



21 December 2023

Lord Coaker
Lord Ponsonby of Shulbrede
Lord Fox of Oulton
House of Lords
London
SW1A 0PW

By email:

Investigatory Powers (Amendment) Bill: Lords Committee stage

Dear Vernon, Fred, and Christopher,

Thank you all for your valuable contributions at Committee stage of the Investigatory Powers (Amendment) Bill on 11th and 13th December. I am grateful for your considered and constructive scrutiny of the Bill. I am writing to set out more detail on the points on which I committed to write during the debates.

Definition of serious crime

Lord Coaker, asked about the definition of serious crime. The test for whether or not offending is 'serious' is not affected by whether the offender is 18 or 21 because the test is whether a theoretical offender of that age would receive a certain period of imprisonment (or a few other particular characteristics¹). This is to be expected, because the definition of serious crime is intended to distinguish between the seriousness of particular types of criminality, rather than to distinguish between particular types of offenders.

The involvement of under-18s in serious crime, if relevant, would be something that would be taken into account when considering the necessity and proportionality of the use of investigatory powers in relation to those individuals. There are also specific steps which must be taken regarding warrantry for use of the powers against those who are under 18, including more regular review of warrants to ensure that the necessity and proportionality case is still made out. Their age would also be taken into account if they were subsequently sentenced for any crime.

As mentioned in the debate, the differing nature of the age at which the serious crime threshold is met for England and Wales compared to Scotland and Northern Ireland relates

¹ In the definition at s263(1) of the Act, this includes if "conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose". For the definition at s86(2A), it also includes offences "which involve, as an integral part [of the offence], the sending of a communication or a breach of a person's privacy."

to the approach to adult sentencing for each Devolved Administration. The way the powers are utilised does not itself differ across the various home nations.

It is important to note that someone who is under the age of 18, or 21 for Scotland and Northern Ireland, could still be subject to the use of investigatory powers **if the necessity and proportionality case is made out**. The definition of “serious crime” at s263(1) applies for the use of all powers under the Act, and that definition is supplemented in relation to the acquisition of communications data in Part 3 of the Act by the definition set out in s86(2A). The definition applies to the sentence which could be given to a person over 18 (or 21 in Scotland and Northern Ireland) for a specific crime, not that the subject of the request is above that age.

Notices

Lord Ponsonby raised several points relating to the changes to the Notices regimes. Firstly, with regards to the review structure of notices, the notification requirement is not meant to be burdensome on operators. Unlike data retention, technical capability or national security notices, the notification notice does not facilitate the acquisition of data or require the operator to make technical changes. The existing review mechanism is an important and proportionate safeguard for these inherently different notices. It is worth noting that the Government made consequential amendments to the Bill at Lords Committee stage to ensure that recipients of the new notification notices will be able to make a complaint about them to the Investigatory Powers Tribunal. This is already the case for the other kinds of notice to which I have referred.

Secondly, Lord Ponsonby asked what the Government considered a reasonable time in which a company should respond. The expression “a reasonable time” is reflective of the language used within the current Technical Capability Notice Regulations with regards to the obligation to notify the Secretary of State of changes. It would be impractical to define reasonable time any further, given reasonableness would be impacted by a number of factors, such as the scale and timing of the proposed change.

Thirdly, he asked about industry engagement. The Government routinely engages with operators that provide lawful access of significant operational value. These operators are therefore aware of the lawful access capabilities that law enforcement and intelligence agencies are utilising and the changes that could potentially impact them. However, the notification notice will seek to formalise this into an obligation, making it clear what services and systems the notice covers and the types of changes of which the operator must notify the Secretary of State. A clear specification setting this out will be of benefit to both the operator and the Government.

Fourthly, he asked for the Government to be more specific about the types of changes that would be considered relevant for this new notification requirement. On 5 December, the Government published a policy statement setting out the proposed content of the draft regulations that would be made under this measure for the notification of proposed changes to telecommunications systems². The types of change that would be considered relevant are set out within this statement. These include:

² [Investigatory Powers \(Amendment\) Bill: policy statement - GOV.UK \(www.gov.uk\)](https://www.gov.uk/government/policy-statements/2018/12/05/investigatory-powers-amendment-bill-policy-statement)

- a) **Changes to data retention periods by the operator.** An operator will retain data for as long as business requirement dictates. An operator may change their data retention periods at any point.
- b) **Changes in the operator's ability to lawfully provide communications data.** Communications data is the 'who', 'when', 'where' and 'how', otherwise known as the metadata.
- c) **Changes in the operator's ability to lawfully provide the content of communications.** Content differs from communication data as, crucially, it is the 'what'.
- d) **Decommissioning of a service.** The decommissioning of a service may require the Secretary of State to vary the notification notice.
- e) **Other relevant change specified in the notification requirement.** Operators provide unique and individual services and may provide specific lawful access capabilities that will be known between the operator and Secretary of State. For the protection of these capabilities, it will be included in the confidential specification agreed between the operator and Secretary of State.

General Data Protection Regulation (GDPR)

During the discussion on Part 4 of the Bill, Lord Fox referred to Article 32 of the GDPR and suggested that the changes being made by this Bill could cause a conflict with obligations in the GDPR. While he is correct that the GDPR does require the implementation of technical and organisational measures to protect the privacy of personal data, there is a great deal of nuance to this. The GDPR does not apply a blanket obligation on controllers and processors to adopt specific measures such as end-to-end-encryption of user data. It simply states that technical and organisational measures to ensure a level of security appropriate to the risk should be implemented "as appropriate".

It further lists other measures that should be considered as appropriate for the purposes of security of processing – for example, "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident."

