House of Commons Library

Research Briefing

21 March 2024

By Joanna Dawson

Investigatory Powers (Amendment) Bill

Image Credits

Communications hardware by Tom Blackwell. Licensed under CC BY 2.0 / image cropped.

Disclaimer

The Commons Library does not intend the information in our research publications and briefings to address the specific circumstances of any particular individual. We have published it to support the work of MPs. You should not rely upon it as legal or professional advice, or as a substitute for it. We do not accept any liability whatsoever for any errors, omissions or misstatements contained herein. You should consult a suitably qualified professional if you require specific advice or information. Read our briefing 'Legal help: where to go and how to pay' for further information about sources of legal advice and help. This information is provided subject to the conditions of the Open Parliament Licence.

Sources and subscriptions for MPs and staff

We try to use sources in our research that everyone can access, but sometimes only information that exists behind a paywall or via a subscription is available. We provide access to many online subscriptions to MPs and parliamentary staff, please contact hoclibraryonline@parliament.uk or visit commonslibrary.parliament.uk/resources for more information.

Feedback

Every effort is made to ensure that the information contained in these publicly available briefings is correct at the time of publication. Readers should be aware however that briefings are not necessarily updated to reflect subsequent changes.

If you have any comments on our briefings please email papers@parliament.uk. Please note that authors are not always able to engage in discussions with members of the public who express opinions about the content of our research, although we will carefully consider and correct any factual errors.

You can read our feedback and complaints policy and our editorial policy at commonslibrary.parliament.uk. If you have general questions about the work of the House of Commons email hcenquiries@parliament.uk.

Contents

Summary

The Investigatory Powers Act (Amendment) Bill was announced in the King's Speech on 7 November 2023. The accompanying briefing said that the Bill would update the Investigatory Powers Act 2016 and deliver "urgent changes" needed to protect the British people.

What is the Investigatory Powers Act 2016?

The Investigatory Powers Act 2016 overhauled the framework governing the powers of public bodies, including the intelligence and security agencies and law enforcement, to obtain the content of communications and communications data (information about a communication).

Reviews of the Investigatory Powers Act

Following a statutory Home Office review (PDF) of the Investigatory Powers Act 2016 in 2022, Lord Anderson was asked to conduct an independent review, considering various proposals for reform.

Lord Anderson's Independent Review of the Investigatory Powers Act 2016 (PDF) was published in June 2023.

Its most significant recommendations was to create a new category of bulk personal dataset(sets of personal information about a large number of individuals, the majority of whom will not be of any interest to the security and intelligence agencies) in which there was a low or no expectation of personal privacy, because, for example, it is already publicly available . This category would be subject to a lighter-touch regime of safeguards than that which currently applies to bulk personal datasets under Part 7 of the Investigatory Powers Act. He made further recommendations about the how long bulk personal data sets can be retained and how they should be renewed.

Lord Anderson also recommended that a new legal basis for accessing internet connection records, records of which internet sites or services have been used, should be added to the Investigatory Powers Act, in order to enable the detection of new subjects of interest.

He also made recommendations about updating certain definitions in the Act and improving the efficiency, flexibility, and resilience of processes around issuing warrants and oversight measures.

Notices under the Investigatory Powers Act

Separately, the Home Office consulted on several proposals to change the notices regime contained in Parts 4 and 9 of the IPA in June 2023.

The regime currently comprises three kind of notice which can be imposed on telecommunications operators by the Government:

- Data retention notices: requiring that operators retain communications data
- Technical capability notices: requiring operators to provide and maintain technical capabilities enabling them to provide any assistance as required by an authorisation under the IPA
- National security notices: requiring operators to take any steps considered necessary by the Secretary of State in the interests of national security. This may include providing services or facilities to enable the intelligence services to carry out their functions or deal with an emergency.

The consultation noted that changes in technology and an increase in data being held overseas risked reducing the capabilities of law enforcement and intelligence agencies. It made proposals, reflected in the Bill, which aim to make it easier to access data held overseas, and to enable intelligence agencies to work with telecommunications operators to ensure lawful access to data.

What would the Bill do?

The Bill would implement most of the proposals from the reviews. In particular it would:

- Introduce a new, lighter-touch regime for the retention and examination of bulk personal datasets where there is a low or no expectation of privacy in the data
- Create an additional condition, allowing authorities to access internet connection records in order to identify individuals accessing specific internet sites and services where necessary to address serious crime or to protect national security
- Create a new requirement for telecommunications operators to notify the Government of proposed changes to products or services which could impede intelligence services in lawfully accessing data

It would extend to the whole of the UK.

Proceedings in the House of Lords and wider reaction

The Bill was introduced in the House of Lords in November 2023 and completed third reading in January 2024.

It had cross party support, although members of the House of Lords tabled probing amendments on issues including the adequacy of oversight provisions and other safeguards. Several Government amendments were agreed, as well as opposition amendments relating to the role of the Prime Minister in approving warrants to intercept the communications of parliamentarians and oversight by the Intelligence and Security Committee.

Some privacy campaigners and technology companies have expressed concerns about whether the Bill strikes the right balance between privacy and security (PDF).

Further information and next stage

The Bill had second reading in the House of Commons on 19 February 2024. It had two Committee sittings on 7 March. Report stage is scheduled for 25 March.

Bill documents, including the explanatory notes, impact assessment and European Convention on Human Rights memorandum are available on the Bill pages.

The Government has also published a series of factsheets on the Bill, draft excerpts from codes of practice, and other relevant documents.

1 Background

1.1 What is the Investigatory Powers Act 2016?

The Investigatory Powers Act 2016 overhauled the framework governing the use of surveillance by the intelligence and security agencies and law enforcement to obtain the content of communications and communications data. It followed three significant reports published in 2015, all of which concluded that the existing framework was unfit for purpose and in need of reform, and a draft Bill that was subjected to pre-legislative scrutiny by three parliamentary committees.

The capabilities the IPA governs are:

- the interception of communications,
- the retention and acquisition of communications data,
- equipment interference, and
- the retention and examination of bulk personal datasets

Interception, acquisition of communications data, and equipment interference powers are provided for both on a targeted basis and in bulk.

The Act also reformed the oversight regime for the use of these powers, replacing the three existing Commissioners with a single body of judicial commissioners led by the Investigatory Powers Commissioner (IPC). For the first time, these the Investigatory Powers Commissioner's Office (IPCO) brought an element of judicial oversight to the process of issuing warrants to the intelligence services.

1.2 Home Office review

The Home Office conducted a review of the operation of the IPA in 2022, as required by section 260.[1] The report of the review was published in February 2023.

[1] S260 required a review by the Secretary of State five years after the Act received royal assent.

The aim of the review was to assess the extent to which the objectives of the Act continue to be met and whether any changes are required to ensure it remains fit for purpose.

According to the report, it has become apparent that some elements of the oversight regime "are now inhibiting the UK intelligence community's ability to work together and with partners". This leaves the public vulnerable to a "wide range of evolving threats", it says.[2]

The report states that although the IPA was designed to be technology neutral, and to therefore endure, a combination of changes in technology and the threat landscape, as well as legal challenges, have cast doubt on the extent to which it remains fit for purpose.

The review considered the following issues:

- Oversight including the role of the IPC, and the warrantry and authorisation processes
- Consistency and appropriateness of safeguards across the IPA
- Whether key definitions remain fit for purpose
- Effectiveness of the notice regime
- Effectiveness of the Bulk Personal Dataset regime in the context of the UK's strategic goals set out in the Integrated Review
- Policy and legal challenges relating to internet connection records
- Overlap between interception and equipment interference and the evidential use of data

Oversight

The review identified several proposals for reform of IPCO to provide greater flexibility and resilience. These included a statutory basis for deputy IPCs; the ability to delegate the hearing of appeals against a refusal of a warrant; and, the ability to delegate some communications data applications to a judicial commissioner.

It noted that IPCO had requested that any non-statutory functions are placed on a statutory footing, and that statutory instruments had been introduced to give effect to this.[3]

---

2 Report on the Operation of the Investigatory Powers Act 2016, 2023, Home Office, p4

3 The Functions of the Investigatory Powers Commissioner (Oversight of the Data Access Agreement between the United Kingdom and the United States of America and of functions exercisable under the Crime (Overseas Production Orders) Act 2019) Regulations 2020; The Investigatory Powers Commissioner (Oversight Functions) Regulations 2022

The review found that there was no case for systemic change to the IPC's role or legal basis.

Warrantry and authorisations

The review looked at challenges and inconsistencies in the warrantry (the issuing of warrants to use investigatory powers) and communications data authorisations process. It identified specific 'pressure points' and proposed solutions aimed at ensuring that the system functions efficiently and effectively.

Access to Secretaries of State and Senior Officials

The review noted that where warrantry decisions are required to be made by the Secretary of State, reliance on their availability creates a pressure point in the process. This can create backlogs, in particular during recess, election periods, or due to foreign travel. The same issue arises with respect to authorisations by Scottish Ministers and senior officials.

The review identified modifications and cancellations of targeted equipment interference warrants by the Director General of the National Crime Agency as a particular issue, as there is no provision for this function to be delegated. It said this can generate delays which can adversely impact operational activity.

The triple lock

Where a warrant is sought to intercept the communications of a person who is a member of a relevant legislature,[4] the IPA requires the authorisation of the Prime Minister, in addition to the Secretary of State and a judicial commissioner.[5]

The review concluded that there may be a need to amend the IPA to allow for deputization of this function in exceptional circumstances, such as if the Prime Minister was incapacitated.

