**Rights & Security International's briefing on clauses 26-28 of the Data Protection and Digital Information (No. 2) Bill**

**Report Stage, House of Commons, November 2023**

## Summary


- Clauses 26-28 (previously clauses 24-26) of the Bill, if enacted, would give the Home Secretary great and unaccountable powers to authorise the police to violate our privacy rights, through the use of 'national security certificates' and 'designation notices'.

- Under the European Convention on Human Rights (ECHR), the UK government must ensure that everything it does, including in the name of national security, complies with human rights laws. This means it must make sure that any time it interferes with the privacy of people in the UK, it obeys the law, has a goal that is legitimate in a democratic society, and only does what is truly necessary to achieving that goal.

- We argue that as currently drafted, clauses 26-28 fall foul of the UK's obligations under the ECHR because they give the Home Secretary discretion that is too broad, and because they do not create sufficient safeguards to prevent their misuse. Under the case law of the European Court of Human Rights, laws that give unfettered or overly broad discretion to the government to interfere with privacy will violate the Convention because the laws must be sufficiently specific to prevent abuses of power. The Court has repeatedly stressed that this is what the 'rule of law' means and that it is an essential principle of democracy.

- Despite multiple requests from MPs and RSI, the government has also failed to explain why it believes these clauses are necessary to safeguarding national security. So far, it has only explained why these new powers would be 'helpful' or would ensure greater 'efficiency' – but those justifications do not meet the standard the ECHR requires when the government wants to interfere with our privacy. The government is not entitled to do anything it finds 'helpful'.


## Clauses 26-28

1. Clauses 26-28 (previously clauses 24-26) of the Bill would give the Home Secretary great and unaccountable powers to authorise the police to violate our privacy rights. The Bill would do this through two means: a shift in what the Home Secretary can do by using 'national security certificates', and a new regime of 'designation notices'.

2. Under clause 26(7), the Home Secretary would be able to issue a 'national security certificate' to tell the police they do not need to comply with many important data protection laws and rules that they would otherwise have to obey. For instance, a 'national security certificate' would give the police immunity when they commit crimes by using personal data illegally – and it would also exempt them from certain provisions of the Freedom of Information Act 2000.

3. The Bill would also expand what counts as an 'intelligence service' for the purposes of data protection law, again at the Home Secretary's wish. Clause 27 would allows the Home Secretary to issue a

'designation notice' allowing law enforcement bodies to take advantage of the more relaxed rules in the Data Protection Act 2018 otherwise designed for the intelligence agencies, whenever they are collaborating with the security services.

4. Both the amended approach to 'national security certificates' and the new 'designation notice' regime would be unaccountable: the courts would not be able to review what the government is doing, and therefore Parliament might never find out.

5. National security certificates are unchallengeable before the courts, meaning that the police and the Home Secretary would be unaccountable if they abused these powers. If the Home Secretary says that the police need to use these increased – and unnecessary – powers 'in relation to' national security, then his word will be final. This includes the power to commit crimes.

6. Designation notices are also a power grab. The Home Secretary is responsible for approving and reviewing their use. Only a person who is 'directly affected' by a designation notice will be able to challenge it – yet the Home Secretary would have the power to keep the notice secret. In which case, how could anybody know that the police have been snooping on their lives under this law?[1]

**Setting up a lengthy court battle**

7. Clauses 26-28 could violate UK's obligations under the Human Rights Act 1998 and the European Convention on Human Rights (ECHR), including because they remove the courts' role in reviewing how the government uses its surveillance powers. The European Court of Human Rights has ruled in the past that large aspects of the law previously governing the UK's surveillance powers were unlawful because they gave the government too much discretion,[2] and because they lacked important safeguards to prevent misuse.[3] Clauses 26-28 could be challenged on similar grounds, and the Court has shown that it is willing to rule on these issues. These weaknesses in the law could also harm important relationships the UK has with the EU around data.[4]

8. Under the ECHR, the government must ensure that everything it does, including in the name of national security, complies with human rights laws. This means it must make sure that anytime it interferes with the privacy of people in the UK, it obeys the law, has a legitimate goal and only does what is truly necessary to achieving that goal. As we explain below, the government has not shown why limiting our rights would be necessary and the least intrusive option. Instead, it has talked about convenience – but it is not allowed to cut out the courts and Parliament, and let police commit crimes, simply because it thinks this is 'efficient'.[5]

[1] The courts have sometimes allowed 'general challenges' to powers such as these by a person who may have been subject to surveillance; however, most individuals will not be in a practical position to bring such challenges, and there would also be legal hurdles.
[2] App. No. 58243/00, *Liberty and others v. the United Kingdom*, 1 July 2008.
[3] App. No. 58243/00, *Liberty and others v. the United Kingdom*, 1 July 2008; App. Nos. 58170/13, 62322/14 and 24960/15, *Big Brother Watch and others v. the United Kingdom*, 25 May 2021.
[4] See Thomas Macaulay, 'New plans for a GDPR replacement have divided Britain's tech sector' (*TNW*, 13 March 2023).
[5] See, e.g. App. No. 47173/06, *Zakharov v. Russia*, 4 December 2015, paras. 229-232; App. No. 8691/79, *Malone v. the United Kingdom*, 2 August 1984, para. 68. For a summary, see European Court of Human Rights, 'Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence' (31 August 2022), paras. 612-631.

