Data (Use and Access) Bill

House of Commons, Committee Stage

5 March 2025

Introduction

1. JUSTICE is a cross-party law reform and human rights organisation working to make the justice system fairer for all. 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. This briefing addresses the Data (Use and Access) Bill ("**the Bill**") at Committee Stage in the House of Commons.

3. This briefing is informed by JUSTICE's long history of considering the protection of fundamental rights and freedoms in the use of data throughout the justice system, in addition to its current workstream, "AI, human rights and the law" and its recently published report in January 2025: *AI in our justice system*.

Summary

4. At a time when the Government wants to "turbocharge" AI and "mainline AI into the veins of the nation",[1] there has never been a more critical time to safeguard the building blocks of AI: **data**.

5. **However, several aspects in the Bill weaken, rather than strengthen, data protection and the protection of fundamental rights and freedoms in the UK.** JUSTICE is troubled that the Bill does so when the future AI policy and legislative landscape, including the contents of a future AI Bill promised in the King's Speech, are unclear. As Baroness Kidron remarked: "*this Bill is flying blind*".[2]

[1] Press release, Prime Minister sets out blueprint to turbocharge AI, 12 January 2025

[2] Data (Use and Access) Bill. House of Lords, Report Stage Day 1, Volume 842, Column 1603, Tuesday 21 January 2025

6. As a preliminary matter, therefore, JUSTICE questions why the Government insists on pursuing data protection reforms which weaken the protection of individual rights while on the cusp of potentially transformative – but as yet unclear beyond high level strategy – AI policies.

7. JUSTICE further supports scrutiny of the following issues in the Commons:

   (a) The ill-conceived new category of "recognised legitimate interests" (Clause 70)

   (b) Weaking protections from automated decision making (Clause 80)

   (c) Unaddressed inadequacies in human rights protections when private companies process data.

   (d) Weakening data protections when police process data in the context of national security (Clauses 87-89)

Recognised legitimate interests – Clause 70

8. Clause 70 of the Bill introduces a new category of lawful data processing "*recognised legitimate interests*" ("**RLIs**"). The list of RLIs, at Schedule 4 of the Bill, includes the prevention of crime, emergencies, and safeguarding vulnerable individuals.[3]

9. This is a significant change of law: currently data controllers can identify a "legitimate interest" to process data, such as a commercial interest,[4] however, they must take responsibility for considering i) whether the purpose is legitimate, ii) whether it is necessary, and iii) whether individual interests or fundamental rights and freedoms of the data subject – in particular where the data subject is a child – override the legitimate interest ("**the balancing test**").[5]

10. **The new RLIs would remove the explicit obligation on data controllers to consider and protect the rights of individuals, and particularly children.** The stated intention of the Government is that this

[3] The RLIs listed are largely similar to those in the previous Data Protection and Digital Information Bill, save for the removal of "democratic engagement" which included political campaigning.

[4] Because another lawfulness ground does not apply, i.e. it is not necessary to perform a public interest task or exercise of official authority; to protect a vital interest of a data subject; performance of a contract; performance of a legal obligation; or has been consented to by the individual. Article 6(1)(a)-(e) UK GDPR

[5] Article 6(1)(f) UK GDPR; Case C-13/16 *Rigas satiskme* EU:C:2017:336; Case C-708/18 *TK v Asociaţia de Proprietari bloc M5A-ScaraA* EU:C:2019:1064

will increase speed and confidence, and reduce confusion, when organisations are processing data for RLI purposes.[6]

Problems with Clause 70

11. JUSTICE considers this an ill-conceived provision, and a step in the wrong direction to ensure responsible, rights-compliant and trustworthy data processing.

    a. Firstly, it is unclear whether the provisions will in fact lead to any change of practice by data controllers on the ground. The new test for RLIs still requires processing to be "necessary". Where that engages individuals' and children's rights, JUSTICE considers any assessment will have to consider that necessity in light of individuals' rights and freedoms. At best, therefore, RLIs may do little speed up data controllers, but rather confuse them about their obligations to balance data subjects' rights.