Targeted communications data authorisations

A legal challenge concerning, among other things, the lack of independent authorisations for access to certain types of communications data by law enforcement and other public authorities for serious crime purposes led to the establishment of the Office for Communications Data Authorisations (OCDA).The IPA was amended to provide for authorisations by OCDA and a serious crime threshold for accessing communications data.[6]

As a result of a subsequent judgment relating to the same judicial review, the Government introduced regulations requiring independent authorisation for

4 Members of Parliament and the devolved legislatures

5 This applies to interception warrants (s26) and equipment interference warrants (s111)

6 Data Retention and Acquisition Regulations 2018/1123

intelligence agencies to access communications data for serious crime purposes. These came into force in January 2023.[7]

Safeguards

The review considered the consistency of safeguards and controls across the Act, and the regime for protecting legally and professionally privileged material and journalistic material.

It noted some inconsistencies in the application of safeguards in relation to certain sensitive data. However, the overarching requirements in section 2 of the IPA, which impose general duties in relation to privacy, together with the requirements in the codes of practice, ensure that there is an obligation to consider a higher level of protection for this material.

The reviews conclusion that public authorities had developed good working practices in applying safeguards was corroborated by the IPC's assessment, it said.[8]

Definitions

The review also considered whether definitions of key terms used in the IPA remained fit for purpose.

It noted that it is not always clear whether a particular type of data or operator falls within the scope of the IPA's definition of 'communications data' or 'telecommunications operator'. This is likely to be an increasing issue given the pace of technological change and the development of new analytical techniques, it said, and the IPC has highlighted specific concerns.

Two particular issues were the utility of the offence of knowingly or recklessly obtaining communications data, given the lack of clarity about the definition, and the fact that some online services do not consider themselves to be telecommunications services. This causes additional bureaucracy because these services seek to comply with the requirements of the Data Protection Act as well as the IPA.

The Home Office has issued interim guidance for public authorities to clarify these definitions, but the review noted that the IPC believes there is a case for legislative change.

7 The Investigatory Powers (Communications Data) (Relevant Public Authorities and Designated Senior Officers) Regulations 2022

8 The review cites the IPC's Annual Report 2020, page 8

Effectiveness of notices

Two issues relating to the effectiveness of data retention notices and technical capability notices were identified by the review:[9]

- Third party data: the review states that where an operator can see or access communications data relating to a service provided by a third party running over their network, but does not process that data, it is regarded as third party data.[10] It says that new technology has brought about unforeseen consequences, and that "this possible impact to current CD retention could be exacerbated over time as standards and business models continue to evolve". It further notes risk relating to the introduction of new routing technologies, and suggests the Act may need to be amended to provide clarity and mitigate the risk.

- Funding model: different funding models apply in relation to reimbursing operators for complying with the IPA. It currently provides that the Secretary of State may decide what level is appropriate and specify it in a notice.[11] Given the need to secure value for money for taxpayers, the review suggests there may be a future case to reassess funding models to ensure consistency.

Bulk personal datasets

Bulk personal datasets (BPDs) are defined by the IPA as "a set of information that includes personal data relating to a number of individuals … such that the majority of the individuals are not, and are unlikely to become, of interest to the intelligence service in the exercise of its functions".[12] They are governed by Part 7 of the Act and the BPD code of practice.

They are typically of a size that means they cannot be processed manually. The review explains that, when the IPA was drafted, intelligence services extracted value from them asking specific questions of the data to retrieve information of intelligence value.

The review identified "limitations" within the IPA which, together with the pace of technological change, are inhibiting intelligence services' ability to take advantage of the evolving digital environment.

It suggested that when the IPA was passed it did not foresee various developments:

9 These are notices, discussed further below at 1.4, which can be given by the Secretary of State to operators, requiring them to retain communications data, and to provide capabilities to enable public bodies to exercise their functions under the IPA, respectively.

10 Meaning that it would be excluded from the scope of a data retention notice.

11 S249

12 S199

- the exponential increase in the use of, complexity and changing nature of data
- the extent to which new technology would enable powerful analysis of datasets
- the possibility that most data referencing human activity can in theory be resolved to real world activity, extending the scope of the definition of BPD to new datasets

Specific recommendations for reform by the review included extending the duration of warrants for the retention and examination of BPDs, and allowing certain functions to be delegated from an Agency head to a Crown servant.

Internet connection records

Internet connection records are a form of communications data , described as 'a record of an event held by a telecommunications operator about the service to which a customer has connected on the internet'.[13]They do not reveal every webpage that a person has visited, or what they did on a particular webpage.

Currently, the IPA allows public authorities, with the exception of local authorities, to access ICRs provided certain conditions are satisfied.[14]

The review explains that the National Crime Agency (NCA) has sought to trial ICR through a small number of operators, with the aim of testing operational, functional and technical aspects of ICR retention. It says that the trial has focussed on access to websites whose sole purpose relates to illegal images of children and has identified over 120 subjects of interest.

The review found that some amendments could be made to the code of practice to clarify oversight arrangements, and that the IPA could be amended to ensure that ICRs can be used for target discovery purposes (the identification of subjects of interest), particularly in the context of identifying child sexual exploitation and abuse offenders.

Conclusions

The review concluded with an analysis of whether or not the IPA had achieved its aims.

It concluded that it had achieved the aims of consolidating existing powers relating to communications data, the interception of communications and equipment interference, and of oversight bodies; and, enhancing oversight and safeguards.

---

13 Communications Data Code of Practice, 2.74, cited at para 4.1

14 S62 IPA and Communications Data Code of Practice, section 9

However, it suggested that some of the issues identified indicated that it had "not been immune to changes in technology over the last six years". Some changes were therefore necessary in the short term, it said, "with more substantial reform inevitably necessary in future". This was a result of technological developments, changes to the way data is stored and used, and the requirements of protecting national security and dealing with serious crime.

1.3 Lord Anderson's review

Lord Anderson subsequently conducted an independent review, which included consideration of a number of proposals put to him by the Home Office and the intelligence services.

Bulk personal datasets

Datasets with low or no expectation of privacy

Lord Anderson noted that the uses of BPDs are evolving rapidly, particularly in light of the use of big data analytics, and that bulk collection and bulk analysis techniques are used to confirm new investigative 'seeds' which can then be developed into usable intelligence using BPDs and transformation tools such as machine learning.[15]

The training of machine learning models requires large quantities of data that is representative of the type of data on which the model is to be deployed, but when building models intelligence services are using the structure and attributes of the whole dataset to build capability, rather than interrogating the data to identify individual records of intelligence interest.

Part 7 of the IPA currently governs the retention and examination of BPDs, applying safeguards including the 'double lock', which requires that warrants be approved by both the Secretary of State and a judicial commissioner. In addition to the requirements of Part 7, there is also a code of practice and internal procedures within each Agency.

Against this background, Lord Anderson made three general observations about the relatively narrow scope of the Part 7 regime:

- It does not apply to the acquisition of BPDs, only to their retention and examination;
- It does not apply to law enforcement (although he noted that the NCA chooses to operate an equivalent non-statutory scheme), or to the public sector, business or third sector;

[15] As above, para 3.9

- It does not apply to personal data held by third parties to which UKIC has access.

He suggested that these "in some respects anomalous" features of the Part 7 regime "prompt reflection as to whether, as a matter of policy, its scope is correctly defined", bearing in mind that BPDs are generally considered to be less intrusive than other bulk powers. He said that the application of the regime to BDPs that are used without restriction by public and private bodies, is seen by UKIC as a "problematic constraint on the agility which is essential to their work".[16]

Following the Home Office report on the IPA, Lord Anderson was asked in particular to consider the effectiveness of Part 7, including

- whether the warrantry process is fit for purpose for all types of dataset
- whether the current duration of warrants should be amended, and
- whether powers vested in Agency Heads could be delegated to Crown Servants.

Having reviewed existing initiatives to increase efficiency in the process, Lord Anderson concluded that the basic structure applicable to BPDs could not be further reformed without amendment to the IPA. He noted that the Part 7 safeguards are perceived as "disproportionately burdensome in their application to publicly-available datasets, specifically those containing data in respect of which the subject has little or no reasonable expectation of privacy".[17]

The Review team observed real-world examples of the problems this could cause, including delay in contexts where a BDP has a rapidly diminishing value, such as a battlefield or fast-moving investigation, and where cooperation with partners might require sharing a BDP.

There were also a number of indirect consequences for cooperation, including:

- Making it harder to maintain cover due to requirements on a data provider to implement BDP safeguards which only apply to UK intelligence services
- Flagging appetite of data partners to cooperate when it requires applying data protection law and BDP safeguards
- A negative impact on the recruitment and retention of talent, who may find bureaucratic processes frustrating when they are not found elsewhere.

16 As above, paras 3.22-3.23

17 As above 3.30

The Review team also heard that the BPD requirements could impact on the viability of using commercially available technology infrastructure to store and hold BPDs and have an opportunity cost due to the resource implications of compliance.[18]

As a result of the impact of Part 7 on operational agility, the intelligence services put forward a proposal to Lord Anderson, which developed during the course of the review, to exempt some categories of BDP from the full requirements. The aim of the proposal would be to significantly reduce the time needed to authorise the use of a BPD where there is a low or no expectation of privacy ('low/no datasets').

