



Home Office

**Rt Hon Tom Tugendhat MBE VR MP**

Security Minister

2 Marsham Street

London

SW1P 4DF

[www.gov.uk/home-office](http://www.gov.uk/home-office)

**Rt Hon Sir John Hayes CBE MP**

**House of Commons**

**London**

**SW1A 0AA**

**By Email Only**

06 March 2024

Dear Sir John,

Thank you once again for your helpful contributions during the Investigatory Powers (Amendment) Bill's Second Reading debate on 19 February. I undertook to write with further information on the bodies affected by Clause 14 of the Bill. I would also like to take this opportunity to respond to the points raised by the Rt Hon Kevan Jones MP on oversight of the authorisations under new Part 7A of the Investigatory Powers Act 2016, as introduced by Clause 2 of the Bill (bulk personal datasets with low or no expectation of privacy), in order to provide clarity on the Government's position.

### **Regulatory authorities (Communications Data)**

During the debate, you asked for confirmation of which bodies will be able to compel the release of communications data ("CD") using regulatory or supervisory powers through the reinstatement of relevant powers in Clause 14. The reinstatement of the power to acquire CD applies to a limited cadre of public authorities with the necessary statutory powers conferred on them by Parliament and only specifically when in support of regulatory and supervisory functions.

This will cover important bodies and central government departments who carry out a range of vital statutory functions including: HM Revenue and Customs, the Financial Conduct Authority, the Department for Work and Pensions, HM Treasury, the National Crime Agency, the Department for Business and Trade and the Competition and Markets Authority. Whilst this is not a fully exhaustive list, all the bodies whose compulsion powers in respect of acquiring CD would be reinstated have had those powers granted by Parliament in support of their statutory functions. Those powers have remained in force in relation to all other relevant information, and this Bill will include CD within the scope of those powers again.

These bodies require what would now be considered as CD in order to carry out a range of regulatory and supervisory duties, including: tackling breaches of sanctions regimes; enforcing the minimum wage; seeking to prevent criminals from retaining the proceeds of their crimes or exploitation of workers; detecting and combating money laundering; and providing oversight of banking and financial markets. Examples of statutory powers relied upon include Regulation 66 of the Money Laundering, Terrorist Financing and

Transfer of Funds (Information on the Payer) Regulations 2017, section 14 National Minimum Wage Act and section 165 Financial Services and Markets Act.

The reinstatement of these powers is not a way to circumvent the safeguards in the IPA. Those who have their civil information gathering powers reinstated in respect of CD will still need to obtain an authorisation under Part 3 of the IPA should they wish to carry out a criminal investigation, and there will be clear guidance in the Code of Practice setting this requirement out. As is currently the case, any public body which is not listed on Schedule 4 to the IPA will not be able to acquire CD in support of criminal investigations.

It is worth noting how we have come to the current state of play following passage of the 2016 Act, and why the Government considers it right to restore information gathering powers for the narrow purposes set out at Clause 14. As you will be aware, when you took the original legislation through Parliament in 2016, statutory purposes were included in Section 61(7) (f) and (j) of the IPA for the acquisition of CD for the purposes of taxation and oversight of financial services, markets, and financial stability, respectively.

When implementing the *Tele2 and Watson* judgment from the Court of Justice of the European Union in 2016, the Government took the opportunity to streamline the statute book. In particular, the judgment required that there should be independent prior authorisation of applications for CD acquisition in relation to criminal investigations for non-urgent and non-national security purposes and set out that the more sensitive “events data” should only be available where the serious crime threshold is met.

This streamlining of the statute book also included the removal of the regulatory provisions contained in Section 61(7) (f) and (j) of the IPA because, at that time, public authorities with those regulatory or supervisory functions were able to acquire the data they needed using their own information-gathering powers. Section 12 of the IPA 2016 had not yet been commenced so they were able to continue to rely on those powers to compel telecommunications operators to comply with their requests. Furthermore, at that time, much of the relevant data was not considered to come within the definition of CD and so was unaffected by the IPA . As more and more activity takes place online, more data has come within the definition of CD and so within the scope of the IPA, and that data is of increased importance to those public authorities with regulatory or supervisory statutory functions.