    b. **The alternative is concerning: data controllers giving no case-by-case consideration to individuals' rights and freedoms.** JUSTICE is concerned that this will not only result in a reduction of responsible data processing, and therefore increased infringement of rights by data controllers, but also negatively impact levels of public trust.

    c. In the House of Lords, Peers expressed considerable concern at RLIs. In response, the Government tabled a concession amendment at Report, to include that the Secretary of State would have to consider that children "merit specific protection with regard to their personal data" when adding new RLIs to the list. However, this provision does not adequately alleviate concerns; rather it identifies why **removing responsibility from individual data controllers to consider the rights of children is a step in the wrong direction.**

Example: A shop owner wants to deter and prevent crime by installing several cameras outside their shop and livestreaming them on their website. The cameras capture a considerable area outside the shop, including overlooking a school playground. Under the new RLI provisions, the shop owner would no longer have to consider the particular rights and freedoms of the school children, including their right to privacy and freedom of expression.

[6] Data controllers' lack of confidence in conducting the "balancing test" was raised by consultees in the Department for Digital, Culture, Media & Sport's public consultation *Data: A New Direction* in 2021. See Government explanation of policy intention of the identical provisions as contained within the Data Protection and Digital Information Bill, House of Lords, Grand Committee, 2nd Day, Volume 837, Column 105GC, Monday 25 March 2024

d. **A further concern is the inclusion of a Henry VIII power: the Secretary of State can amend the list of RLIs by secondary legislation.** As explained by the Attorney-General, Lord Hermer KC: "excessive reliance on delegated powers … upsets the proper balance between Parliament and the executive. This not only strikes at the rule of law values … but also at the cardinal principles of accessibility and legal certainty".[7]

e. At Committee Stage in the House of Lords, Peers raised concern about this regulatory power, and the need for democratic debate of future categories.[8]

> *For example, the Government decides to add "work productivity" as an RLI, as being within the public economic interest of the UK. This allows employers to impose employee surveillance and monitoring measures, without them being in pursuance of a contract nor subject to consent. This would create a wholesale shift in the lawfulness of employee surveillance and monitoring, with negligible Parliamentary scrutiny.*

f. JUSTICE agrees with both the Constitution Committee and the Delegated Powers and Regulatory Reform Committee, which **assessed the power to be inappropriate and the case for it insufficiently made.**[9]

12. JUSTICE considers RLIs to be ill-conceived, disposing of the consideration of individuals' rights for speed and convenience. **JUSTICE therefore urges Members to oppose the Question that Clause 70 stand part of the Bill.**

13. **Should the clause stand part, JUSTICE supports Victoria Collins's Committee Stage amendment New Clause 5** which would slightly improve Parliament's ability to scrutinise changes or additions made to the RLIs when the Secretary of State exercises his delegated powers under clause 70.

---

[7] Attorney General's 2024 Bingham Lecture on the rule of law, 14 October 2024

[8] The Government has highlighted that future RLIs would have to be in line with public interest objectives as listed in Article 23(1) UK GDPR. (This requirement was not in the previous DPDI Bill under the last Government.) However, this list contains extremely broad categories, including a catch all objective: "other important objectives of general public interest, in particular an important economic or financial interest of the United Kingdom."

[9] House of Lords, *Delegated Powers and Regulatory Reform Committee,* 9th Report of Session 2024–25 Data (Use and Access) Bill HL Paper 49

Automated Decision Making – Clause 80

14. Currently, individuals have a right not to be subject to significant decisions based solely on automated processing of their personal data,[10] with certain specified exceptions.[11]

15. **Clause 80 repeals this right, in both the law enforcement and general processing contexts. It creates a new starting point: entirely automated decision making** ("ADM") **including profiling, is allowed.** Only ADM involving "special category data"[12] would continue to be prohibited.

