# INVESTIGATORY POWERS (AMENDMENT) BILL [HL]

# EXPLANATORY NOTES

## What these notes do

These Explanatory Notes relate to the Investigatory Powers (Amendment) Bill [HL] as brought from the House of Lords on 31 January 2024 (Bill 157).

- These Explanatory Notes have been prepared by the Home Office in order to assist the reader of the Bill. They do not form part of the Bill and have not been endorsed by Parliament.
- These Explanatory Notes explain what each part of the Bill will mean in practice; provide background information on the development of policy; and provide additional information on how the Bill will affect existing legislation in this area.
- These Explanatory Notes might best be read alongside the Bill. They are not, and are not intended to be, a comprehensive description of the Bill.

# Table of Contents

## Commentary on provisions of Bill 33

# List of Acronyms and Abbreviations

3PD – Third Party Bulk Personal Dataset

BPD – Bulk Personal Datasets

CD – Communications Data

CHIS – Covert Human Intelligence Sources

CSA – Child Sexual Abuse

CJEU – Court of Justice of the European Union

DIPC – Deputy Investigatory Powers Commissioner

DG – Director General

DRN – Data Retention Notice

EI – Equipment Interference

FOIA – Freedom of Information Act 2000

HRA – Human Rights Act

ICRs- Internet Connection Records

IPA 2016 – Investigatory Powers Act 2016

IPC – Investigatory Powers Commissioner

IPCO – Investigatory Powers Commissioners Office

JC – Judicial Commissioner

ML – Machine learning

MOD – Ministry of Defence

NCA- National Crime Agency

NSN – National Security Notices

OCDA – Office for Communications Data Authorisations

Ofcom – Office of Communications

PECR – The Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI/2003/2426)

PO – Postal Operator

RIPA – Regulation of Investigatory Powers Act 2000

RIP(S)A – Regulation of Investigatory Powers (Scotland) Act 2000

TAB – Technical Advisory Board

TCN – Technical Capability Notice

TEI – Targeted Equipment Interference

TXEI – Targeted Examination Equipment Interference

TO – Telecommunications Operator

TRO – Telecommunications Restriction Orders

# Overview of the Bill

1. The Investigatory Powers (Amendment) Bill updates elements of the Investigatory Powers Act 2016 (IPA 2016) to ensure the United Kingdom's (UK) investigatory powers framework remains fit for purpose in the face of evolving threats.

2. The introduction of this Bill follows the publication of the Home Secretary's statutory report on the IPA 2016 in February 20231, and a subsequent independent review by the former Independent Reviewer of Terrorism Legislation, Lord Anderson of Ipswich KBE KC, published in June 20232. These reports set out the case for change and Lord Anderson's report broadly endorsed the proposed policy approaches.

3. The key objective of the Bill is to make targeted reforms to the IPA 2016 to ensure that it remains fit-for-purpose for intelligence services, law enforcement and other public authorities.

4. The main elements of the Bill are:

    a. Changes to the Bulk Personal Dataset (BPD) regime, which will improve the intelligence services' ability to use less sensitive datasets (such as publicly and commercially available data).

    b. Placing the intelligence services' examination of bulk personal datasets held by third parties (i.e. an external organisation outside of the intelligence services) on a statutory footing. If the examination was of datasets retained by intelligence services, existing provisions in the IPA 2016 would apply.

    c. Changes to the Notices regimes, which will help the UK anticipate and develop mitigations against the risk to public safety posed by multinational companies rolling out technology that precludes lawful access to data for the statutory purposes set out under the IPA 2016.

    d. Creating a new condition for the use of Internet Connection Records by the intelligence services and the National Crime Agency (NCA).

    e. Improvements to the oversight regime to support the Investigatory Powers Commissioner (IPC) to effectively carry out their role, including powers to enable the IPC to delegate some of their functions to Judicial Commissioners (JCs), appoint deputies and putting certain functions on a statutory basis.

    f. Measures to increase resilience of the warrantry authorisation processes for the intelligence services as well as for the NCA.

    g. Changes to the Communications Data regime to provide greater certainty on the circumstances for lawful data acquisition.

---

[1] Home Office report on the operation of the Investigatory Powers Act 2016 (accessible version) - GOV.UK (www.gov.uk)

[2] Independent review of the IPA 2016 (publishing.service.gov.uk)

# Policy background

5. The IPA 2016 was introduced to provide a clear legal framework for the intelligence services, law enforcement, and other public authorities to obtain and utilise communications, and data about communications, where it was deemed necessary and proportionate and in line with the statutory purposes set out in the Act.

6. These powers, supported by safeguards, play an integral part in helping to keep the public safe from a range of threats including terrorism, state threats, and serious and organised crime, such as child sexual abuse and exploitation.

7. Since the introduction of the IPA 2016, the world has changed. Technology has advanced, and the type of threats the UK faces continue to evolve. The Investigatory Powers (Amendment) Bill therefore seeks to make targeted changes to the IPA 2016 to support the intelligence services in keeping pace with a range of threats against a backdrop of accelerating technological advancements, which provide new opportunities for criminals such as terrorists, hostile state actors, child abusers, and criminal gangs.

8. As per section 260 of the IPA 2016, the Home Secretary conducted a Statutory Review of the functioning of the Act. The report on the findings of this review was published in February 2023[3]. The overarching conclusion of the review was that parts of the Act were inhibiting the ability of the intelligence services to keep the country safe from both current and evolving threats.

9. Engagement with law enforcement, the intelligence services, wider public authorities, and government departments found that, while in high-level terms the IPA 2016 has broadly achieved its aims, there is a case for immediate legislative change to some targeted parts of that Act.

10. To complement the Home Secretary's review and noting the value of the independent scrutiny that informed the passage of IPA 2016, the Home Secretary appointed Lord Anderson to conduct an independent review into the Act to inform any potential legislative change.

11. Lord Anderson's review was entirely independent from the Home Secretary's statutory review. His subsequent report on his review, published in June 2023, focused on the effectiveness of the bulk personal dataset regime, criteria for obtaining internet connection records, the suitability of certain definitions within the IPA 2016, and the resilience and agility of warrantry processes and the oversight regime.

12. The measures being taken forward in the Investigatory Powers (Amendment) Bill have been driven by the Home Secretary's review and the recommendations made in Lord Anderson's report.