An example of the impact of the expansion of the scope of CD as a result of activity increasingly taking place online relates to the provision of Know Your Customer (KYC) data. Banks and other financial institutions are required to provide KYC data to regulators to ensure that organisations and individuals to whom they provide services are operating legally. As many banking services are now provided online, data that would not have previously been within the scope of CD now meets the definition of CD, and banks and financial institutions providing these services are considered as telecommunications operators for the purposes of the IPA. As such, they require a Part 3 authorisation to provide CD to requesting bodies who are obtaining KYC for the purposes of regulatory or supervisory functions, but as these enquiries do not meet the criminal threshold, it is not possible to provide a Part 3 IPA authorisation. As such, without immediate action, these important functions will continue to be inhibited.

In the light of the above, following your stewardship of the Investigatory Powers Bill, Parliament always intended to permit those bodies in Schedule 4 to acquire CD for regulatory and supervisory purposes set out in Section 61(7)(f) and (j). Clause 14 of the Bill will reinstate those regulatory and supervisory powers for public authorities relating to those statutory purposes as well as for other important functions, including those in Schedule 4, provided there is no intention of seeking a criminal prosecution in reliance on CD acquired under those powers.

You raise an important point, and I look forward to continuing engaging with you on this issue as the Bill progresses through the Commons.

## “Low/no” Bulk Personal Datasets – notification of authorisations

The Rt Hon Kevan Jones MP asked why the Government would not agree to require the intelligence services to notify the Investigatory Powers Commissioner (IPC) when an individual bulk personal dataset (BPD) is authorised in reliance on a category authorisation.

Firstly, I would like to reiterate that the new Part 7A does not represent an increase in powers or access to personal data. Bulk personal datasets, including those to which the new Part 7A applies, may already be retained and examined under the existing Part 7 regime. The safeguards in Part 7 are intended to accommodate the most sensitive of datasets; they do not make provision for datasets in respect of which there is a low or no reasonable expectation of privacy. It would not be appropriate for the strictest of safeguards to be applied to a very wide variety of less sensitive datasets.

The Government has therefore introduced Part 7A to ensure that the safeguards that are applied to these datasets are proportionate. The intention of the new regime is to encompass datasets including, but not limited to, news articles, academic papers, public and official records, online encyclopaedias, audiobooks and podcasts, content derived from online video sharing platforms, publicly available information about public bodies, corporate registry/trade data, and internet infrastructure and operating data. The safeguards are therefore calibrated to reflect the sensitivity of these datasets and the intrusion that is likely to arise from their retention and examination. This will ensure that the rights of the individuals to whom the data relates are adequately protected whilst also enabling the intelligence services to make more effective use of these datasets.

The change proposed by the Hon Member would be more onerous than the requirements under the existing provisions for BPDs under Part 7. Not only is this unnecessary, but it would also impose additional burdens on the intelligence services, with no meaningful increase in oversight given the comprehensive package of safeguards that is already included in Part 7A.

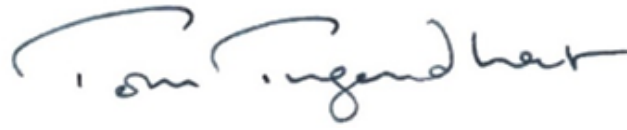
The IPC already has extensive oversight of Part 7A in the provisions set out in the Bill. The IPC’s judicial commissioners have a role in the authorisation process and his inspectors will carry out regular inspections of the intelligence services’ use of the new provisions. **Prior judicial approval is required for all category authorisations and for all individual authorisations that do not rely on a category authorisation.** The intelligence services may also seek prior judicial approval, even when it is not required, if they consider it appropriate to do so. Once granted, an authorisation is valid for twelve months and must then be renewed.

On inspection, IPCO will be entitled to see all authorisations granted under Part 7A and can review the datasets under it. Any irregularities or errors may be reported by the IPC in his annual report. This is the approach taken in inspections of the existing Part 7, whereby datasets retained under class warrants are reviewed by IPCO inspectors. We consider that the overall package of safeguards in Part 7A is appropriate and proportionate to the nature of the datasets with which it is concerned. We do not see the case for adding a new, more onerous, dataset-by-dataset requirement here. It is highly unlikely that the Rt Hon Member’s suggestion for “*a one-line email to the Investigatory Powers Commissioner containing the name and description of the bulk personal dataset*” would add anything to this oversight framework that was in any way meaningful.

I hope this letter has provided sufficient assurances and has clarified the Government’s position on these important issues. I look forward to further discussion on this vital Bill.

A copy of this letter goes to the Rt Hon Kevan Jones MP. I am also placing a copy of this letter in the House of Commons Library.

Yours,

A handwritten signature in black ink that reads "Tom Tugendhat". The signature is written in a cursive, flowing style.

**Rt Hon Tom Tugendhat MBE VR MP**  
Security Minister