16. ADM includes different forms of automation: it could be in accordance with a simple algorithm, which produces the same outputs for the same inputs, or it could be a more complex model, for example involving machine learning, which is capable of generating content, and can be commonly referred to as "artificial intelligence" ("**AI**"). **Legalising ADM paves the way for increased use of AI across all fields of personal data decision-making without human involvement.**

Problems with Clause 80

17. The Post Office/Horizon scandal is an ongoing reminder of what can go wrong when too much reliance is placed on machines, and the difficulties and power imbalances faced by individuals who challenge the reliance on those machines by powerful actors.

18. There are established risks with ADM and partially automated decision making of unfair, discriminatory and harmful decisions.

> *Examples:*
> *The Department for Work and Pensions has been using automated systems to detect welfare fraud. These systems have been revealed to often be wrong – last year, two-thirds of the claims flagged by a DWP automated system as potentially high risk were in fact legitimate.[13] Furthermore, an internal DWP "fairness analysis" has revealed bias according to according to people's age, disability, marital status and nationality, leading to a "statistically significant outcome disparity".[14] This has been criticised as a "hurt first, fix later" policy, impacting some of the most vulnerable in society.*

[10] Article 22 UK GDPR in relation to general processing, and ss. 49-50 Data Protection Act 2018 with respect to law enforcement processing.

[11] Exceptions are explicit consent; necessity for performance of a contract; or when authorised by a law which suitably protects the data subject's rights, freedoms and legitimate interests – Article 22, UK GDPR

[12] Personal data revealing racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data (used for identification purposes); data concerning health; data concerning a person's sex life; and data concerning a person's sexual orientation. Article 9 UK GDPR

[13] Robert Booth, 'DWP algorithm wrongly flags 200,000 people for possible fraud and error' (*The Guardian,* 23 June 2024)

[14] Robert Booth, 'Revealed: bias found in AI system used to detect UK benefits fraud' (*The Guardian* , 6 December 2024)

Amazon previously used a machine learning artificial intelligence tool to make recruitment decisions. The tool was supposed to be gender neutral and did not collect or process the sex of the applicant as a discrete data point. Despite this, it began discriminating on the basis of sex using proxy data points, perpetuating an existing disparity in the workforce, which was majority male.[15]

In the US criminal courts, an automated tool called COMPAS gives a score of "risk" of reoffending to inform sentencing. An investigation by non-profit news organisation, Propublica, found embedded racial discrimination in the tool: Black defendants were more likely than white defendants to receive a "false positive" from the tool, i.e. be incorrectly judged to be at a higher risk of recidivism, while white defendants were more likely than Black defendants to receive a false negative, i.e. be incorrectly flagged as low risk.[16]

19. The ECHR Impact Assessment of the Bill, which was updated in December 2024, recognises this potential for discriminatory effect in contravention of human rights law:

> *It is acknowledged that AI systems are capable of reproducing and augmenting the patterns of discriminatory treatment that exist in society. [...] [T]here is a risk that the increase in scope of Article 22 processing could potentially lead to discrimination under Article 14 [read with Article 8*".[17]

20. In light of these clear risks, the Bill proposes several **safeguards**.[18] Controllers must:
    a. provide information of the decision,
    b. enable individuals to make representations,
    c. enable individuals to obtain human intervention, and
    d. enable individuals to contest decisions.

21. **JUSTICE considers these safeguards to be inadequate, for 3 reasons**:
    a. **They shift the burden to the individual.** Instead of an onus on the data controller to prevent harm to the individual, the burden is shifted on the individual to complain if the ADM they have been subject to is unfair, discriminatory or even unsafe. This is insufficient, since

[15] See original Reuters report as archived by the Irish Times: Jeffrey Dastin, "Amazon scraps secret AI recruiting tool that showed bias against women". (*Reuters,* 2018)

[16] See Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, 'Machine Bias' and 'How we analysed the COMPAS recidivism algorithm', *Propublica* (23 May 2016).