Four principles were proposed as relevant to the test of whether a dataset is a low/ no dataset, based on the reasonable expectation of privacy at the core of the Article 8 right to privacy under the ECHR:

- Nature of the data: the extent to which the nature of the data is such that an individual to whom the data relates would be considered to have a reasonable expectation of privacy;
- Data subject: the extent to which there is evidence (i) that the data has been manifestly made public by the data subjects, or (ii) that the data subjects have consented for the data to be made public;
- Publication: the extent to which the data has been published subject to editorial control and/ or the application of professional standards, and how widely known the dataset it; and
- Use (or further use): the extent to which data has been used already in the public domain such that further use by the intelligence services for the purpose of theirs functions is unlikely to lead to further intrusion.

Lord Anderson suggested that many decisions to classify a dataset as low/ no are likely to be relatively straightforward, and provided the following examples of the types of dataset falling into this category: 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 proposal would involve amending the IPA to remove low/ no sets from the scope of Part 7, and apply a lighter touch set of safeguards.

Lord Anderson decided to support the proposed change for the following reasons:

[18] Paras 3.32-3.36

- The deregulatory effect would be relatively minor – it would only apply to a small minority of BPDs; they would still be subject to the Data Protection Act 2018, and to the lighter touch safeguards;
- There appears to be no international consensus for a regime as strict as Part 7, with the USA, Canada and Australia taking a different approach;
- The operational arguments for the proposed deregulation are compelling;
- The threat context has changed with intelligence work moving away from the often unsophisticated terrorist threat of the past 20 years, meaning that the value of BPDs is increasing.

In addition to a code of practice containing safeguards in relation to issues such as the initial examination, internal authorisation process, storage, access and examination, Lord Anderson also proposed a statutory requirement of prior approval by a judicial commissioner. He further proposed that the Secretary of State could be invited to authorise and JCs to approve classes of low/ no BPDs to which, once approved, intelligence services could allocate datasets without further approval. BPDs falling into an approved class could be notified to a JC, whereas those that did not would require specific JC approval.[19]

Duration

The Home Office asked Lord Anderson to consider a proposal to extend the existing duration of six months for BPD warrants to 12 months, for the following reasons:

- The intelligence value of BPDs tends to be more static and predictable than that of warrants targeting the acquisition of communications;
- BDPs often support long-term strategic intelligence activities rather than short term tactical actions;
- Bulk interceptions and equipment interference (EI) warrants, which cease to have effect after 6 months are inherently more intrusive.

Having considered compliance with existing rules on BPDs , additional requirements in the code of practice, and the fact that no extension request has ever been refused to date, Lord Anderson concluded that the advantages of the proposal outweighed any disadvantages.[20]

---

[19] Recommendation 1: Amend Part 7 of the IPA to recognise a new category of BDP in which there is a low or no expectation of privacy, with a less onerous set of safeguards; Recommendation 2: Low/ no classes should be authorised and approved via the double lock, and any proposed low/ no BPD falling outside the terms of a class should be approved by a JC as meeting the low/ no criteria

[20] Recommendation 3: section 213 of the IPA should be amended to provide that BPD warrants cease to have effect 12 months after they were issued, unless they have been renewed or cancelled.

Delegation

Some provisions in the IPA explicitly allow for functions to be performed by a Crown servant on behalf of an Agency Head.

However in relation to BPDs the following functions do not include specific provision for this:

- A requirement to consider whether specific BPDs consist of or include protected data, health records or sensitive personal data, or raise novel or contentious issues (s202);
- A requirement to consider whether specific BPDs contain health records (s206);
- A requirement to conduct initial elements of the examination of specific datasets (s220);
- A requirement, so far as reasonably practicable, to secure that where a JC refuses to approve a decision to issue an urgent warrant, anything being done in reliance on that warrant stops as soon as possible (s210);
- A requirement to apply, after the non-renewal or cancellation of a BPD warrant, for a further period of up to 3 months in which the material can continue to be retained and examined (s219);
- A requirement to apply for a direction that BPDs obtained pursuant to any other authorisation under the IPA, with the exception of a bulk acquisition warrant, be retained and examined under Part 7 (s225)

Lord Anderson suggested that, with the exception of section 210, each of these tasks is of a routine nature, comparable to other delegable functions in the IPA, and capable of being carried out by officials with relevant expertise.[21]

Internet connection records (ICRs)

Lord Anderson noted that, while in some ways ICRs are analogous to telephone CD logs, the extent to which people live their lives online means that browsing history can reveal appreciably more about a person.

As such, they are subject to additional safeguards by comparison with telephony CD under the IPA.[22]

---

[21] Recommendation 4: sections 202, 206, 215, 219 and 220 (but not section 210) should be amended to provide that the functions they provide for can be delegated to a Crown servant by an Agency Head. The reference to section 215 in this recommendation is an error, and should in fact be section 225, as per para 3.81 & FN119 of the report.

[22] Section 62

Lord Anderson further noted that the operationalisation of ICRs has been slow, reflecting the fact that their collection and use is not straightforward.

He identified three potential capabilities of ICRs:

- To attribute communications with a known internet service to an individual device and user
- To identify the communications sites used by a subject of interest To gather intelligence on web-browsing activity on sites both suggestive of criminality and generally

Lord Anderson was asked to consider a specific issue relating to one of the conditions that needs to be satisfied in order to obtain ICRs.

Condition A, provided for section 62(3) of the IPA, is that it is necessary for one of the statutory purposes listed in section 61(7) to obtain the data to identify which person or apparatus was using an internet service where the service and time of use are already known but the identity of the user or apparatus is not.

This condition therefore enables target discovery. However there are concerns that it allows devices and users to be identified when they are already known to have contacted a site at a particular time, but does not permit new targets to be detected on the basis of visits to sites which might indicate criminality or a national security threat.

Lord Anderson concluded that intelligence services should have access to them, subject to appropriate safeguards, for the following reasons:

- They are likely to make a decisive contribution to the prioritisation and pursuit of national security and serious crime investigations
- They have particularly high potential in relation to common and hard to detect types of internet-enabled crime
- They are subject to several existing safeguards, and
- The intrusiveness of the proposed new power is no greater than existing powers

Lord Anderson proposed that additional safeguards would be appropriate, namely limiting the new power to the intelligence services and to national security and serious crime investigations.[23]

[23] Recommendation 5: a new condition should be inserted into section 62, so that UKIC can obtain ICRs when authorised by the Investigatory Powers Commissioner (IPC), when necessary and proportionate for a national security or serious crime investigation to detect persons or devices using specific internet services.

Data retention notices

Data retention notices (DRN) may be served on telecommunications operators by the Secretary of State requiring them to retain relevant communications data if it is necessary and proportionate for a purpose such as national security, the prevention of crime, or the prevention of death or injury. DRNs are subject to approval by a judicial commissioner.[24]

DRNs cannot require the retention of third party data, including applications or services running over the top of a provider's network, such as Google and Facebook.[25]

Lord Anderson was asked to consider a possible unintended consequence of the current drafting in relation to inbound roamers – users of a foreign SIM within the UK – in light of future technology that will mean 4G and 5G services being routed via the home network (ie outside the UK).[26]

The Review team were told by operators that the exclusion of inbound roamers from DRNs was intentional and that it would be costly and technically difficult to retain this kind of communications data.

Lord Anderson also acknowledged that it would be possible for inbound roamers to circumvent DRNs by using over the top services and encryption.[27]

However, he agreed with the Home Office's view that inbound roaming data is not comparable with other forms of third party data because it has traditionally been available to law enforcement, and that it would continue to be so were it not for the new technology.[28]

Changes to definitions

Lord Anderson was asked to review several definitions in the IPA to ensure that they remain fit for purpose. In particular, he was asked to look at the definition of communications data in section 261. He also considered the lack of definition of lawful authority for the purposes of section 11, which creates an offence of unlawfully obtaining communications data.

He noted widespread confusion over the definition of communications data, Another difficulty was distinguishing between content, which is excluded from the definition, and communications data.

24 IPA ss87-89
25 S87(4)
26 Para 5.9
27 Para 5.16
28 Recommendation 6: amend section 87(4) of the IPA to allow DRNs to be applied for in relation to inbound roaming data

Lord Anderson agreed with the Home Office's proposal to amend section 261 to increase clarity.[29]

He noted that the IPC felt that there were further practical issues with the current definition of CD, and suggested that other related clarifications should be considered.[30]

Section 11(3) provides a defence to the offence of unlawfully obtaining CD where the person acted in the reasonable belief that they had lawful authority. Lord Anderson noted that the lack of clarity may deter officers from seeking CD because of concerns that they may inadvertently commit a criminal offence. He set out the circumstances in which lawful authority to obtain CD is currently recognised by the code of practice – specific matters in the public interest and publicly or commercially available data – and suggested that they be placed on a statutory footing.[31]

Warrantry

Warrants for the most intrusive powers provided for by the IPA are subject to the 'double lock': they are issued by the Secretary of State and approved by a judicial commissioner. Warrants to intercept the communications of a parliamentarian are also subject to the additional approval of the Prime Minister (the 'triple lock').

Lord Anderson was asked to consider whether efficiency and resilience in the system could be improved.

Targeted equipment interference warrants

The first issue he considered was authorisation by the NCA of targeted equipment interference warrants, which enable access to communications by permitting interference (hacking) with devices or services. They can currently only be issued by the Director General of the NCA (where the warrant is sought by the NCA).[32] This can be delegated to a senior NCA officer designated for the purpose in an urgent case.

The Home Office proposed that the IPA should be amended to allow senior NCA officers to authorise these warrants, bringing it into line with other law enforcement organisations.