# Bulk Personal Datasets (BPDs)

13. The retention and examination of bulk personal datasets (BPDs) by the intelligence services is regulated by Part 7 of the IPA 2016. This defines a BPD as a set of information that includes personal data relating to a number of individuals, the nature of the dataset is such that the majority of the individuals are unlikely to be or to become of interest to the intelligence services, and that is retained electronically by an intelligence service and held for analysis in the exercise of

[3] Home Office report on the operation of the Investigatory Powers Act 2016 (accessible version) - GOV.UK (www.gov.uk)

its statutory functions.

14. Part 7 sets out the safeguards that apply to BPDs. All datasets that meet the current definition of a BPD may only be retained and examined under a warrant that has been subject to prior judicial authorisation under the "double lock" authorisation process. BPD warrants are currently valid for six months.

15. The "double lock" authorisation process requires warrants authorised by the Secretary of State to be approved by an independent JC before warrants can be issued.

16. BPDs are used by the intelligence services in multiple different ways; for example, to provide 'building block' intelligence, such as names, dates, communication identifiers, details of travel, associates, etc. Traditionally, the critical value of a BPD is in the ability to make targeted queries of the data (for example, to identify a subject of interest), cross-reference them with other BPDs and then overlay the results with other data from a variety of sources, (such as intelligence derived from other investigatory powers). This allows analysts to pull together an assessment on the possible meanings of the fragmentary intelligence that the intelligence services receive.

17. Since IPA 2016 entered into force there has been a considerable growth in volume and types of data across all sectors of society globally, and at the same time the threat to the national security of the UK and its allies has diversified (as set out in the Integrated Review Refresh 2023[4]). The information the intelligence services require to disrupt threats is increasingly fragmented amongst growing and varied data.

18. The Home Secretary's Statutory Review of the functioning of the Act stated that limitations within the IPA 2016 are inhibiting the intelligence services' ability to maximise the benefits of digital transformation, and to ultimately protect national security. The intelligence services need to acquire increasing quantities of data, much of which is publicly available. It is anticipated that the data will improve analysis and in particular will enable the development of machine learning capabilities at the pace and scale the intelligence services need to identify and disrupt threats.

19. As set out in Lord Anderson's review of the IPA 2016 is restricting the intelligence services' ability to make use of machine learning (ML) (including training to avoid biases) to support human lead analysis and to manage increasing volumes of data and increase speed and quality of human decision making. It also restricts access to open resources such as telephone directories which can still be valuable for the more traditional uses of BPD.

20. The training of ML models requires large quantities of open source or publicly available data that is representative of the type of data on which the model will be deployed, but which is voluminous enough to overcome or minimise any inherent biases.

21. Unlike traditional uses for BPD, when training ML models the intelligence services do not examine the data to look for information on specific individuals featured in the data. Instead, BPDs are used for ML because they are representative examples of the structure or attributes of data the intelligence services are interested in. For example, the intelligence services may want to build a model to be able to identify weapons within images; the model will do this by learning from the training data features that make types of weaponry similar. Such models can be used to scan and triage images, before they are passed to human experts to assess. Developing models that can assist the intelligence services with growing volumes of data aims to make best use of

[4] Integrated Review Refresh 2023: Responding to a more contested and volatile world - GOV.UK (www.gov.uk)

resources in protecting national security.

22. In his *Independent Review of The Investigatory Powers Act 2016*[5] Lord Anderson made the following recommendations, which are being taken forward via this legislation:

    a. That IPA 2016 Part 7 should be amended to recognise a new category of BPDs in respect of which there is a low or no expectation of privacy, to which a distinct and less onerous set of safeguards should apply.

    b. That IPA 2016 s213 be amended to provide that BPD warrants cease to have effect 12 months after they were issued, unless they have already been renewed or cancelled.

    c. That IPA 2016 ss202, 206, 215, 219 and 220 (but not s210) be amended so as to provide explicitly that the functions with which they are concerned may be exercised by a Crown servant on behalf of an agency head.

23. Building on these findings, the Government is seeking to bring forward a narrow set of provisions that would:

    a. Amend safeguards for the retention and examination of BPDs where there is low or no reasonable expectation of privacy. This will create a new regime alongside the current Part 7. The intention of these changes is to enable the intelligence agencies to make more effective and efficient use of datasets in respect of which individuals have low or no expectation of privacy (such as online encyclopaedias and content from established news media).

    b. Amend IPA 2016 s213 to allow for the extension of the duration of a BPD warrant from 6 to 12 months. Currently BPD warrants need to be renewed every 6 months. BPDs are often used to support long-term strategic intelligence activities rather than short-term tactical actions. The aim of introducing a longer warrant duration is to enable the value of the BPD to be more appropriately and accurately demonstrated.

    c. Make clear that agency heads can delegate certain existing functions in relation to BPD warrants. This would enable agency heads to delegate certain functions to an appropriate Crown servant, whilst still being accountable for decisions that are taken on their behalf. The agency heads would still be required to personally carry out functions where risks are higher (such as under the existing duty in s210 to cease activity where a judicial commissioner refuses to sign off an urgent BPD warrant and the agency head must ensure the activity ceases).

## Third Party Bulk Personal Datasets (3PD)

24. A third party bulk personal dataset (3PD) is a dataset which would fall within Part 7 of IPA 2016 if an intelligence service were to retain it, but which is instead held by a third party (such as Government departments or commercial entities). The Bill seeks to insert a new 3PD regime into the IPA 2016 that would apply where an intelligence service has relevant access to the 3PD and examines it in situ (that is, on the third party's systems) for the purpose of their statutory functions (see the Security Service Act 1989 and the Intelligence Services Act 1994).

25. For example, an intelligence service may access Government held immigration related datasets to conduct checks to ensure those entering the UK do not pose a risk to national security. Many

[5] Independent review of the IPA 2016 (publishing.service.gov.uk)

commercial companies acquire various datasets as part of their own business objectives and offer access to these to a variety of customers. Access to such datasets may offer the intelligence services different capabilities and insights to support them in carrying out their statutory functions. It may be more proportionate or practical for the intelligence service to examine a dataset held by a third party rather than acquire and retain the data themselves.

26. 3PDs are held by a third parties and contain personal data relating to a number of individuals, where the nature of the set is such that the majority of the individuals are not of intelligence interest, and are unlikely to become so.

27. The Bill seeks to provide a statutory regime for intelligence service examination *in situ* of datasets held by third parties, which would constitute a BPD if retained by an intelligence service. It also includes statutory oversight by the Investigatory Powers Commissioner.

28. The proposed measures would also introduce 3PD warrants, which will be subject to a "double lock", whereby the warrant would need to be approved by both the Secretary of State and an independent Judicial Commissioner. This would build on the statutory regime that already exists in the IPA 2016 to underpin other powers.