[17] Data (Use and Access) Bill: European Convention on Human Rights Memorandum 6 February 2025, para 83

[18] To be inserted by Clause 80: Articles 22A – 22D UK GDPR for general processing; ss. 50A – 50D Data Protection Act 2018

people may not complain due to lack of knowledge, confidence, intimidation, and various other intersecting vulnerabilities.

b. **There is no obligation to provide any safeguards before the decision is made.** The Bill does not require information to be given or any opportunity for representations to be given ***prior*** to a decision. This not only offends the core principles of fair decision-making - the right to advance notice and representations[19] - it also means that there are no protections against harm being incurred before an individual knows about it.

c. **The Secretary of State has delegated powers to vary the safeguards by regulations**. She can also state conclusively what does or does not satisfy them.[20] These are broad powers which allow for significant policy decisions which could undermine the safeguards in practice. JUSTICE repeats its concerns regarding overuse of delegated powers, as discussed at paragraph 11(d) above with regard to RLIs.

22. JUSTICE agrees with Lord Clement-Jones in his assessment of Clause 80:

> *the Bill significantly weakens safeguards around ADM, creates legal uncertainty due to vague definitions, increases the risk of discrimination, and limits transparency and redress for individuals—ultimately undermining public trust in the use of these technologies.*[21]

23. Furthermore, in light of the Government's intent to and "mainline AI into the veins of the nation",[22] including the public sector, JUSTICE has significant concerns that Clause 80 will lead to a vast proliferation of unfair, discriminatory decision making across society.

24. **JUSTICE therefore urges Members to oppose the Question that Clause 80 stand part of the Bill.**

25. **JUSTICE also encourages calls for more transparency and accountability for ADM, rather than less. As such, JUSTICE supports Victoria Collins's Committee Stage amendments as follows:**
    a. **New Clause 1** which requires notice on a public register of decisions made using ADM in whole or in part; meaningful and personalised explanations for individuals affected; and monitoring, evaluation and auditing of processes and outcomes.
    b. **New Clause 4** which requires a public register for ADM and other semi-automated systems used to make or materially influence important decisions about individuals.

---

[19] *The duty to give advance notice and an opportunity to be heard to a person against whom a draconian statutory power is to be exercised is one of the oldest principles of what would now be called public law*. *Bank Mellat v HM Treasury* [2013] UKSC 39 at §29

[20] Draft Article 22D in Clause 80

[21] Data (Use and Access) Bill. House of Lords, Report Stage Day 1, Volume 842, Column 1680, Tuesday 21 January 2025

[22] Press release, Prime Minister sets out blueprint to turbocharge AI, 12 January 2025

c. New Clause 5 which would slightly improve Parliament's ability to scrutinise changes or additions made to ADM safeguards when the Secretary of State exercises his delegated powers under clause 80.

d. New Clause 7 which creates a new right for data subjects to demand more information about the factors influencing the outcomes of high-risk AI decisions, as well as requiring the Secretary of State to define the criteria and thresholds for 'high-risk AI decisions'.

Human rights and private actors

26. As quoted above, the ECHR memorandum for the Bill acknowledges the discriminatory treatment which can be perpetuated by AI systems, and the likelihood that ADM use will increase across society. However, the ECHR memorandum for the Bill goes on to dispute the relevance of such human rights issues when private actors are using ADM:

> *the additional processing by private bodies will generally not raise ECHR concerns, because Article 8 ECHR will not be engaged because the controller is not an emanation of the State*.[23]

27. This is in reference to s.6 of the Human Rights Act 1998, which only makes it "*It is unlawful for* ***a public authority*** *to act in a way which is incompatible with a Convention right*." (Emphasis added.)

28. In the House of Lords, Lord Thomas and Lord Clement-Jones expressed concerns about the abuse of human rights by private data controllers falling outside the scope of data protection law, as a result of post-Brexit changes to UK GDPR. The result of these changes is that the phrase "fundamental rights and freedoms" – which occurs often in the UK GDPR – no longer refers to the EU Charter of Fundamental Rights, but instead now is a reference to the ECHR and the Human Rights Act 1998.[24] While the two human rights instruments contain many similar provisions, data protection experts have noted the EU Charter has been applied horizontally to private bodies in a way the ECHR does not.[25]

---

[23] ECHR Memorandum, para 84

[24] The Data Protection (Fundamental Rights and Freedoms) (Amendment) Regulations 2023 stipulate that "references [within the UK GDPR] to fundamental rights or fundamental freedoms (however expressed) are to the Convention rights within the meaning of the Human Rights Act 1998" para 2(3).

