INDEPENDENT REVIEWER OF TERRORISM LEGISLATION
INDEPENDENT REVIEWER OF STATE THREAT LEGISLATION

NOTE ON CRIME AND POLICING BILL: ACCESS TO REMOTELY STORED DATA UNDER NATIONAL SECURITY PORTS POWERS

1. The Second Reading of the Crime and Policing Bill is due on Thursday 16 October 2025, and the purpose of this Note is to draw attention to some important additional national security powers contained in the bill affecting access to 'cloud' data.

2. I apologise that I have not drawn Parliament's attention to this earlier. I understand that this topic has not been considered in earlier debates.

3. The relevant clause is clause 135 ('Extraction of online information: ports and border security'). Clause 135 falls within Part 10 ('Powers of Police etc') and belongs in the group of clauses 130-137 which relate to extraction of online information in both ordinary police and national security investigations.

4. Clause 135 is designed to amend Schedule 7 Terrorism Act 2000, and Schedule 3 Counter-Terrorism and Border Security Act 2019, which permit no-suspicion examination of persons and digital devices at UK ports and at the Northern Ireland border for the purpose of countering terrorism and hostile state activity respectively. At present, police can only examine and copy data held on devices such as mobile phones which the person 'has with him' (paragraphs 8, 11A(1)).

5. The effect of Clause 135 is to add a power for examining officers to extract information from online accounts, meaning access to information in the 'cloud' rather than information on devices. This considerably extends the volume of information to which examining officers may access, simply because an individual passes through a UK port or border.

6. The principal proposed limitation is that the online account must be accessible from the device seized under Schedule 7. However, this is not a huge restraint because, in principle, if a person accesses gmail from their phone, the entirety of their gmail account may be examined and copied; if their photos are synced with icloud, all their icloud photos may be examined and copied.

7. In these circumstances, Parliament may wish to consider, in relation to this proposed power:
    - What safeguards will prevent excessive data being extracted and copied?
    - How will journalistic and legally privileged material on an online account be protected?
    - Given the quantity of personal data which members of the public knowingly or unknowingly hold on the cloud, accessible from their devices, is merely travelling through a port or border a sufficient reason to surrender so much of their privacy?

JONATHAN HALL KC
13 October 2025