Critically, the requirement is not an absolute or minimum one, rather controllers and processors must always consider and implement "appropriate technical and organisational measures" relative to the specific risk in each case.

The Principles

I would first like to state that the Government recognises and welcomes the important oversight provided by the Intelligence and Security Committee of Parliament (ISC). I would also like to follow the Prime Minister in thanking the Committee for the comprehensive and detailed nature of their International Partnerships Report and the extensive work behind it.

While discussing the ISC, Lord Fox, asked about "*The Principles relating to the detention and interviewing of detainees overseas and the passing and receipt of intelligence relating to detainees*" (The Principles) and requested clarity on the Government's position on this. While this topic is not strictly a matter for the Bill, I would like to give some further detail.

The Principles were published on 18 July 2019 and came into effect from 1 January 2020. The Principles are the result of a review by the then-Investigatory Powers Commissioner, Sir Adrian Fulford, of the July 2010 Consolidated Guidance or the Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees.

The Principles – like the Consolidated Guidance before them – give instructions to officers in the intelligence and security agencies, the Ministry of Defence, the National Crime Agency and SO15 (Metropolitan Police) when engaging with international partners on the detention and interviewing or detainees overseas. They are designed to ensure that any such activity is consistent with UK and international law, and with the UK the Government’s stance on torture, unlawful killing, extraordinary rendition, and cruel, inhumane, and degrading treatment (CIDT).

The Investigatory Powers Commissioner (IPC) has the authority to oversee the application of The Principles. Furthermore, the Investigatory Powers Commissioner’s Office (IPCO) conducts regular reviews of this work and publish their findings in their annual report.

The Government complies with UK and international law. The Government does not participate in, solicit, encourage, or condone the use of torture or of cruel, inhumane, or degrading treatment for any purpose. In no circumstance should UK personnel ever take action amounting to torture, unlawful killing, extraordinary rendition, or CIDT.

The UK takes great care to assess whether there is a real risk that a detainee will be subjected to torture, unlawful killing, extraordinary rendition or CIDT. In each case, the UK investigates whether it is possible to mitigate any such risk, including through seeking assurances from partners. If, despite efforts to mitigate this, there is a ‘real risk’ of torture, unlawful killing or extraordinary rendition, there is a presumption that the activity will not proceed. Ministers can authorise activity in the interests of national security, even where it has not been possible to mitigate the risks to ‘less than real’.

Many of these decisions are complex. Ministers are supported by a robust legal framework and are scrutinised by the IPC. As the ISC noted in its International Partnerships report: “The Principles appear to be working well, and are well integrated into Agency processes.”

European Convention on Human Rights Cases

Lord Fox, spoke to amendments, the effect of which would have been to introduce an obligation for MPs to be notified if they had been subject to interception or equipment interference Lord Fox explained that a person can only bring a case based on unlawful interference with their Article 8 rights if they know those rights have been interfered with in the first place. He referred to two cases from the European Court of Human Rights, *Klass v Germany* in 1978, which was reiterated in *Weber and Saravia v Germany* in 2006.

I hope it will reassure Lord Fox that, as I set out in the debate, there are a number of existing accountability routes that allow any individual – whether or not they are a member of a relevant legislature – to challenge the activities of the intelligence services. Foremost among these is the Investigatory Powers Tribunal, which provides a cost-free right of redress to anyone who believes they have been the victim of unlawful actions by a public authority using covert investigative techniques. The European Court of Human Rights (in the case of

Big Brother Watch v the UK in 2021) and our own domestic courts have endorsed the Investigatory Powers Tribunal as a robust and judicial remedy.

Any Member of Parliament could complain to the IPT and ask them to investigate, if they believe they have ever been the victim of unlawful interception by a public authority using covert techniques. The IPT would then investigate the matter. Furthermore, the IPT may ask IPCO to investigate matters that it determines are necessary, which could include matters relating to warrants authorising the interception of communications to or from Members of Parliament.

Finally, along with their general oversight and inspection duties, the IPC also have an obligation to notify serious errors in the use of investigatory powers to affected persons under section 231 of the IPA. This applies to all members of the public, regardless of whether they happen to be Members of Parliament or not, where it is in the public interest to do so.

There is already a comprehensive suite of interlocking safeguards from the start to the end of the process that protect members of relevant legislatures from unlawful interception. Adding a notification requirement is both unnecessary and potentially harmful, for the reasons set out by Baroness Manningham Buller during the debate.

Triple Lock – Mayors

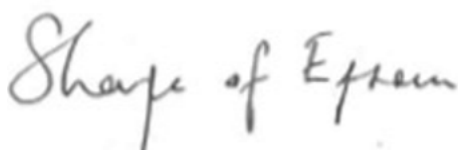
Lord Fox asked an important question about whether the communications of elected Mayors should be protected by the triple lock process in the same way as members of relevant legislatures (MRLs).

The protections afforded to MRLs are so significant because of the representative role that they play in both national and constituency affairs, and access to their communications with their constituents should be subject to this extra oversight. Mayors do not have this same level of interaction and have, in any case, never been subject to the Wilson Doctrine. The communications of elected Mayors, Police and Crime Commissioners, and Council Leaders are sufficiently protected, in the same way that the public's communications are protected, by the double lock mechanism in the IPA and the remedies set out above.

I hope this provides the additional information and assurance requested by Noble Lords on these various issues.

A copy of this letter will be placed in the House library.

Yours Sincerely,

A handwritten signature in cursive script that reads "Sharpe of Epsom".

**Lord Sharpe of Epsom OBE
Parliamentary Under Secretary of State
Home Office**