Lord Anderson agreed that this was clearly sensible.[33]

---

29 Recommendation 7: amend the definition of communications data in section 261(5) of the IPA so that the carve out for content does not apply in respect to subscriber data

30 Paras 6.13-6.14

31 Recommendation 8: introduce a statutory definition of lawful authority to obtain communications data to include certain situations where lawful authority is currently recognised by the code of practice

32 IPA Section 106

33 Recommendation 9: make provision for senior officers of the NCA other than the Director General to authorise targeted equipment interference warrants

Triple lock

Sections 26 and 111 provide for the triple lock, which requires the authorisation of the Prime Minister in addition to the Secretary of State and a judicial commissioner, in relation to interception warrants and targeted examination warrants[34] respectively.

There is no provision for the Prime Minister to delegate this function. The hospitalisation of the then Prime Minister in 2020 gave rise to questions as to whether such as power was needed.

Lord Anderson considered that such a need was obvious, suggesting that a deputy should be a Secretary of State, and that a list might include the Home Secretary, the Foreign Secretary, the Northern Ireland Secretary and the Defence Secretary.[35]

Notification of targeted EI warrant

Lord Anderson was also asked to consider whether the Secretary of State should have to be notified when the scope of a targeted EI warrant is reduced.

The IPA currently permits modifications to be made to the scope of these warrants, either by the Secretary of State, Scottish Ministers, or senior officials on their behalf.

Such modifications are required to be notified to a judicial commissioner when made by the Secretary of State or Scottish Ministers, unless they have the effect of reducing the scope of the warrant by removing names or other matters.

Modifications by senior officials are required to be reported to the Secretary of State or Scottish Government, even if they have the effect of reducing the scope of the warrant.[36]

Lord Anderson agreed with the Home Office that there is no obvious reason why the Secretary of State should be notified of the removal of something from the warrant.[37]

---

34 A warrant to authorise the selection for examination of protected material obtained under a bulk warrant.

35 Para 8.17. Recommendation 10: permit the use of a deputy for the purpose of the triple lock when the Prime Minister is unable to approve a warrant to the required timescale (in particular through incapacity, conflict of interest or inability to communicate securely)

36 Ss118-121

37 Recommendation 11: amend section 121 of the IPA so that section 121(3) does not apply to a modification of a targeted EI warrant where it is to remove any matter, name or description included in the warrant

Oversight

The IPA established the role of the IPC, supported by 17 judicial commissioners who are former senior judges, to provide oversight of the use of investigatory powers, including, but not limited to, those provided for by the IPA.

The Technical Advisory Panel (TAP) advises the IPC on the impact of changing technology and its impact on privacy.

Deputies and delegation

The IPC can delegate functions to a judicial commissioner, but this does not apply to the appointment of judicial commissioners and TAP members, or certain functions relating to the authorisation of access to communications data.[38]

The Home Office report noted that the Covid-19 pandemic had highlighted the need for resilience and flexibility in the approach to oversight. Lord Anderson agreed with a number of pragmatic proposals put forward by the Home Office to enable the appointment of deputies and the further delegation of functions:

- to make statutory provision for the IPC to nominate two deputies to whom functions may be delegated[39]
- deputy IPCs should be able to appoint judicial commissioners, members of the TAP and deputy IPCs when the IPC is unable to act within the required timescale[40]
- appeals should be capable of being determined by deputy IPCs when the IPC is unable to determine them[41]
- section 227(9A) of the IPA should be repealed, enabling the IPC to delegate the power to grant targeted authorisations for obtaining CD under s60A IPA , beyond circumstances where the IPC is unable to do so[42]
- deputy IPCs should have the power to appoint temporary judicial commissioners s when the IPC is unable to act within the required timescale[43]

38 Section 227
39 Recommendation 12
40 Recommendation 13
41 Recommendation 14. Appeals on the part of public authorities whose applications are refused by judicial commissioners
42 Recommendation 15.
43 Recommendation 16. The power to for the IPC appoint temporary JCs was provided for by the Coronavirus Act 2020

Prime Ministerial Directions

The IPC has expressed a wish that its non-statutory functions should be placed on a statutory footing.

The Prime Minister has a power under section 230 to give a direction to the IPC to keep under review the carrying out of any aspect of the functions of an intelligence service, a head of an intelligence service or any part of the armed forces or Ministry of Defence, so far as engaging in intelligence activities. This power does not extend to other public authorities.

The Home Office has proposed that the functions which may be the subject of a direction be extended to any public authority in so far as they engage in intelligence activities. Lord Anderson agreed with this proposal.[44]

Oversight of telecommunications restriction orders

Courts have a power to impose telecommunications restriction orders (TROs) for the purpose of preventing or restricting the use of mobile phones by those detained in custody.[45] The IPC is required by section 229(3)(c) of the IPA to keep the use of this power under review.

Lord Anderson agreed with the Home Office that this oversight function is of little value, given that TROs are always authorised by a judge.[46]

1.4 Consultation on the notices regime

The Home Office consulted on several proposals to change the notices regime contained in Parts 4 and 9 of the IPA in June 2023.[47]

The regime currently comprises three kind of notice which can be imposed on telecommunications operators by the Government:

- Data retention notices:[48] requiring the retention of communications data
- Technical capability notices:[49] requiring operators to provide and maintain technical capabilities enabling them to provide any assistance as required by an authorisation under the IPA

44 Recommendation 17: the list of bodies specified in section 230(1) whose intelligence related activities may be the subject of Prime Ministerial direction to the IPC should be expanded to include wider public authorities, so far as engaging in intelligence activities

45 Under the Serious Crime Act 2015

46 Recommendation 18: section 229(3)(c) should be repealed

47 Consultation on revised notices regimes in the Investigatory Powers Act 2016, Home Office, 2023

48 S87

49 S253

- National security notices:[50] require operators to take any steps considered necessary by the Secretary of State in the interests of national security. This may include providing services or facilities for the purpose of enabling the intelligence services to carry out their functions or deal with an emergency

These notices are subject to approval by judicial commissioners.[51] Their existence may not be revealed by the operator or their employees,[52] and it is Home Office policy not to confirm or deny the existence of a notice.[53]

The consultation noted that the power to issue notices was longstanding and that it was concerned with the efficacy of the existing regime rather than the creation of new powers.

It said that changes in technology and an increase in data being held overseas risked having a negative effect on the capabilities of law enforcement and intelligence agencies.

It identified a need for companies to work openly and willingly with governments to tackle threats such as child sexual exploitation and terrorism and suggested that the proposed changes were necessary to achieve this in light of rapid technological changes.

The consultation set out the proposed changes in the form of a series of "overriding objectives":

- Ensuring that a notice has effect during any period that it is under review, following an operator exercising its statutory right to request a review of a notice it objects to;[54]

- Requiring operators to cooperate with the consultation process that takes place before a notice is given, and with any subsequent review, including sharing relevant technical information;[55]

- Amending the extraterritorial application of notices to ensure that they apply to operators with complex corporate structures, with different legal entities in different jurisdictions, and the accompanying enforcement regime;[56]

- Requiring operators in some circumstances to notify the Government of planned technical changes to a service that could have a negative effect

50 S252
51 S254
52 S255(8)
53 Consultation on revised notices regimes in the Investigatory Powers Act 2016, Home Office, 2023
54 Objective 1
55 Objective 2
56 Objective 3

on investigatory powers, with a view to ensuring that access to data is maintained;[57]

- Requiring the Investigatory Powers Commissioner to consider the need to renew a notice, two years after the last time it was given, renewed or varied.[58]

[57] Objective 4. As the consultation notes, existing technical capability notices can include a notification requirements: Investigatory Powers (Technical Capability) Regulations 2018, sched 2, para 13

[58] Objective 5

2 The Bill

The Investigatory Powers Act (Amendment) Bill was announced in the King's Speech on 7 November 2023. The accompanying briefing said that the Bill would update the IPA and deliver "urgent changes" needed to protect the British people. It explained that the Bill would not create new powers, but would recalibrate aspects of the existing regime to ensure it is fit-for-purpose. It noted that the measures taken forward in the Bill reflect the Home Office review of the IPA and the recommendations of Lord Anderson's independent review.[59]

The Bill had second reading in the House of Lords on 20 November 2023. It was considered by a Committee of the whole House from 11-13 December and had report stage and third reading in January 2024.

It was introduced in the House of Commons on 31 January and will have second reading on 19 February.

The House of Lords Library published a briefing in advance of second reading: Investigatory Powers (Amendment) Bill [HL] (PDF)

Clause numbers refer to the Bill as introduced in the House of Commons: Bill 157

2.1 Bulk personal data sets

According to the explanatory notes, BPDs enable the intelligence agencies to cross reference fragmentary bits of intelligence in order to pull together an overall assessment.[60]

Since the IPA was passed, the volume and categories of data have expanded and the threat to the UK and its allies has diversified. As a result, the intelligence services need to acquire increasing volumes of data, much of which is publicly available, but are currently inhibited by the requirements of the IPA.[61]

The explanatory notes endorse Lord Anderson's conclusion that the IPA is restricting the intelligence services' ability to use machine learning, as well as

59 King's Speech 2023: background briefing notes, Prime Minister's Office, 7 November 2023
60 Explanatory notes to the Investigatory Powers Act (Amendment) Bill (PDF), para 16
61 As above, para 17

access to open resources. They explain that the training of machine learning models requires large quantities of data that is representative of the type of data on which the model is deployed, but is voluminous enough to overcome or minimise biases. The use of such models to assist the intelligence services with growing volumes of data aims to make the best use of resources in protecting national security, they say.[62]

Low or no expectation of privacy

Part 1 of the Bill would introduce a new process for retaining and examining BPDs in which there is a low or no expectation of privacy, by inserting a new Part 7A to the IPA.[63]

It would apply to datasets the nature of which is such that the individuals to whom the data relates could have no, or only a low, reasonable expectation of privacy in relation to the data. This would depend on all the circumstances, including:

- The nature of the data
- The extent to which is has been made public, either by the individual or with their consent
- Whether it was subject to editorial control, if published, or by a person acting in accordance with professional standards
- The extent to which it is widely known about, if published or in the public domain
- The extent to which it has already been used in the public domain[64]

New Part 7A would enable internal authorisations for this category of BPD, where the head of an intelligence service, or someone acting on their behalf, considers it necessary for the conduct of intelligence service functions and proportionate to what is sought to be achieved. Arrangements would also need to be in place for the secure storage of the BPD, and approved by the Secretary of State.