[25] Eleonor Duhs, Partner & Head of Data and Privacy, Bates Wells, The Data (Use and Access) Bill – areas of risk to the continued free flow of data from the EU to the UK, "CJEU case law has confirmed that the consideration of the data subject's rights and freedoms required the (private sector) controller".

29. The risk of this apparent reduction of protection, and the interpretation given by the ECHR memorandum, is that human rights and freedoms are less protected now than they were previously when private bodies are processing personal data.

> *For example, a shopping mall installs live facial recognition technology. The cameras overlook the entrance to the community centre, where several groups gather to discuss a range of religious and political matters, and several protests take place throughout the year. This engages not just the right to privacy (Article 8) of individuals, but also their freedom of assembly, freedom of conscience and religion, and freedom of expression (Articles 9-11). While the shopping mall would have to conduct a data protection impact assessment which considers the risk to "fundamental rights and freedoms," the implication of the ECHR memorandum suggests that that assessment may not, in fact, have to consider those ECHR concerns because the controller is not an emanation of the state.*

30. The response from the Minister Baroness Jones of Whitchurch thereafter contradicted the ECHR Memorandum:

> *The Human Rights Act requires legislation to be interpreted compatibly with convention rights, whether processing is carried out by public or private bodies. ECHR rights are therefore a pervasive aspect of the rules that apply to public and private controllers alike.*[26]

31. This brief statement seemingly contradicts the ECHR memorandum and JUSTICE is concerned at this confusion in such an important area.

32. JUSTICE therefore encourages Members to request clarification of the seemingly mixed messages given by the ECHR memorandum to the Bill and by the Government, as quoted above, regarding the responsibilities of private actors for protecting human rights of data subjects. To do so, JUSTICE recommends a similar amendment to that of Lord Thomas (not moved) at Grand Committee in the House of Lords:

> *"Application of the European Convention on Human Rights to the processing of personal data by private bodies*
>
> *(1) Where personal data is processed by any private body not subject to the obligations under the European Convention on Human Rights as enacted by the Human Rights Act 1998, that private body is to be treated as subject to the obligations under the Convention*

[26] Day 3 Grand Committee, House of Lords, Volume 842, Column 4GC 16th December 2024

as if it were a public authority and must ensure that such processing is not incompatible with a Convention right.

(2) If a private body fails to ensure that the processing of personal data is in accordance with subsection (1), the private body is liable to any person whose rights under the Convention are infringed as if it were a public authority."[27]

33. JUSTICE also notes that the change from the EU Charter to the ECHR may have impacted the UK's data adequacy, and therefore supports Victoria Collins's New Clause 2 amendment, which would require the Secretary of State to carry out an assessment of the likely impact of this Act on EU data adequacy decisions.

National security exemptions for law enforcement (Clauses 88-90)

34. Clauses 88-90 weaken the data protection obligations binding law enforcement authorities when processing data in circumstances of national security,[28] matching those which are already available to intelligence services.[29] These amendments include:

    a. **Removing the requirement for "proportionality":** Previously, for a national security exemption to apply, it would have to be "necessary and proportionate" to protect national security. The Bill proposes to replace this with "when required to safeguard national security".

    b. **Expanding the number of rights and obligations open to exemption**: Currently only four rights are capable of being restricted by law enforcement when necessary and proportionate to protect national security.[30] They are:

        (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.

