Peers expressed concern about the transparency of

[13] Lord Ashton of Hyde (Parliamentary Under-Secretary of State, Department for Digital, Culture, Media and Sport), Data Protection Bill, Lords second reading (10 Oct 2017), Vol 785 Col 126

national security certificates (some are available online but there is no obligation to publish them) and the difficultly of an individual knowing whether they were directly affected.[14]

21. A new judicial commissioner role was suggested in the Lords, supported in Committee by Lord Clement-Jones and Lord Paddick and at Report Stage by Baroness Hamwee and Lord Paddick, however neither were moved to a vote. This was a pre-emptory judicial oversight role, rather than an *ex post facto* appeal, inspired by the judicial commissioner role which exists in the different but not altogether dissimilar context of investigatory powers. The amendments in Public Bill Committee in the Commons[15] mirrored those in the Lords, but were voted down.

22. A Judicial Commissioner role could provide much needed pre-emptory oversight, given Ministers of the Crown would be able to issue a national security certificate over a far broader array of data protection rights and obligations than currently, and the certificate could simply state they are "all" necessary exemptions with no further specification or description. This increased power could be argued to require increased scrutiny.

23. Therefore JUSTICE supports consideration of the judicial commissioner role again, as would be achieved by amendment 135C.

Amendment 135C

Clause 28, page 49, line 35, leave out subsection 8 and insert –

(8) Omit section 79 (national security certificate) and insert -

"**79A National Security: Certificate**

(1) A Minister of the Crown must apply to a Judicial Commissioner for a certificate if exemptions are sought under section 78A(2) from the specified provisions in relation to any personal data for the purpose of safeguarding national security.

(2) The decision to issue the certificate must be approved by a Judicial Commissioner.

(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—

[14] See Col 2048 at https://hansard.parliament.uk/lords/2017-11-15/debates/9DC4D211-3573-4D97-82DB-92B75547B506/DataProtectionBill(HL)# Amendments paper here: https://publications.parliament.uk/pa/bills/lbill/2017-2019/0066/18066-IV.pdf

[15] Debated at fourth sitting on 15 March 2018, PBC (Bill 153) 2017 – 2019 Cols 107-132 at https://publications.parliament.uk/pa/cm201719/cmpublic/DataProtection/PBC153_Combined_1-8_22_03_2018_REV.pdf amendment paper 161-169 here: https://publications.parliament.uk/pa/bills/cbill/2017-2019/0153/amend/data_rm_pbc_0313_Copy.pdf

(a) whether the certificate is necessary, and

(b) whether the conduct that would be authorised by the certificate is proportionate, and

(c) whether it is necessary and proportionate to exempt all of the provisions specified in the certificate.

(4) An application for a certificate under subsection (1)—

(a) must identify the personal data to which it applies by means of a general description, and

(b) may be expressed to have prospective effect.

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

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

(7) Any person who believes they are directly affected by a certificate under subsection (1) may appeal to the Tribunal against the certificate.

(8) If, on an appeal under subsection (7), the Tribunal finds that it was not necessary or proportionate to issue the certificate, the Tribunal may—

(a) allow the appeal, and

(b) quash the certificate.

(9) The power to apply for a certificate under subsection (1) 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."

Explanatory statement

This amendment seeks to introduce pre-emptory independent oversight of national security certificates from a judicial commissioner, given the far increased scope of data rights, principles and obligations from which competent authorities can be exempted in national security certificates under Clause 28.

4) *Pre-emptory oversight of the information commissioner for designation notices at Clause 29*

24. During Committee Stage of this Bill, Stephanie Peacock MP sought to improve the pre-emptory oversight of the Information Commissioner before the joint processing designation notices are issued. Her amendment sought to change the duty to consult the Information Commissioner in Clause 29 to an obligation to apply to him for permission.

25. JUSTICE supports Peers' consideration of this amendment.

Amendment 135E

Clause 29, page 52, line 23, leave out "must consult the Commissioner" and insert "must apply to the Commissioner for authorisation of the designation notice on the grounds that it satisfies subsection (1)(b)."

Explanatory statement

This amendment seeks to increase independent oversight of designation notices by replacing the requirement to consult the Commissioner with a requirement to seek approval of the Commissioner.