29. Lord Anderson's review of the IPA 2016 noted that the Investigatory Powers Commissioners Office (IPCO) conducted an 'extensive review' of third party datasets in 2019 and concluded that the intelligence service's current access was compliant with Part 7, as reported in IPCO's 2019 Annual Report[6]. However, IPCO's report recommended that the Government consider bringing third party datasets within IPCO's oversight. The proposed new regime draws on the already well-established Part 7 IPA 2016 regime and incorporates statutory safeguards, including making provision for independent judicial oversight by the Investigatory Powers Commissioner.

## Improvements to the Notices Regime

30. For many years, the UK government has had the power to place requirements on telecommunications operators to assist with national security and law enforcement; for example, the power in section 94 of the Telecommunications Act 1984. A Telecommunications Operator is defined in Section 261(10) of the IPA 2016 as:

> *"Telecommunications operator" means a person who—*
>
> *(a) offers or provides a telecommunications service to persons in the United Kingdom, or*
>
> *(b) controls or provides a telecommunication system which is (wholly or partly)—*
>
> *(i) in the United Kingdom, or*
>
> *(ii) controlled from the United Kingdom.*

31. The IPA 2016 currently provides for three different types of notice that can be issued to telecommunication operators (and in some cases postal operators):

    - Data Retention Notices (DRNs) require the retention of specified types of communication data (communications data is the 'who', 'when', 'where' and 'how' – often known as metadata) by telecommunications operators.

[6] Annual Report 2019 – IPCO

- Technical Capability Notices (TCNs) require telecommunications operators to provide and maintain technical capabilities enabling them to respond to relevant IPA 2016 authorisations or warrants allowing access to communications data, the content of a communication (the 'what'), or to enable equipment interference. A notice does not itself authorise the activity that the technical capability is intended to enable.
- National Security Notices (NSNs) require the telecommunications operator to take such specified steps as the Secretary of State considers necessary in the interests of national security. This may include providing services or facilities for the purpose of facilitating or assisting an intelligence service to carry out its functions or dealing with an emergency (within the meaning of Part 1 of the Civil Contingencies Act 2004).

32. All three types of notices must be 'double-locked' (approved by both the Secretary of State and an independent Judicial Commissioner) before they can be given to the operator in question. Section 88(1) and 255(3) of the IPA 2016 also lays out the factors the Secretary of State must consider when deciding whether to give a notice. These matters include:

    - The likely benefits of the notice,
    - The likely number of users (if known) of any postal or telecommunications service to which the notice relates,
    - The technical feasibility of complying with the notice,
    - The likely cost of complying with the notice, and
    - Any other effect of the notice on the person (or description of person) to whom it relates.

33. A notice itself does not allow access to data. Even when there is a notice in place with a Telecommunications Operator (TO), the public authorities and intelligence communities must also have the relevant warrant or authorisation in place before they are able to access data. The decision to issue a warrant or grant an authorisation will, itself, be subject to appropriate safeguards to ensure that it is necessary and proportionate.

34. When it was introduced, one of the main aims of the IPA 2016 was to ensure the powers were fit for the digital age. In the period since 2016, the global volumes of data that exist have grown exponentially, and significant, fast-paced technological change has become the norm. The efficacy of the powers has shifted with these changes, resulting in a negative effect on the capabilities of the UK's law enforcement and intelligence agencies.

35. Between 5 June and 31 July 2023, the Government ran a public consultation on the revised notices regimes in the IPA.[7] The consultation set out the Government's proposed objectives to improve the effectiveness of the current notices regimes in response to technological changes and the risk they pose to investigatory powers, as well the increase in data being held overseas. The consultation sought input to inform potential policy and legislative proposals intended to mitigate those risks whilst still promoting technological innovation and the privacy of citizens.

36. The Government consultation response was published on the same day as the Investigatory Powers (Amendment) Bill. This set out the amendments to Part 4 and Part 9 of the IPA 2016 that are proposed in this Bill to maintain the efficacy of these long-standing powers. These measures include: strengthening the notice review process by maintaining the status quo during the notice review period; clarifying the scope and definition of a telecommunications operator; introducing a notification requirement that requires relevant telecommunications operators (who will be directly informed that they are bound by the obligation by the Secretary of State) to inform the

[7] Consultation on revised notices regimes in the Investigatory Powers Act 2016 (accessible version) - GOV.UK (www.gov.uk)

Secretary of State if they propose to make changes to their products or services that would negatively impact existing lawful access capabilities; and introduce a notice renewal process with a statutory role for the IPC in order to increase oversight; and allowing the Secretary of State to set a timeline for the overall review period of a Notice.

37. Additionally, under section 255(9) - (11) of the IPA 2016, any TCN is enforceable by civil proceedings against a person in the UK. Only TCNs that provide for interception and targeted communications data acquisition capabilities are enforceable against a person overseas. Section 95 of the IPA 2016 also provides that a Data Retention Notice (DRN) is enforceable by civil proceedings against a person in the UK, but there is no express provision permitting the enforcement of a DRN against a person outside the UK. The Bill therefore seeks to amend Section 95 and 97 to allow extraterritorial enforcement of DRNs to strengthen policy options when addressing emerging technology, bringing them in line with TCNs. The intention of this would be to ensure that notices given to international telecommunication operators can be enforced should they need to be for UK security purposes in the light of the increasing volume of data of interest held by international companies. The Bill also seeks to clarify that the non-disclosure obligation imposed on persons to whom a Technical Capability Notice (TCN) or National Security Notice (NSN) is given, at section 255(8), is also enforceable by civil proceedings, bringing it in line with the enforcement provision at section 95(2) and (5).

38. Section 87(4) of the IPA 2016 provides that a DRN cannot require the retention of so-called 'third party data'. There is no intention to revisit the point of principle; however, the Bill contains measures seeking to amend section 87(4) in order to address some discrete and unintended consequences which have unduly broadened the effect of that subsection and restricted the type of data that can be subject to a DRN.

39. The Government's consultation response also set out where the Government decided not to proceed with certain proposals – including compelling telecommunications operators to engage in the consultation process for a notice or strengthening enforcement mechanisms – on the grounds that it is in both the Secretary of State and the operator's best interest to have a workable notice which is necessary and proportionate and that the IPA 2016 already has strong enforcement options, therefore it's not necessary to amend enforcement at this time.