**The government has failed to explain why these powers are necessary**

9. Under the ECHR, for any government interference with our privacy in the name of national security or detecting crime to be lawful, it must be necessary to meet the goal – and this is a high standard.[6] The standard is high because secret surveillance and other secret access to our data threaten to tip the balance of power between ordinary people and the state in a manner that can be dangerous to the directly affected people and to democratic society as a whole.[7] The government and the police should not be interfering in our private lives just because it makes their jobs easier.

10. The government argues that the clauses create a 'simplified' legal framework that would improve the 'efficiency' of police operations when working with intelligence services. However, this is far from meeting the 'necessity' standard under the ECHR. The European Court would require the government to provide sufficient information to demonstrate why its surveillance regime is *necessary*, as opposed to merely convenient. UK courts should be using similar standards under the Human Rights Act.

11. Despite repeated requests from MPs and by RSI, the government has failed to explain why it thinks these powers will allow the police to protect national security – let alone why they are the least restrictive option. In particular, it has not explained why other possible reforms, such as better training and clearer frameworks for data storage and use, would not be viable alternatives. Without such explanations, the only conclusion is that clauses 26-28 must be removed from the Bill.

12. The government has sought to justify clauses 26-28 on the grounds that they would aid operational efficiency.[8] Law enforcement agencies, such as the Metropolitan Police and the National Crime Agency, have also supported clauses 26-28 on these grounds. Helen Hitching, Deputy Director of the Chief Data Office at the National Crime Agency, gave evidence to this effect before the Public Bill Committee:

> *'[Clauses 26-28] brings in the ability to put the [law enforcement] data protection framework on the same level [as the intelligence services], so we can share data in an easier fashion and make it less complex'.*[9]

13. Aimee Reed, Director of Data at the Metropolitan Police, also gave evidence to this effect before the Public Bill Committee:

> *'We are retaining the very different sections of the Act under which different organisations operate, and the sections that look to improve joint working across part 3 and part 4 agencies are very welcome… In essence, it is going to get simpler and easier to share data…'*[10]

[6] App. Nos. 30562/04 and 30566/04, *S and Marper v. the United Kingdom*, Judgment, 4 December 2008, paras 101-104. Judgment, 25 February 1997, para. 94; App. No. 37138/14, *Szabó and Vissy v. Hungary*, Judgment, 12 January 2016, paras. 67, 72-73.
[7] See e.g. App. No. 5029/71, *Klass and others v. Germany*, 6 September 1978, paras. 32-33.
[8] Hansard, Data Protection and Digital Information (No.2) Bill, Wednesday 8 March 2023, Col 729
[9] Hansard, Data Protection and Digital Information (No.2) Bill (Second sitting), 10 May 2023, Col 57.
[10] Hansard, Data Protection and Digital Information (No.2) Bill (Second sitting), 10 May 2023, Col 57.

14. 'Efficiency' is not the same as 'necessity'. The government should not be allowing the police to use our personal data without accountability, just because it makes their jobs easier. There are other, less intrusive, reforms that could make the police more efficient. As RSI told the Public Bill Committee:

> *'Looking through the Second Reading debate, the impact assessment and the European Convention on Human Rights analysis, there is no reference to anything that would be akin to necessity. It is all, "It would be easier for law enforcement to have these extra powers. It would be easier if law enforcement were potentially able to use people's personal data in more ways than they are at the moment." But that is not the necessity standard.'*[11]

15. Additionally, the government has frequently used the Fishmongers' Hall and Manchester Arena attacks to support the idea that clauses 26-28 are desirable.[12] However, inquiries have shown that a difference in data protection regimes was not the issue in either case. Instead, the problems centred around failures in offender management along with a lack of communication between intelligence services and local police.[13] The government has not explained how clauses 26-28 would have prevented either incident or why it thinks they are necessary to preventing whatever forms of violence the government regards as most likely to occur in the future.

16. Nor would the law restrict the use of these powers to counter-terrorism cases. The police would be able to exercise these powers in any context where the Home Secretary says that they are needed 'in relation to' national security. The Home Secretary gets to decide what 'national security' means, with no guidance or oversight.

17. The government has had sufficient opportunity to explain the rationale for these clauses, yet it has failed to do so. **For these reasons, we urge MPs to support amendments 226, 227 and 228. These will remove clauses 26-28 from the Bill.**

## About Rights & Security International

Rights & Security International is a London-based charity working to eliminate human rights abuses committed in the name of national security. We challenge religious, racial and gender bias in national security policies, and advocate for justice and transparency for victims of human rights abuses.

[11] Hansard, Data Protection and Digital Information (No.2) Bill (Second sitting), 10 May 2023, Cols 73-74.
[12] Hansard, Data Protection and Digital Information (No.2) Bill (Fourth sitting), 16 May 2023, Cols 171-172.
[13] Fishmongers' Hall Terror Attack Inquest: Regulation 28 Report on Action to Prevent Future Deaths, pp. 65 and 68; Manchester Arena Inquiry Volume 3: Radicalisation and Preventability, paras. 25.95-25.112.