[27] Amendment 72, debated Day 2 Grand Committee, House of Lords, Volume 841, Column 452GC 10th December 2024

[28] In Part 3 of the Data Protection Act 2018 ("**DPA 2018**")

[29] In Part 4 of the DPA 2018

[30] Ss 44(4), 45(4), 48(3) & 68(7) DPA 2018

Under clause 88, law enforcement authorities would be exempted from a vastly broader range of obligations, including:

(i) Compliance with the six data protection principles, except for lawfulness;

(ii) Compliance with new ADM safeguards (provided for in Clause 80);

(iii) Several oversight mechanisms of the Information Commissioner, including inspection powers and enforcement notices;

(iv) Liability for statutory data offences, including unlawful obtaining and selling of data, and the offence of altering, destroying or concealing information to prevent it being disclosed to the data subject. These offences already have statutory defences of the prevention of crime or acting in the public interest.

c. Broadening national security certificates: Certificates would permit wholesale exemption from *all* the eligible rights and obligations permitted by way of national security certificates, rather than certificates specifying which exemptions apply.

d. A new joint processing regime: Designation notices made by a Minister of the Crown would empower law enforcement and intelligence services to jointly process personal data. This removes several requirements, including

(i) data protection officers to be designated;

(ii) logging and records of processing activities;

(iii) data protection impact assessments;

(iv) consultation with the Commissioner in the creation of high risk filing systems.

An appeal would lie to the tribunal by a person who is directly affected by the notice if there were no reasonable grounds to issue it.

Problems with Clauses 88-90

35. JUSTICE does not dispute the need for necessary and proportionate interference with privacy for the purposes of national security. Protecting national security is a core function of the State, and is an established legitimate derogation of the right to privacy under Article 8 ECHR. In particular, the need to reduce the data subject's access rights is clear within a national security context.

36. However, that has long been the case and is secured by the current regime under the Data Protection Act 2018 ("DPA 2018"). This regime ensures there are derogations from data subjects rights, for example the right of access. But critically, behind closed doors, police still currently have to abide by the data protection principles and make sure data processing is limited, accurate, etc. In 2018 these provisions were described as being "*carefully constructed*" [...to] "*ensure that investigations, prosecutions and public safety are not compromised*" while also 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.*"[31]

37. However, under the new regime proposed by clauses 88-90, law enforcement would be able to go much further in allowing derogation from fundamental data protection principles (except lawfulness) and other broader derogations.

> *Example: a woman is being investigated as part of a group suspected of a national security threat. She faces suspicion over her alignment with their terrorist ideology, but she maintains she has been a victim of abuse and trafficking. Under a Clause 88 exemption, law enforcement authorities:*
>
> a. *would not have to ensure her data is accurate;*
>
> b. *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;*
>
> c. *could make decision about her, and profile her, using automation, without providing safeguards; and*
>
> d. *could even falsify her data or conceal it with immunity (usually a statutory offence).*
>
> *The woman would furthermore have no right of information about whether she was subject to an exemption or not. However, the burden of holding law enforcement to account is on her, since the only avenue of independent oversight would be an appeal by her.*

38. JUSTICE is concerned that the justifications for clauses 88-90 thus far have been brief and inadequate.

[31] Data Protection Bill, Lords second reading (10 Oct 2017), Volume 785 Column 126

39. JUSTICE supports the New Clause 8 amendment from Victoria Collins, which would provide enhanced oversight from the Commissioner over data sharing between law enforcement and intelligence services, if such oversight would cover the new joint data processing provisions at Clause 89. However, such this would not improve the oversight of national security exemptions under clause 88, as in the above example.

40. JUSTICE therefore encourages further amendments to better understand whether these new provisions are indeed necessary, and if so whether the impact on data quality could be reduced while maintaining the national security protections.

41. For example JUSTICE requests Committee members consider tabling the following three amendments:

Amendment: *Clause 88, page 107, line 8, leave out paragraph (a)*

Explanation: This amendment would not allow law enforcement to be exempted from processing data in accordance with all the data protection principles, even in national security contexts.

Amendment: *Clause 88, page 107, line 26, leave out sub-paragraph (ii)*

Explanation: This amendment would not allow law enforcement to be exempted from criminal offences related to personal data even in national security contexts, including unlawful obtaining and selling of data, and the offence of altering, destroying or concealing information to prevent it being disclosed to the data subject.

Amendment: *Clause 88, page 108, line 5, 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—

(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."

Explanation: 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 law enforcement can be exempted under Clause 88.

For more information, please contact:

Ellen Lefley, JUSTICE – elefley@justice.org.uk