## Internet Connection Records (ICRs)

40. An Internet Connection Record (ICR) is a record, held by a Telecommunications Operator, about the service to which a device has connected on the internet, for example that someone has accessed 'illegalsite.com.' The Government's policy position is that better use of these ICRs could revolutionise the ability of investigators to discover and prosecute serious criminals.

41. The way in which the IPA 2016 is currently drafted requires certain thresholds to be met on the 'known' elements of the investigation, such as when a website has been accessed. This limits the ability of the intelligence services and NCA to use ICRs to detect previously 'unknown' criminals online. The proposed changes would help the intelligence services and NCA to detect and locate individuals involved in serious criminal activities, such as in the grooming of children online, those engaged in widespread internet enabled fraud or those who seek to undermine the security of the UK.

42. The Bill seeks to achieve this by adding a new condition to the list of existing conditions for the use of ICRs at s62 of the IPA 2016. The intention of this is to enable target detection, which is currently not possible using ICRs without disproportionately increasing the level of intrusion. This new condition would only be available to the intelligence services and the NCA for a more limited set of lawful purposes relating solely to national security, the economic wellbeing of the UK (so far as those interests are also relevant to the interests of national security), and serious

crime.

43. The policy objective of this measure is to improve the intelligence services' and the NCA's ability to detect previously unknown individuals who are using the internet to commit high-harm crimes. This would only be a small change as the intelligence services and the NCA are already permitted to use ICRs for subject identification but are currently required to know the time of access and service in use to do so, limiting utility of the capability to assist in detecting new subjects of interest.

44. The measure aims to allow target detection of high-impact offenders by removing the requirement to unequivocally know a specific time or times of access, and service in use and instead allows these parameters to be set out in the application, based upon detailed analysis and subject matter expertise.

45. ICRs could be used to identify high-risk child sexual abuse (CSA) offenders, including those who both access multiple CSA platforms and have access to children. Intelligence derived from ICR applications could enable law enforcement partners to prioritise their efforts against CSA, protecting children and bringing offenders to justice.

46. High-harm fraud often involves online behaviour that could be identified by ICRs. ICRs could be used, for example, to search for devices which were simultaneously connecting to legitimate banking applications and to malicious control points. Such behaviour could indicate that a financial fraud is in progress. Improved access to ICRs could enable the intelligence services to detect such activity more effectively and to inform law enforcement colleagues of the identity of the potential fraudsters and of any associated organised crime groups. The intention is that flagging suspicious behaviour in that way can lead to action being taken to prevent criminals from defrauding their intended victims.

47. The policy intent in the proposals is that the period of time to be specified, and the service(s) to be queried must still meet necessity, proportionality and collateral intrusion tests and service(s) could not be queried, or for any longer, than was absolutely necessary to meet the operational objective of the ICR application. The applicant would have to explain their reasoning with reference to tangible supporting information which would be subject to the existing oversight and safeguards of the regime.

## Warrantry

48. The IPA 2016 provides for a warrantry process – the process through which activity under the Act is authorised. The authorisation process is multi layered, involves independent oversight by the judiciary and is based on the principles of necessity and proportionality. Depending on the powers being authorised for use by which authority, different authorisation processes are followed.

49. For example, all warrant applications for interception require approval from the Secretary of State and a Judicial Commissioner whereas the use of equipment interference powers by police forces must be authorised by a Chief Constable and a Judicial Commissioner.

50. Exceptionally, warrants for the use of interception or equipment interference, where the purpose is to obtain the communications of a member of a relevant legislature, must additionally be approved by the Prime Minister. This is known as "the triple lock".

51. Following the Home Secretary's statutory review of the IPA 2016 and Lord Anderson's independent review, several areas were identified where processes around warrantry could be made more resilient and effective. This part of the IPA 2016 regime balances the requirement for strong statutory oversight with the operational requirements of the operational community and the Government has identified potential ways to improve the regime while maintaining this

balance.

52. Firstly, given the restrictive nature of the current approvals process for warrants the purpose of which is to intercept or examine the communications of members of a relevant legislature under Sections 26 and 111 IPA 2016, critical intelligence gathering opportunities may be missed as a result of Prime Ministerial unavailability. The Bill proposes amendments to the IPA 2016 with the intention of ensuring that lack of availability of those individuals or office holders required by the IPA 2016 to authorise certain warrants or activities does not come at the cost of critical operations. It would do this by providing that alternative approvers of sufficient rank or office are able to approve warrant applications in urgent circumstances. In the case of Section 26 or 111 warrants, the Bill would make provision for the Prime Minister to nominate a cadre of five Secretaries of State who will be empowered to exercise the Prime Minister's power to provide the final authorisation of the "triple lock". The procedure for the use of an alternative approver would only become available where the requirement for the authorisation is urgent and the Prime Minister is unable by virtue of medical incapacitation or a lack of access to secure communications; .

53. Secondly, the Bill proposes provision to add a Deputy Director General of the National Crime Agency to the list of law enforcement chiefs who are able to delegate the function of considering Targeted Equipment Interference (TEI) applications under s.106 IPA 2016, to appropriate delegates (as described in the table in Part 1 of Schedule 6 IPA 2016) in urgent cases. Equipment interference (EI) allows the security and intelligence agencies, law enforcement and the armed forces to interfere with equipment to obtain electronic data. This includes computers, tablets, smartphones, cables, wires and static storage devices. EI can be carried out either remotely or by physically interacting with equipment. The policy objective of this proposed change is to improve the resilience of the process and ensure that the lawful authorisation of warrants critical to investigations is not reliant on a potential single point of failure in the authorisation process, while remaining at a suitably senior level.

54. Thirdly, under the IPA 2016 as it was enacted, the processes associated with the removal of a subject from a TEI warrant did not provide a power for the Secretary of State to make any decisions about the authorisation at the point of removal stage in the process, but do require the Secretary of State to be notified of the removal. The removal of a subject will not result in further interference with privacy rights, so it could be considered unnecessary to notify the Secretary of State at this stage. The Bill includes an amendment to the processes associated with the removal of a subject from a TEI warrant which would have the effect of removing the requirement to notify the Secretary of State at the point of the removal of the subject.

55. Fourthly, amendments to the table in Part 1 of Schedule 6 of the IPA 2016 are proposed with the intention of rectifying a drafting error in the column providing for the delegation, in urgent circumstances, of the authorisation of an equipment interference warrant from a Chief Constable to a Deputy Chief Constable or an Assistant Chief Constable. At present, the IPA 2016 refers to a repealed provision within an extant piece of legislation to allow for this delegation. The relevant power of delegation is now set out in different legislation, so Schedule 6 of the IPA 2016 would be updated to reflect this.