This would still be subject to approval by a judicial commissioner, unless the BPD falls within a category that is already authorised, or it is considered to be urgent.[65]

In an urgent case, a judicial commissioner would be required to decide whether to approve the decision within three working days of it being granted. If they refuse to approve the decision, the authorisation would cease

62 Explanatory notes to the Investigatory Powers Act (Amendment) Bill (PDF), paras 19-21
63 Clause 2
64 New s226A
65 New s226B

to have effect and the head of the intelligence service would be required to stop the use of the dataset as soon as possible.[66]

The head of an intelligence service or a person acting on their behalf would also be able to authorise the retention or examination of a category of BPDs in which there is a low or no expectation of privacy, subject to approval by a judicial commissioner. A category may, but would not necessarily, be defined by reference to the use to which the datasets would be put.[67]

Judicial commissioners would be required to review the decision to grant an authorisation on the basis that the BDP or category of BPD had a low or no expectation of privacy. This would be done applying the same principles as a court would in an application for judicial review (as with other 'double-lock' approvals in the IPA). They would further be required to do this with sufficient care so as to comply with the overarching requirements in section 2 to protect privacy.

If a judicial commissioner did not approve an authorisation, the decision maker could ask the IPC to approve the decision.[68]

Authorisations would generally last for 12 months after which they would cease to have effect unless renewed (on the basis that they continued to fulfil the original conditions), subject to approval by a judicial commissioner. Urgent authorisations would last for five days.[69]

The decision maker would be able to cancel the authorisation at any time, and would be required to do so if they considered that the conditions were no longer met.[70]

The heads of the intelligence agencies would be required to produce an annual report for the Secretary of State about the BPDs authorised under new Part 7A.[71] The Secretary of State would be required to provide an annual report to the Intelligence and Security Committee of Parliament (ISC) on the use of category authorisations.[72]

Bulk personal dataset warrants

The Bill would make some changes to the existing regime for BPD warrants in the IPA. It would change the duration from six months to 12,[73] and it would provide that certain functions conferred on the heads of the intelligence services could be carried out on their behalf by a Crown servant.[74]

66 New s226BC
67 New s226BA
68 New s226B
69 New section 226C
70 New s226CB
71 New s226DA
72 New s226DB
73 Clause 3
74 Clause 4

This reflects the fact that BPDs are often used to support long-term strategic intelligence activities. A longer duration would therefore enable the value of the BPD to be more accurately demonstrated, according to the explanatory notes.[75]

Allowing delegation to Crown servants reflects Lord Anderson's recommendations.

Third party bulk personal datasets

The Bill would also insert a new section 7B into the IPA, setting out a process for examining third party BPDs.

According to the explanatory notes, the intelligence services can currently access third party BPDs through "relevant information gateways" including the Intelligence Services Act 1994 and the Security Services Act 1989.[76] The Bill would therefore provide an explicit statutory regime, incorporating existing safeguards from Part 7. This reflects a recommendation from IPCO.[77]

It would apply to datasets to which the intelligence services have access, but are held electronically by a third party, provided they otherwise fulfil the definition of a BPD.

Access for this purpose would mean electronic access which is made available to the intelligence service as a result of arrangements with the third party, and is not generally available.[78]

Examination of a third party BPD would require authorisation by a warrant (referred to in the explanatory notes as a '3PD warrant'),[79] unless it is subject to a warrant or authorisation provided for elsewhere in the IPA.[80]

The head of an intelligence agency, or someone acting on their behalf, could apply to the Secretary of State for a warrant, who would be able to issue it if it was necessary for national security, serious crime, or economic well-being purposes (as with other BPD warrants in the IPA).[81]

The application would need to include a general description of the BPD,[82] and to note if it is known to include protected data, health records, sensitive personal data, or if its examination is likely to raise novel or contentious issues.[83]

---

75 Explanatory notes to the Investigatory Powers Act (Amendment) Bill (PDF), para 23

76 These piece of legislation set out the general functions of MI5, MI6 and GCHQ and were the first statutory acknowledgment of their existence.

77 Explanatory notes to the Investigatory Powers Act (Amendment) Bill (PDF), para 29

78 Clause 5, new s226E

79 New s226F

80 New s226FA

81 New s226G

82 New s226G(2)

83 New s226G(6). These categories of data are defined in ss202, 203, and 206 of the IPA.

As with other warrants and authorisations, the Secretary of State would need to be satisfied that the authorised conduct was proportionate; that there were satisfactory arrangements for storage of the data; and, a judicial commissioner must approve the warrant, unless it is urgent.[84]

When considering whether to approve the warrant the Judicial Commissioner would need to review the Secretary of State's conclusions as to its necessity and proportionality, applying the same principles as in an application for judicial review. A refusal would be subject to reconsideration by the IPC.[85]

The duration of a standard warrant would again be 12 months, subject to renewal or cancellation.[86]

Additional safeguards are set out which would require the Secretary of State to ensure that arrangements are in force to secure that any examination of data is necessary and proportionate in all the circumstances, having "regard to the information that is reasonably available to the intelligence services in relation to the examination of such data".[87]

The Secretary of State would also have to specifically approve criteria for the examination of data where the purpose or likely effect would be to identify legally privileged material relating to an individual in the UK. This would only be given if there were exceptional and compelling circumstances that made it necessary, and would be subject to approval by a judicial commissioner. In determining whether such circumstances existed, the Secretary of State would be required to consider whether the public interest in obtaining the information outweighed the public interest in the confidentiality of legally privileged material, and whether it was necessary in the interests of national security or preventing death or significant injury.[88]

If legally privileged material is retained following an examination, the IPC would be informed, and would then be responsible for determining whether it should be retained or used, weighing up the necessity and public interest.[89]

It would be an offence, subject to a maximum sentence of two years, to examine data in a third party BPD, knowing or believing that it was not necessary and proportionate.[90]

84 New s226G(4) & new s226GB
85 New s226GA
86 New ss226H-226HC
87 New s226IA
88 New s226IB
89 New s226IC
90 New s226ID. This is similar to an existing offence provided for by s224 IPA.

2.2 Oversight arrangements

Part 2 of the Bill would make amendments to the oversight regime contained in Part 8 of the IPA. According to the explanatory notes, these are intended to increase resilience and flexibility, and provide greater legislative clarity.[91]

It would provide that the IPC could appoint two judicial commissioners as deputy IPCs.[92] The IPC would be able to delegate certain functions to these deputy IPCs and to judicial commissioners.[93]

Certain functions, such as hearing an appeal or review of a decision made by a judicial commissioner, could only be delegated to a deputy when the IPC was unavailable.[94]

The Bill would also enable the IPC, with the agreement of the Secretary of State, to appoint temporary judicial commissioners in exceptional circumstances resulting in a shortage of persons able to carry out the role.[95]

As the explanatory notes state, this would replicate measures that were put in place during the Covid-19 pandemic by the Coronavirus Act 2020.

Some of the main functions of the IPC, set out in section 229, would also be amended by the Bill.[96] It would remove functions relating to the oversight of prevention or restriction of use of communications devices by prisoners.[97] It would place oversight of the Ministry of Defence's policies on the use of investigatory powers on a statutory footing.[98] It would enable the Prime Minister to direct the IPC to oversee other public authorities insofar as they are carrying out intelligence activities.[99] And, it would expand the scope of the IPC's error reporting function, whereby the IPC is required to inform individuals of errors by public authorities in the exercise of powers that have caused them serious harm or prejudice.[100]

Personal data breaches

A clause which was added to the Bill at report stage in the House of Lords would require the IPC to notify affected individuals of serious personal data breaches relating to warrants issued under the IPA, if it is determined to be in

91 Explanatory notes to the Investigatory Powers Act (Amendment) Bill (PDF, paras 57-59
92 Clause 7
93 Clause 8
94 New subsections (8A) & (8B) of s227
95 Clause 9, which would insert new s228A
96 Clause 10
97 S229(3)(c). As recommended by Lord Anderson. According to the explanatory notes, the county courts already provide judicial approval of this: Explanatory notes to the Investigatory Powers Act (Amendment) Bill (PDF), para 66.
98 New subsection 229(3E). This is currently overseen on a non-statutory footing
99 S230 currently lists the intelligence services, heads of the intelligence services, and the armed forces and Ministry of Defence
100 S321

the public interest.[101] It would apply when an operator was prevented from reporting a breach to the Information Commissioner, as would otherwise be required, because of a restriction imposed by the IPA. Judicial commissioners would be required to report the breach to the Information Commissioner.

Introducing the amendment, Lord Sharpe said that it would bring much-needed clarity in respect of how personal data breaches committed by operators are regulated. It would also ensure that there is a clear statutory basis for the Information Commissioner and the IPC to be notified.[102]

2.3 Communications data

Unlawfully obtaining communications data

Part 3 of the Bill would amend a number of provisions in the IPA relating to communications data.