56. Finally, the way in which the IPA 2016 is currently drafted means that a Targeted Examination Equipment Interference (TXEI) warrant under Part 5 of the IPA 2016 cannot be issued for the purpose of national security where it relates to equipment located in Scotland. The issue has been remedied through a partial commencement. Regulation 9 of The Investigatory Powers Act 2016 (Commencement No. 5 and Transitional and Saving Provisions) Regulations 2018 came into force on 27th June 2018. The Government is seeking to tidy up the IPA 2016 and correct the error in legislation by amending section 102(4) IPA 2016 so that the Secretary of State would no longer need to rely on the partial Commencement of a provision.

# Investigatory Powers Commissioner (IPC) Functions

57. The IPA 2016 contains oversight arrangements that have strengthened the safeguards that apply to the use of investigatory powers. The IPA 2016 created the IPC and their office. The IPC independently oversees the use of investigatory powers, ensuring that they are used in accordance with the law and in the public interest. The Commissioner is supported in their duties by 17 other JCs and the IPCO, who oversee the use of covert investigatory powers by more than 600 public authorities including the intelligence agencies, law enforcement, and local authorities.

58. The proposed reforms to the IPA 2016 in this Bill aim to provide additional safeguards in areas not currently covered by the IPA 2016. As highlighted in the Home Secretary's review, the IPA 2016 does not provide an easy mechanism to manage change, causing issues with resilience and flexibility in respect of the IPC and wider IPA 2016 oversight regime. These proposed measures also aim to formalise the IPC's oversight functions and provide greater legislative clarity in respect of the oversight regime.

59. All of the proposed amendments regarding the IPC's oversight functions, where these fell within Lord Anderson's terms of reference, were supported by the conclusions of the Review. IPCO has also supported all the measures that are being taken forward.

## IPC's oversight functions

60. The incumbent IPC, Sir Brian Leveson, has expressed the value of the role's non-statutory functions being placed on a formal statutory footing. In line with this, the Government has included a proposed measure in the Bill to increase transparency in IPC's oversight, by amending s.229 of the IPA 2016 to place the IPC's oversight of compliance by the Ministry of Defence (MoD) onto a statutory footing. The IPC currently provides oversight of the MoD's overseas covert human intelligence sources (CHIS) and surveillance operations on a non-statutory basis. This oversight is carried out at the request of the Ministry of Defence (MoD), and a similar form of oversight has been provided in the form of annual inspections by IPCO's predecessors since at least 2005. The measure would not give the MoD or the IPC any new powers; however, it does seek to formalise this agreement to increase oversight.

## Flexibility and resilience

61. The Bill contains proposals to amend the role of the IPC and wider oversight regime with the intent of providing increased flexibility and resilience, and to formalise the IPC's functions.

62. Under the current legislation, there are currently two mechanisms by which the IPC's functions can be amended. This is either by: regulations made by the Secretary of State under s.239 of the IPA 2016 to amend s.229 of the IPA 2016; or by a direction issued by the Prime Minister under s.230. Such directions under s.230 are currently limited to the activities of the intelligence agencies and the MoD, so far as engaging in intelligence activities. The Government's policy intent is to achieve greater consistency in how the Government can direct the IPC to oversee the activities of public authorities whose activities fall within the remit of the IPA 2016, by extending the power of the Prime Minister to issue such directions to other public authorities that use the IPA 2016, so far as engaging in intelligence activities. The aim of this would be to ensure clearer parameters regarding the IPC's oversight and that law enforcement agencies such as the NCA would be included in the scope of s.230, with the flexibility that would allow a rapid response to emerging oversight requirements.

63. The way the IPA 2016 is drafted also means there is currently no provision for the IPC to formally appoint a Deputy IPC (DIPC) to exercise functions that are personally conferred on the IPC (such as, the ability to review a decision of a JC not to approve a warrant or the decision of a Secretary of State to give a notice). Lord Anderson's report highlights that this could hamper IPCO's resilience and agility, particularly in circumstances where the IPC may be unavailable to carry out their role.

The amendment proposed in the Bill would be to appoint up to two Deputy IPCs, given that the IPC is contracted to work for 3 days per week and JCs are contracted to work for 90 days per year to provide further resilience. The policy intent is that the IPC would be able to formally appoint up to two DIPCs because of the risk that a single Deputy would be unavailable. The specific appointment and removal from office of Deputy IPCs would be the responsibility of the IPC.

64. The Bill contains a measure seeking to delegate all the IPC's appellate functions to the newly created Deputy IPCs when the IPC is unable or unavailable to determine them for any reason. This proposal is relevant in the context of authorisations under the IPA 2016 and Schedule 3 of the Counter Terrorism Boarder Security Act 2019, regarding appeals to the IPC against a JC's decision. This measure seeks to give Deputy IPC's the power to determine such appeals when the IPC is unable or unavailable to determine them.

65. Under the current legislation, the IPA 2016 was amended by the Data Retention and Acquisition Regulations 2018 to add a new provision to give the IPC power to authorise the acquisition of Communications Data (CD) (Section 227(9A) of the IPA 2016). The IPC's power to delegate functions to a JC under s.227(8) of the IPA 2016 does not extend to the IPC's functions relating to CD under ss.60A and 65(3B) IPA 2016 and extends only to where the IPC is unable to exercise these functions because of illness or absence or for any other reason. For example, this restriction caused issues during the Covid pandemic, where although office access was limited, the IPC was arguably not "unable" carry out his functions within the meaning of s.227(9A) IPA 2016. This Bill looks to amend the IPA 2016 to remove this limitation and allow the IPC's power in respect of CD authorisation to be generally exercised by JCs.

66. This Bill also seeks to remove the IPC's oversight functions relating to telecommunications restriction orders (TROs) for prisoners under s.229(3)(c) of the IPA 2016. TROs are already subject to judicial approval in the county court, which provides the necessary degree of assurance and oversight, and the Government has not identified any additional benefit in the IPC overseeing this process after the event.

67. There is currently no provision in the IPA 2016 for the IPC to formally appoint temporary JCs. The ability to appoint temporary JCs under the Coronavirus Act 2020 proved vital to the continued operation of the IPA 2016 and its oversight regime during the COVID-19 pandemic. As this emergency legislation is now suspended, the Home Office proposes to replicate the procedures, safeguards, and terms of appointment set out in ss. 22 and 23 of the Coronavirus Act 2020, but to remove the connection to coronavirus and widen its application to exceptional circumstances which result in a shortage of JCs. Specifically, the powers proposed would specify that: the IPC may appoint temporary JCs to carry out the functions conferred on JCs by any enactment; a temporary JC would be appointed for one or more terms not exceeding six months each and not exceeding three years in total; and the Secretary of State and the IPC must also agree that an exceptional circumstance which results in a shortage of JCs exists before these powers are exercised.

## Greater clarity to oversight functions

68. The Bill proposes measures to clarify the scope of error reporting notifications that are to be made to the IPC to include errors of a description identified in codes of practice issued under the Regulation of Investigatory Powers Act 2000 (RIPA 2000), Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A 2000) and the Police Act 1997 (in addition to the IPA 2016). In practice, these relevant errors are already reported to IPCO by public authorities. However, this proposal would make this reporting of a relevant error a statutory requirement, with the policy aim of closing the gap regarding these reporting obligations by ensuring that there is oversight in respect of errors as described in codes of practice issued under RIPA 2000 and other relevant legislation, which currently do not fall within the IPA 2016's error regime (s.231(9)) and clarify

that such errors fall within the IPC's remit.

# Freedom of Information Act 2000

69. The Freedom of Information Act 2000 (FOIA) provides a general right of access to recorded information held by 'public authorities', as defined by section 3 with reference to bodies listed in Schedule 1, or companies as defined within section 6.

70. IPCO is not listed as a Schedule 1 'public authority' for the purposes of FOIA and therefore the information it holds is not accessible under that legislation. However, the current legislative position means that information shared by IPCO, or which relates to its activities, and which is held by a public authority as defined in FOIA is accessible. While a public authority, in consultation with IPCO, may seek to apply one of the exemptions in FOIA, the final decision on disclosure (including where applicable the balance of the public interest) rests with the public authority.

71. This Bill seeks to add JCs (a term that includes the IPC) to the list of bodies dealing with security matters at section 23 of FOIA. Section 23 is an absolute exemption, thereby protecting information held by other public authorities which relates to the activities of JCs.

# Communications Data (CD)

## Section 11

72. Section 11 of the IPA 2016 created an offence for a relevant person within a relevant public authority of "knowingly or recklessly" obtaining CD from a TO or a Postal Operator (PO) without lawful authority. A relevant public authority is an authority listed in Schedule 4 of IPA 2016. At present, there is no definition as to what constitutes "lawful authority" under section 11 whereas section 6 does provide a definition of "lawful authority" in respect of interception.

73. When the legislative provision was created it was to ensure there were adequate safeguards and oversight to protect privacy, especially personal data that is not publicly or commercially available and was to be obtained from private sector TOs. The offence set out under section 11 combined with the complexity of the CD definition poses significant challenges to public authorities. This Bill therefore sets out examples of authorities that will amount to "lawful authority" for the purposes of section 11 with the aim of providing greater reassurance to public authorities when acquiring CD from TOs.

74. It was also not the policy or legislative intent to prevent data sharing between public sector organisations required to meet their statutory duties and obligations when administering public services or systems, for example authenticating a citizen's benefits application against government tax systems and preventing and detecting fraud.

75. Government departments are likely to fall within the definition of a TO in the IPA 2016 because of the services they offer via digital platforms for citizens to manage their access to public services, for example submitting tax returns, and applying for benefits, passports, or driving licenses. The proposals in this Bill aim to remove the risk of them committing a section 11 offence by receiving CD from another public sector organisation in the exercise of their functions. When referring to public sector organisations the Government is relying upon the definition as set out in the Procurement Act 2023. Not all such organisations will be TOs.

76. The sharing of CD between public authorities would still be required to comply with data protection legislation and would continue to be subject to sufficient oversight. There is an agreement between the IPC and the Information Commissioner about where their responsibilities may overlap.

## Section 12

77. As businesses move more of their service offerings online, some of the data that they capture is now falling within the definition of CD.

78. Section 12 and Schedule 2 IPA 2016 removed general information gathering powers from public authorities, ensuring that those authorities could only secure the disclosure of CD from a TO, without that TO's consent, via certain routes. These routes included obtaining a Part 3 IPA 2016 authorisation, a court order or other judicial authorisation, under certain "regulatory powers" relating to the regulation of TOs or POs or "postal powers", or as secondary data from interception and EI warrants.

79. As a result, there are concerns that several bodies with regulatory or supervisory functions, such as those with responsibility for supervising the financial sector and ensuring compliance with Money Laundering and Terrorist Financing Regulations, may be unable to perform their statutory functions as effectively as they need to.

80. For those regulatory or supervisory bodies with IPA 2016 powers, this issue remains extant where there is an inability to meet the serious crime threshold in the IPA 2016 for the acquisition of certain types of CD in their enquiries. For example, they may be able to acquire CD where there is a serious crime involved with the possibility of a prison sentence of one year or more, but not if the matter can only lead to the imposition of a civil penalty or large fine.

81. For regulatory or supervisory bodies without IPA 2016 powers this issue remains due to the position held by the sectors they regulate or supervise in that some of the data for which disclosure is required for those bodies to carry out their statutory functions effectively now falls within the definition of CD and requires an IPA 2016 authorisation to acquire it. The changes to legislation proposed in this Bill aim to make it easier for these organisations to carry out their lawful functions.

82. Section 12 recognises the need for bodies with "regulatory functions" to acquire CD. This is currently limited to organisations such as the Office of Communications (Ofcom) and the Information Commissioners Office for their regulation of TOs. This measure would amend the IPA 2016 to expand the definition of 'Regulatory Powers' to include those with wider, lawfully established and recognised regulatory or supervisory responsibilities, with the intention of returning their general information gathering powers and enabling them to gather the information they need to perform their lawful functions and where the CD is not being acquired in the course of a criminal investigation.

83. Where the purpose of the investigation is in the course of a criminal investigation, the Part 3 IPA 2016 authorisation process should still be followed by those organisations authorised under Schedule 4.

84. The acquisition of CD using non-IPA 2016 powers by these public authorities for the purposes of regulation or supervision, but which then is subsequently used for criminal prosecution, will be subject to oversight by the IPC.

## Section 261

85. The IPA 2016 provides the definition of CD for the purposes of acquiring such data under Part 3 and retention under Part 4. That definition of CD is made up of "Entity data" (for example, phone numbers or other identifiers linked to customer accounts) and "Events data" (for example, the fact that someone has sent or received an email, phone call, text or social media message and the location of a person when they have made a mobile call or used a Wi-Fi hotspot), with a carve-out to exclude the "Content" of a communication.