Section 11 of the IPA created an offence of knowingly or recklessly obtaining communications data from an operator without lawful authority, which can be committed by a person working for a relevant public authority.

The explanatory notes say that the existing drafting of section 11 together with the complexity of the definition of communications data pose significant challenges to public authorities.[103]

The Bill would amend section 11 to make clear that the offence only applies in the context of obtaining data from a private sector operator. The explanatory notes say that the offence was created as a safeguard in this context and it was not intended to prevent data sharing between public sector organisations.[104]

The Bill would also insert into section 11 a list of examples of what would constitute lawful authority, bringing consistency with equivalent provisions concerning unlawful interception.

Definition of communications data

Section 261 of the IPA defines various terms, including communications data. The definition includes "entity data" (eg phone numbers and identifiers linked to customer accounts) and "events data" (eg the fact that someone sent a message), and specifically excludes the content of a communication.

---

101 Clause 11

102 HL Deb 23 January 2024, c698

103 Explanatory notes to the Investigatory Powers Act (Amendment) Bill (PDF), para 73

104 Clause 12. Explanatory notes to the Investigatory Powers Act (Amendment) Bill (PDF), paras 74-75

The explanatory notes say that there is currently insufficient clarity as to whether subscriber and account data is communications data or content.[105] The Bill would amend section 261 to make clear that subscriber and account data are not content, thereby creating a clear basis for their acquisition under the communications data provisions of the IPA.[106]

Powers to obtain communications data

Section 12 and Schedule 12 of the IPA abolished certain "general information powers" under which public authorities could obtain communications data from operators without their consent. The purpose was to ensure that communications data was obtained in accordance with the IPA.

According to the explanatory notes, this has resulted in a concern that several bodies with a regulatory or supervisory function may be unable to effectively perform their statutory functions. This would be the case either because they do not have IPA powers, or because they are unable to meet the serious crime threshold required for obtaining some types of communication data under the IPA.[107]

The Bill would amend section 12 to restore "general information powers" for regulatory or supervisory purposes, outside the context of a criminal investigation (for which the IPA process should be followed).[108]

Internet connection records

Internet connection records (ICRs) are classed as a category of communications data by the IPA, but are subject to additional access restrictions in recognition of their more intrusive nature.

They can be accessed by law enforcement and intelligence services to determine:

- Which sites or services have been accessed by a known subject of interest or device (subject/ target development)
- Which customers or devices have accessed a known site or service at a specified time (subject/ target identification)

There are concerns that the requirement to know both the site or service of interest, and the time it was accessed, for the purposes of subject identification could limit the utility of ICRs in this context, according to the explanatory notes.[109]

105 Explanatory notes to the Investigatory Powers Act (Amendment) Bill (PDF), paras 85-87
106 Clause 13
107 Explanatory notes to the Investigatory Powers Act (Amendment) Bill (PDF), paras 80-81
108 Clause 14
109 Explanatory notes to the Investigatory Powers Act (Amendment) Bill (PDF), para 117

The Bill would amend section 62 of the IPA, which sets out the (alternative) conditions that must be met in order to authorise access to ICRs, by adding an additional condition.[110] This would be that it is necessary for the relevant statutory purpose (such as the interests of national security or preventing serious crime) to identify the person or device that accessed a specified internet service in a specified period (rather than at a specific time).

The explanatory notes say that this would assist in identifying subjects of interest where serious criminality may be denoted by a specific pattern of connections.[111]

The new capability would be limited to the intelligence services and the NCA, who according to the explanatory notes have the appropriate expertise to formulate appropriate queries to derive the correct subset results.[112]

It also reflects the recommendations of Lord Anderson.

2.4 Notices

Part 4 of the Bill would amend the notices regime provided for in Parts 4 and 9 of the IPA. These reflect some of the proposals put forward in the Government's consultation, discussed above.

Third party data

Section 87(4) currently limits the types of communications data that can be required to be retained under a data retention notice, including providing that an operator cannot be required to retain data which relates to the use of a telecommunications service provided by another operator.

The Bill would amend section 87(4) to disapply it to data which is, or can only be obtained by processing, an ICR, or data that does not relate to a "relevant roaming service". A relevant roaming service is defined as a telecommunications service provided by an operator under an agreement with a non-UK operator, which facilitates access for those in the UK to services of the non-UK operator.[113]

These amendments would mean that these categories of data could be required to be retained under a data retention notice, where that would currently be prohibited by section 87(4).

110 Clause 15
111 Explanatory notes to the Investigatory Powers Act (Amendment) Bill (PDF), para 121
112 As above, para 124
113 Clause 16

The explanatory notes suggest these measures are intended to "address some discrete and unintended consequences which have unduly broadened the effect of that subsection".[114]

Enforcement

The Bill would amend the provisions of the IPA governing enforcement of data retention notices in order to provide that civil enforcement proceedings may be brought against a person subject to a duty under a notice, even if they are not in the UK.[115]

The explanatory notes say that this would "strengthen policy options when addressing emerging technology" and would make them consistent with technical capability notices. This is necessary in light of the increasing volume of data of interest held by international companies.[116]

The Bill would also provide that the duty not to disclose the existence of a technical capability notice or a national security notice is enforceable through civil proceedings, in line with the position for data retention notices.[117]

Review period

Under the IPA, an operator served with a notice can refer it to the Secretary of State for review, if dissatisfied with it.[118] During the review process there is no obligation to comply with the notice.

The explanatory notes say that if an operator was seeking to make changes to their system that would have a detrimental effect on a current lawful access capability during the review period, this could create a capability gap.[119]

The Bill would amend these provisions to require operators not to make any changes during the review period that would have a negative effect on the ability to comply with any warrant, notice, or authorisation given under the IPA.[120]

Meaning of telecommunications operator

The Bill would amend the definition of "telecommunications operator" in section 261 of the IPA. It would be expanded to include a system which is not

114 Explanatory notes to the Investigatory Powers Act (Amendment) Bill (PDF), para 38
115 Clause 17
116 As above, para 37
117 Clause 18(4)
118 Sections 90 and 257
119 Explanatory notes to the Investigatory Powers Act (Amendment) Bill, para 104
120 Clause 18

wholly or partly in or controlled from the UK, but which is used to offer or provide services to people in the UK.[121]

The explanatory notes say that this change of definition is being made out of an "abundance of caution" to ensure that obligations apply to all entities of a company, irrespective of where the entity providing the service or controlling the system is based.[122] This is necessary to ensure that large companies with complex corporate structures are covered in their entirety.[123]

Further amendments to section 253 are intended to ensure that a technical capability notice may be issued to one entity in relation to another entity's capability.[124]

Renewal of notices

The Bill would provide a new regime for the renewal of all types of notice after two years (provided the notice has not been varied so as to require additional obligations, renewed, or revoked before that point). The Secretary of State would need to consider the ongoing necessity and proportionality of the notice, and the decision would be subject to approval by a judicial commissioner.[125]

The explanatory notes say that this will increase oversight.[126]

Notification of proposed changes

The Bill would introduce a new power to issue a notice in the IPA. It would enable the Secretary of State to impose an obligation on an operator, requiring them to give notification of any changes to a service or system, as specified in regulations.

The Secretary of State would be required to consider whether the notice was necessary for maintaining the capability of the operator to provide assistance in relation to a warrant, authorisation or notice issued under the IPA. They would also need to consider if the conduct required was proportionate.[127]

As with other notices, consultation with the operator would be required prior to giving the notice, and there would be an obligation on the operator and its employees to keep the notice confidential, enforceable through civil proceedings.[128]

---

121 Clause 19

122 Explanatory notes to the Investigatory Powers Act (Amendment) Bill (PDF), para 102

123 As above, para 315

124 Clause 19(3). As above, para 316

125 Clause 20

126 Explanatory notes to the Investigatory Powers Act (Amendment) Bill (PDF), para 36

127 Clause 21

128 New section 258A(8)-(10)

The new power would apply to operators that provide assistance in relation to warrants, authorisations or notices under the IPA. The explanatory notes say that this is to ensure the requirement does not disproportionately affect all operators.[129]

2.5 Other provisions

Part 5 of the Bill contains various miscellaneous provisions.

Warrantry

Warrants are required in order to exercise certain powers under the IPA, including interception and equipment interference. These generally require approval from the Secretary of State or the Chief Constable of a police force and a judicial commissioners, and in some instances, the Prime Minister.