86. At present, there is insufficient clarity over whether subscriber and account data is CD or content,

for example in the context of registration details provided in online forms when an individual is setting up an account or taking up a service over the internet.

87. Due to the complex nature of whether subscriber and account data amount to CD or content, this Bill proposes amending s261 IPA 2016 with the intention of removing any potential ambiguity. This change aims to provide a clear basis for the acquisition of subscriber and account data as CD and also aims to make it clearer when an error has occurred.

88. The amendments to section 261 covering "subscriber data" and "content" would not affect the oversight function of IPCO which continues to inspect and highlight any errors.

## Interception

89. Section 56 of the IPA 2016 makes it clear that any intercepted communication and any secondary data obtained from a communication is excluded from being used in or for legal proceedings. There are exceptions to this set out in Schedule 3 to the IPA 2016.

90. Although an exception applies in respect of parole proceedings in Northern Ireland (paragraph 13 of Schedule 3), Parole Board proceedings in England and Wales do not currently benefit from an exemption. This means that panel members of the Parole Board for England and Wales are unable to review key interception materials as evidence to make parole considerations. It is Government policy that panel members of a Parole Board need to be able to review intercepted materials to make more informed assessments as to the risk of harm to the public from terrorists and other dangerous prisoners by considering all classified materials. The Bill therefore seeks to amend the IPA 2016, allowing intercepted communications and relevant secondary data to be considered in proceedings before the Parole Board and proceedings that arise out of those hearings.

91. Another exception is being introduced as an amendment to Schedule 3 to the IPA 2016 to give relevant Northern Ireland coroners and Scottish sheriffs conducting investigations into deaths the power to review intercepted materials in line with their counterparts in England and Wales. This would enable relevant coroners in Northern Ireland and sheriffs in Scotland the opportunity to review all relevant evidence in inquiries and inquests related to deaths in Northern Ireland and Scotland.

## Bulk Equipment Interference

92. Bulk equipment interference (IPA 2016 Chapter 3) includes methods involving interference with multiple computers and devices. This could include implanting software into devices for the purpose of data retrieval to locate potential targets of interest. Only the intelligence agencies have the power, under IPA 2016, to undertake equipment interference in bulk and it is reserved for activity with a foreign focus.

93. Section 195 of Chapter 3 currently provides additional safeguards for journalistic material, requiring that the Investigatory Powers Commissioner be informed if material thought to contain confidential journalistic material or sources of journalistic material is retained, following examination, for a purpose other than its own destruction.

94. This Bill introduces prior independent authorisation to Section 195, the intended effect of which will be to add an additional layer of scrutiny over the intelligence's agencies' handling of material which may contain confidential journalistic material or sources of journalistic material. It is also intended to bring journalistic safeguards into alignment with the bulk interception regime which is being amended via the Investigatory Powers Act 2016 (Remedial) Order 2023 which was laid before Parliament on 18th October 2023.

# Legal background

## Bulk Personal Datasets (BPDs)

95. The current Part 7 regime requires the intelligence services to apply the same standard of safeguards to the retention and examination of all bulk personal datasets regardless of the level of intrusion associated with their retention and examination. Whilst some BPDs may contain sensitive personal information in respect of which stringent safeguards are necessary, the current Part 7 safeguards go beyond what the ECHR requires[8] for certain datasets that have low or no reasonable expectation of privacy.

96. The ECHR will want to ensure that the statutory regime provides for adequate and effective safeguards against abuse. The Court's assessment will take account of all the circumstances. In the context of pre-IPA 2016 bulk interception, the Grand Chamber dealt with this point in Big Brother Watch v UK[9] at §361:

> "361. In assessing whether the respondent State acted within its margin of appreciation (see paragraph 347 above), the Court would need to take account of a wider range of criteria than the six Weber safeguards. More specifically, in addressing jointly "in accordance with the law" and "necessity" as is the established approach in this area ([…]), the Court will examine whether the domestic legal framework clearly defined:
>
> 1. the grounds on which bulk interception may be authorised;
>
> 2. the circumstances in which an individual's communications may be intercepted;
>
> 3. the procedure to be followed for granting authorisation;
>
> 4. the procedures to be followed for selecting, examining and using intercept material;
>
> 5. the precautions to be taken when communicating the material to other parties;
>
> 6. the limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed;
>
> 7. the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to

[8] Under the Human Rights Act 1998, respect for private and family life is a qualified right. This means interference by a public authority with the exercise of this right is acceptable provided it is done in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[9] (2022) 74 EHRR 17; see also: https://hudoc.echr.coe.int/eng?i=001-210077

address non-compliance;

8. the procedures for independent ex post facto review of such compliance and the powers vested in the competent body in addressing instances of non-compliance."

97. We think it is also instructive to have regard to the pre-IPA 2016 decision of the Investigatory Powers Tribunal in Privacy International v Secretary of State for Foreign and Commonwealth Affairs.10 This case specifically concerned the acquisition and retention of bulk communications data and bulk personal datasets under the Telecommunications Act 1984 (to note: not datasets that could be said to be low/no datasets). As to safeguards and foreseeability, at §62 the Tribunal set out the following:

"62. Accordingly, by reference to our considered assessment of the ECHR jurisprudence, we can summarise in short terms what we conclude the proper approach is:

(i) There must not be an unfettered discretion for executive action. There must be controls on the arbitrariness of that action. We must be satisfied that there exist adequate and effective guarantees against abuse.

(ii) The nature of the rules fettering such discretion and laying down safeguards must be clear and the ambit of them must be in the public domain so far as possible; there must be an adequate indication or signposting, so that the existence of interference with privacy may in general terms be foreseeable.

(iii) Foreseeability is only expected to a degree that is reasonable in the circumstances, being in particular the circumstances of national security, and the foreseeability requirement cannot mean that an individual should be enabled to foresee when the authorities are likely to resort to secret measures, so that he can adapt his conduct accordingly.

(iv) It is not necessary for the detailed procedures and conditions which are to be observed to be incorporated in rules of substantive law.

(v) It is permissible for the Tribunal to consider rules, requirements or arrangements which are 'below the waterline' i.e. which are not publicly accessible, provided that what is disclosed sufficiently indicates the scope of the discretion and the manner of its exercise.

(vi) The degree and effectiveness of the supervision or oversight of the executive by independent Commissioners is of great importance, and can, for example in such a case as Kennedy, be a decisive factor."