Members of relevant legislatures

Currently, certain warrants targeted at members of relevant legislatures[130] are subject to the 'triple lock' process, which requires the authorisation of the Prime Minister, in addition to the Secretary of State and a judicial commissioner. These are targeted interception warrants,[131] and warrants for targeted equipment interference or examination.[132]

The explanatory notes say that under these arrangements, critical intelligence gathering opportunities may be lost as a result of Prime Ministerial unavailability.[133]

The Bill would amend the relevant provisions to provide that when the Prime Minister is unavailable, another Secretary of State could be designated to approve these warrants if the decision is urgent.[134]

Equipment interference

Targeted equipment interference warrants required for serious crime purposes or preventing death or serious harm are currently issued by certain "law enforcement chiefs" listed in Schedule 6, with the approval of a judicial commissioner.[135] Where necessary, this function can be delegated. The Bill would add a Deputy Director General of the NCA to the list of law enforcement chiefs who are able to delegate this function in Schedule 6.[136]

---

129 Explanatory notes to the Investigatory Powers Act (Amendment) Bill (PDF), para 324
130 Members of Parliament and the devolved legislatures
131 S26
132 S111
133 Explanatory notes to the Investigatory Powers Act (Amendment) Bill (PDF), para 52
134 Clauses 22 & 23
135 S106
136 Clause 24

The explanatory notes say that the policy objective of the proposal is to improve the resilience of the process and ensure warrants are not reliant on a "potential single point of failure" in the process.[137]

The Bill would also correct some drafting errors and inconsistencies in relation to the equipment interference provisions in the IPA.[138]

Safeguards for journalistic material

Where material obtained under a bulk equipment interference warrant is retained, and includes confidential journalistic material, the IPA currently requires the subject of the warrant to inform the IPC.[139]

The Bill would replace the existing provision with a requirement for prior authorisation from the IPC before criteria can be used to select material obtained under a bulk equipment interference warrant for examination. This would apply where the purpose was to identify confidential journalistic material or confirm a source, or where the criteria mean that this outcome is highly likely.[140]

In urgent cases the approval could be given by a senior official with the IPC informed subsequently.[141]

Legal proceedings

Currently, the IPA provides that intercept material cannot be used in any legal proceedings.[142] Schedule 3 lists a number of exceptions to this rule.

The Bill would add further exceptions to Schedule 3, including proceedings before the parole board in England and Wales relating to the release of prisoners, and inquests and inquiries and inquests in Scotland and Northern Ireland.[143]

Freedom of information

The Freedom of Information Act 2000 (FOIA) provides a general right of access to information held by public bodies.

IPCO is not listed as a public authority for the purposes of FOIA and information it holds is therefore not subject to that general right. However, information shared by IPCO with other public bodies may be accessible.

137 Explanatory notes to the Investigatory Powers Act (Amendment) Bill (PDF), para 53
138 Clauses 25-26. See Explanatory notes to the Investigatory Powers Act (Amendment) Bill (PDF), paras 54-56
139 S195
140 Clause 27, inserting new s195
141 New s195A
142 S56
143 Clause 28

The Bill would add judicial commissioners to the list of bodies in section 23 of FOIA, which provides an absolute exemption for all information supplied by, or relating to, certain bodies dealing with security matters.[144]

[144] Clause 29

3 Proceedings in the House of Lords

3.1 Second reading

Introducing the Bill, Lord Sharpe, Parliamentary Under-Secretary of State at the Home Office, explained that the Bill sought to make targeted amendments to the IPA in order to support the security and intelligence services to keep pace with a range of evolving threats and technological advancements. He also said that the Bill would maintain and strengthen "world-leading safeguards".[145]

Lord Coaker (Lab) said that the Opposition fully supported the Bill, but that it would need to be "cautiously challenged" in Committee, given the fundamental rights at stake. He raised a number of issues requiring further scrutiny, including how a low expectation of privacy would be defined; why the new ICR power should be available to law enforcement, rather than just the intelligence services as recommended by Lord Anderson; and the relationship between the Bill and data protection law.[146]

Lord Fox (LD) outlined three principles that would inform his party's response to the Bill: there should be no weakening of encryption; the role of judicial authorisation is vital; and, in relation to bulk powers, the British public are entitled to expect privacy.[147] He expressed concern that the Bill could "push legislation further past the point of balance", but said that his comments were intended in the spirit of constructive support for the Bill.[148]

Lord Anderson (CB) suggested that were a few points that he might seek to probe in Committee, but he described the Bill as "an honest attempt to strike a fair balance in these difficult areas", and suggested that operational gains might be compromised if the Bill was radically amended.[149]

145 HL Deb 20 November 2023, c620
146 HL Deb 20 November 2023, c626
147 As above, c629
148 As above, c631
149 As above, c633

3.2 Committee

There were no divisions in Committee. Members of the House of Lordstabled probing amendments on a number of issues and the Government tabled some minor and technical amendments which were agreed.

Low or no expectation of privacy

In Committee Lord Coaker and Lord Fox tabled probing amendments seeking to explore inconsistencies between the definitions of datasets with low or no expectation of privacy in the Bill and equivalent concepts in the Data Protection Act (DPA), and the relationship between the two regimes.

Lord Sharpe responded, explaining that using the same terminology as the DPA would risk creating a link between BPDs retained under the Bill's provisions and the processing of sensitive data under the DPA, where none existed. He suggested this would risk doing more harm than good.[150]

Lord Sharpe also explained that the law concerning the reasonable expectation of privacy is likely to develop over time, and that the Bill is designed to be sufficiently flexible to accommodate that.[151]

Lord Fox also tabled amendments that would have required urgently granted BPD authorisations to be reported to a judicial commissioner immediately.

Oversight of BPDs

Probing amendments were also tabled aimed at improving oversight of the new bulk personal dataset regime by requiring annual reports on the use of the powers to be sent to the Intelligence and Security Committee and IPCO.

In response to the amendments aimed at improving oversight, he suggested that they were not necessary, given that the IPC would have oversight of the regime anyway, and that the ISC has a well established role in the oversight of the agencies to whom the Bill would apply.[152]

Notices

Lord Fox opposed certain clauses concerning notices. These were the clauses that would extend extraterritorial enforcement powers for data retention notices, govern the process for reviewing notices, and allow the Secretary of State to impose notices on operators requiring notification of changes.[153] He said that these proposals had raised a huge amount of external concern because of the implications for end-to-end encryption. He also tabled

150 HL Deb 11 December 2023, c1740
151 As above, c1741
152 As above, cc1745-46
153 Clauses 16, 17 and 20 in the Bill as introduced in the Lords

amendments aimed at ameliorating the effect of the notices regime in order to address concerns, as did Lord Coaker.

Lord Fox suggested that the Bill would allow the Government to block, in secret, the release of a product or service, before a notice could be independently reviewed. He expressed concern at the effect on legal users of encryption services, and about the message sent to authoritarian regimes by the inclusion of a provision enabling forced decryption. Lord Fox also suggested that the extraterritorial reach of the provisions would cause conflict with laws in other jurisdictions.[154]

Lord Sharpe pointed to the requirements of necessity and proportionality, and the double lock process as safeguards, and suggested that some of the concerns raised were misplaced. He also emphasised that the process of imposing notices was intended to be consultative, and that enforcement was a last resort.[155]

In response to an amendment tabled by Lord Coaker which sought to place the double lock requirement on notification notices, Lord Sharpe said it was not necessary because these notices do not intrude on privacy.

The Government tabled amendments to provide that the Investigatory Powers Tribunal can consider complaints about notification notices in the same way as other notices in the IPA. These were agreed without debate, along with some minor drafting amendments.[156]

Triple lock

Lord West (Lab; member of of the ISC) tabled amendments which would specify that the only exceptional circumstances in which the Prime Minister would be permitted to use a designate to approve a warrant would be incapacity or lack of access to secure communications. He suggested that the provision should be restricted to situations where the Prime Minister was genuinely unable to take a decision. The amendments would also provide that only the Secretaries of State with current warrantry powers should be available as designates, and that the Prime Minister would review the decision as soon as possible.[157]

Similar amendments were tabled by Lord Hope and Lord Anderson, and by Lord Coaker.

Lord Sharpe responded by pointing out that the draft code of practice contained examples of circumstances in which the Prime Minister was unavailable, noting that they were consistent with the proposed amendment.

154 HL Deb, 11 December 2023, c1763-64
155 As above, cc1767-68
156 Amendments 33 and 40-42
157 HL Deb 13 December 2023, cc1898-1900

He suggested the current drafting would be applied in this way, but allowed more flexibility for unforeseen circumstances.

3.3 Report and third reading

At Report stage, Lord Fox tabled an amendment that would require a person granting an urgent authorisation in relation to a BPD to notify a judicial commissioner within, at most, 24 hours.

He noted that the three day deadline proposed in the Bill would enable the intelligence services to spend that time interrogating a dataset which might be found to be unlawful.

Lord Sharpe said that the Government remained opposed to the amendments because they would create inconsistency with other parts of the IPA and risk operational confusion. He also said that it may not be practical in an urgent operational context to deal with the paperwork.[158]

There was a division on the amendment and it was disagreed by 227 votes to 201.[159]

Lord West again tabled amendments which would provide for ISC oversight of BPD authorisations. The Government also tabled an amendment which would place a statutory obligation on the Secretary of State to provide the ISC with an annual report on category authorisations granted under the new Part 7A of the IPA. Lord Sharpe explained that the amendments tabled by Lord West would not appropriately address the issue, because the information required in the annual report to the Secretary of State would not necessarily be the same as that required by the ISC, reflecting their different functions. This amendment was agreed.[160]

The government tabled further amendments relating personal data breaches (discussed above at 2.2), as well as further clarifications and corrections.

Lord West also re-tabled amendments aimed at limiting the circumstances in which the Prime Minister could designate a Secretary of State to approve warrants on their behalf, and to limit the Secretaries of State to whom this would apply. Lord Anderson also re-tabled amendments on the issue of designating Secretaries of State, which would replace the word "unavailable" with "unable" with respect to the Prime Minister.

Lord Sharpe explained that the Government opposed Lord Anderson's amendment because it would introduce a requirement to make a judgment on the Prime Minister's ability to consider a warrant application. He said this

158 HL Deb 23 January 2024, c692

159 As above, cc694-696

160 HL Deb 23 January 2024, c690. This was Government amendment 4, now new s226DB of the IPA, as inserted by clause 2 of the Bill

would go against clear constitutional principles regarding the Prime Minister's powers.[161]

However, he indicated that the Government was able to support Lord West's amendments, and they were therefore agreed (subject to possible drafting clarifications).[162]

Another Government amendment was agreed which would replace the existing section 195 of the IPA to provide for prior judicial approval before any confidential journalistic materials are selected for examination, having been obtained via a bulk equipment interference warrant.[163]

Lord Sharpe noted that this would bring the bulk equipment interference regime into alignment with bulk interception, which is currently being amended the same way via the Investigatory Powers Act 2016 (Remedial) Order 2023.

No further amendments were made at third reading.

161 As above, c728

162 Amendments 39 and 41

163 As above, c730

4 Commentary

The Bill engages fundamental rights, in particular the right to privacy under Article 8 of the European Convention on Human Rights.[164] As such, it has provoked a long standing debate about the correct balance to be struck between privacy and security. Its provisions on notices have proved the most controversial, with privacy campaigners and technology companies in particular.

A joint briefing by Big Brother Watch, Liberty, Open Rights Group, Rights and Security International, Privacy International and the Internet Society highlighted a number of concerns, including that it would:

- Weaken safeguards around BPDs, potentially allowing intelligence agencies to "harvest millions of facial images and social media data"
- Permits the processing of ICRs for "generalised, massive surveillance"
- Expand the range of politicians that can authorise the surveillance of parliamentarians, and
- Force technology companies, including those based overseas, to inform the Government of plans to improve security or privacy measures[165]

Apple wrote to Peers during the passage of the Bill objecting to the notice provisions and the proposal for extraterritorial enforcement. It said

> The Home Office's proposals to expand the IPA's extraterritorial reach and to grant itself the power to pre-clear and block emerging security technologies constitute a serious and direct threat to data security and information privacy. To ensure that individuals have the tools to respond to the ever-increasing threats to information security, the Home Office's proposal should be rejected.[166]

Responses to the notices consultation

The Government's response to the notices consultation says that most respondents commented on the proposal relating to a notification notice, and on the potential impact on end-to-end encryption. The response also noted that the majority of responses were from members of the public as a result of a campaign by Open Rights Group and were therefore broadly consistent in their content.

164 Home Office ECHR memorandum, November 2023
165 Joint Briefing on the Investigatory Powers (Amendment) Bill, January 2024
166 HL Deb 20 November 2023, c 649

The predominant objection was that the proposal would allow the Home Office to veto or block the roll out of new technology, or pre-emptively direct the design of products and services.

The Government rejected this argument, noting that the IPA already provides for a notification requirement within the notices regime, and that the new requirement will not enable the Secretary of State to prevent a technical change to an existing service or the roll out of a new service.[167]

Addressing the specific concerns about end-to-end encryption, it said

> The government has always been clear on its position on private and secure communications technologies, including encryption. We fully support the responsible use of strong encryption, including end-to-end encryption, where public safety is designed in. We know it is possible to implement end-to-end encrypted services in a way which is consistent with public safety.

However, it went on to say that end-to-end encryption and other privacy technologies had severely eroded the ability of law enforcement and intelligence agencies to detect and disrupt the most serious crimes and threats to national security. Further, it said that tech companies have "a moral duty to ensure they are not blindfolding themselves from abhorrent crimes".

It pointed to a joint statement signed in 2020 by the Governments of Australia, Canada, India, Japan, New Zealand, the USA and the UK on encryption and public safety as evidence that the UK's position is not unique.[168]

Joint Committee on Human Rights

The JCHR undertook scrutiny of the Bill and wrote to the Home Secretary on 6 March noting a few points that could benefit from further clarification, whether on the face of the Bill, in undertakings to the House, or in policy documents.[169] These included:

- Greater clarity to help understand the sorts of things within and outwith the scope of the low or no expectation of privacy category of BPDs.
- A child rights analysis should be undertaken for all of the powers in the IPA and the Bill, explaining any impact on children and how this will be factored in to decision making.
- Clarity as to whether third party dataset warrants will only be sought where they have been lawfully obtained.

---

167 Government response to the Home Office consultation on revised notices regimes, Home Office, 8 November 2023

168 International Statement: end-to-end encryption and public safety

169 Letter to James Cleverly from the Chair of the Joint Committee on Human Rights, 6 March 2024

- A commitment that notice requirements will not cover, impede or delay essential security upgrades, including placing these guarantees on a clear legal footing.

5 Progress of the Bill in the House of Commons

The Bill had second reading in the House of Commons on 19 February 2024. It had two Committee sittings on 7 March. Report stage is scheduled for 25 March.

5.1 Second reading debate

The Bill was broadly welcomed at second reading, as was the Government's acceptance of amendments promoted in the House of Lords by members of the Intelligence and Security Committee (ISC).

Shadow Home Secretary Yvette Cooper said that the Bill was necessary because of fast moving technology and the need to avoid the security services to be outpaced. She accepted the need for most of the proposed changes without caveat, but indicated that she would press the Home Secretary on the need to update the memorandum of understanding between the Prime Minister and the ISC.[170]

Stuart Mc Donald (SNP) said that his party had concerns that certain provisions represented a significant expansion of what are "already extraordinarily wide powers by international standards". He raised in particular the proposals in relation to bulk personal datasets and the notices regime, as well as internet connection records, and authorisation for obtaining the communications of parliamentarians.[171]

Dr Julian Lewis (Con), Chair of the ISC, said that the Committee welcomed the Bill, having been able to take classified evidence, and to scrutinise the case put forward by the intelligence agencies and the Government. However, he said any expansion of powers should be accompanied by increased oversight. He also said that the ISC had an "overarching concern about the diminution of parliamentary powers in respect of national security".[172]

170 HC Deb, 19 February, 2024 c527-530
171 As above, c532
172 As above, c543

5.2 Committee stage

Amendments made

Four substantive Government amendments were made to the Bill in Committee:[173]

- Amendments 1 and 2 would amend clause 11, which would enable the IPC to be informed of serious personal data breaches relating to warrants issued under the IPA, and to notify affected individuals if it is determined to be in the public interest.

  They would provide that the Investigatory Powers Tribunal (IPT) has the jurisdiction to consider and determine complaints about personal data breaches committed by telecommunications operators and grant a remedy.

  The Security Minister, Tom Tugendhat, said that the IPT already has significant experience of considering complaints from individuals who believe they have been the victim of unlawful interference by public authorities, and as a result is the appropriate forum to consider such complaints.[174]

  The amendment was agreed without a division.

- Amendments 3 and 4 would amend clauses 22 and 23, which would enable a Secretary of State to authorise warrants relating to parliamentarians in certain specified circumstances when the Prime Minister is unavailable.

  They would replace the existing requirement in the Bill that the Secretary of State in question issues warrants as part of their routine duties, with one that they have the necessary operational awareness.

  The Minister said that the existing wording, inserted by the Lords, was over-restrictive and would undermine the resilience of the triple-lock. He said the amendment would ensure resilience and flexibility while maintaining a proportionate scope for delegation.[175]

  In response to questions as to what would constitute being "operationally aware", the Minister explained that it would be people who were "briefed into the warrantry process", and that the requirement would be detailed further in a code of practice. He said that the Government envisaged the four alternative approvers to be the Home

[173] Other amendments were minor or technical

[174] PBC 7 March 2024, c30

[175] PBC 7 March 2024, c57

Secretary, the Foreign Secretary, the Defence Secretary and the Northern Ireland Secretary.[176]

Other issues debated

There was debate about several other issues, which did not lead to divisions, but may return at Report stage. These included:

- Amendments tabled by Dan Jarvis, Shadow Security Minister, which would amend clause 2 to require that the IPC be notified when a new bulk personal dataset is added by an intelligence agency to an existing category authorisation.[177] The amendment was supported by Kevan Jones and Sir John Hayes, members of the ISC, who explained that the intention was not to create another form of authorisation, but a light touch process to support oversight. A similar amendment was tabled by Stuart McDonald, which would require the ISC to be provided with information about the scale and nature of use of category authorisations.[178] The Minister said the amendments were unnecessary, but committed to further discussion.[179]

- During the stand part debate on clause 15, concerning the new condition for accessing internet connection records, Stuart McDonald suggested, with the support of Kevan Jones, that judicial oversight should be required, rather than internal authorisation. In response, the Minister said that there was judicial oversight in place in the form of the IPC's inspection function. He also said that it was important to balance the ability to act quickly with the ability to be controlled from outside when considering oversight mechanisms. He pointed to the fact that anyone using the powers would have to exercise them in accordance with the principles of necessity and proportionality.[180]

- Amendments tabled by Dan Jarvis, which would amend clauses 22 and 23 to require that where a Secretary of State performs the 'triple lock' function due to the unavailability of the Prime Minister, the Prime Minister should be notified as soon as reasonably practicable.[181] He said that the Opposition believe that the Prime Minister's overall involvement in the process should be retained, even if it was retrospective. The Minister said that the requirement was unnecessary because it was "inconceivable" that the Prime Minister would not be notified in such circumstances. He said he would look at putting the requirement in guidance.[182]

176 As above, c59
177 Amendment 15
178 Amendment 38
179 PBC 7 March 2024, cc18-22
180 PBC 7 March 2024, cc37-49
181 Amendments 17 and 18
182 As above, cc60-61

The House of Commons Library is a research and information service based in the UK Parliament. Our impartial analysis, statistical research and resources help MPs and their staff scrutinise legislation, develop policy, and support constituents.

Our published material is available to everyone on commonslibrary.parliament.uk.

Get our latest research delivered straight to your inbox. Subscribe at commonslibrary.parliament.uk/subscribe or scan the code below:

commonslibrary.parliament.uk

@commonslibrary