10 [2017] 3 All ER 647; see also: https://investigatorypowerstribunal.org.uk/judgement/privacy-international-and-1-secretary-of-state-for-foreign-and-commonwealth-affairs-2-secretary-of-state-for-the-home-department-3-government-communications-headquarters-4-security-service-5/

98. The changes proposed in the Bill have the intention of introducing a new regime, alongside the current Part 7, which would be concerned with datasets in respect of which there is a low or no reasonable expectation of privacy. This test is one that is to be applied in all of the circumstances.11 The new regime proposed in the Bill would set out certain factors, germane to the context, to which intelligence services must have particular regard when assessing the expectation of privacy. Authorisations for the retention, or retention and examination of such a dataset may be granted by the head of an intelligence service, or a person acting on their behalf. The new provisions proposed in the Bill would establish a system of prior judicial approval to provide reassurance that assessments being made are appropriate. As with the other powers in the IPA 2016, there will also be ex-post facto oversight by the IPC, and the redress mechanism of the Investigatory Powers Tribunal.

99. Proposed provisions in the Bill would also make minor changes to Part 7, extending the duration of BPD warrants from six months to twelve months. The proposed changes would also provide that certain functions that hitherto had to be performed by the head of the intelligence service could now formally be carried out on his or her behalf by a Crown Servant, in common with other functions in the IPA 2016 (such as applying for a warrant).

## Third Party Bulk Personal Datasets (3PD)

100. The intelligence services can currently access 3PDs in the exercise of their functions through relevant information gateways such as the Intelligence Services Act 1994 and the Security Services Act 1989. This regime places intelligence service access to 3PDs onto a statutory footing. See above policy background for further detail.

## Changes to the Notices Regime

101. Notices are issued to TOs that hold data of operational relevance in order to provide and maintain investigatory powers capabilities, this ensures the intelligence services and law enforcement have access to data required for their investigations.

102. Proposed provisions in the Bill would amend the definition of a TO out of an abundance of caution to ensure that obligations imposed by the IPA 2016 apply to all entities of the company, irrespective of where the entity providing the "telecommunications service" is based or the entity controlling the "telecommunications system" is based. Proposed provisions also aim to clarify that a notice may be given to one entity in relation to another entity's capability.

103. When giving a notice for the first time, the Secretary of State has a statutory obligation to engage in a consultation period with the relevant operator. Following this consultation, and taking into consideration the views of the operator, the Secretary of State then considers whether to formally give the notice. Should they decide to do so, the notice must then be approved by a JC and formally given to the company before its obligations become binding on them. If at this point the operator is dissatisfied with the terms of the notice, they have a statutory right to refer the notice (or part of it) to the Secretary of State for review as set out in sections 90 and 257 of the IPA 2016.

104. The Secretary of State must then consult the Technical Advisory Board (TAB) and a JC. The TAB's membership includes representatives from the telecommunications industry, government/public authorities, and independent members including an independent chair. As it stands, during a review period the operator is not required to comply with the notice, so far as referred, until the Secretary of State has determined the review. Where an operator is seeking to make significant

---

[11] See *ZXC v Bloomberg LP* [2022] UKSC 5

changes to their services or systems that would have a detrimental effect on a current lawful access capability, this could create a capability gap during the review period.

105. After considering reports from the Technical Advisory Board (TAB) and the JC, the Secretary of State may decide to vary, revoke, or confirm the effect of the notice. Where the Secretary of State decides to confirm or vary the notice, the IPC must approve the decision. Clause 8 amends s.227(8) to allow the IPC to delegate this function to the newly created Deputy IPCs, in the event that the IPC is unable or unavailable to exercise this function.

106. The proposals in this Bill aim to ensure that the TO maintains the status quo, by not making any changes that may have a negative impact on lawful access capabilities, until the review by the Secretary of State has concluded (Clause 18).

107. Sections 90(1) and 257(1) include regulation making powers in relation to a review of a notice. The Investigatory Powers (Review of Notices and Technical Advisory Board) Regulations 2018 (SI/2018/354), made pursuant to s.90(1) and s.257(1), set out the period and circumstances within which notices maybe referred back to the Secretary of State for a review. However, the existing power does not give the Secretary of State the power to specify in regulations a time limit regarding the overall review process. Clause 18 introduces a new regulation making power that will enable the amendment of existing regulations (SI/2018/254) to specify both the length of time the Secretary of State can take to reach a decision on the review of a notice, upon receipt of the report by the JC and TAB, and the overall length of time a review of a notice can take. This will provide clarity to both operators and operational partners regarding how long a review of a notice can take and therefore how long the status quo must be maintained by the operator.

108. It is also necessary to make provision for a JC to issue directions to the Secretary of State and the person seeking the review, as they see fit, to ensure the effective management of the notice review process. Clause 18 will give a JC the power to give directions to both parties specifying the time period for providing their evidence or making their representations and give the JC the power to disregard any submissions provided outside these timelines. This will ensure the JC has the appropriate power to deal with non-compliance and provides clarity to all parties regarding timelines and expectations.

109. A TO, or any person employed or engaged for the purposes of the business of a TO, must not disclose the existence or contents of a notice to any other person without permission of the Secretary of State. This prohibition is enforceable by civil proceedings under Section 95(2) and (5) for DRNs, however there currently is no equivalent enforcement provision for TCNs or NSNs. Proposed provisions in the Bill would amend s.255(10) IPA 2016 with the intention of ensuring that the duty not to disclose the existence or contents of a TCN or an NSN is also enforceable by civil proceedings.

110. TOs who are already subject to a notice are required to inform the Secretary of State of any changes that may impact their existing notice obligations. This ensures that changes do not have a negative effect on investigatory powers. This Bill proposes to impose obligations on TOs who have not already been issued with a notice, to inform the Secretary of State of relevant changes, including technical changes that might affect lawful access, before such changes are implemented.

111. Under the current IPA 2016 provisions, the approval of a JC is required where the Secretary of State proposes to vary a notice and that variation would impose additional requirements on the TO (sections 94(4) and 256(4) and (5). The IPA 2016 also requires that the Secretary of State keeps relevant notices under regular review (sections 90(13) and 256(2), with the review process described in the relevant Codes of Practice. This Bill proposes to create a statutory role for the IPC within a formalised notice renewal process, if a period of two years has elapsed since a notice was first given, varied or renewed. This introduces an additional safeguard. With the introduction of the notice renewal process, a consequential amendment is required to the IPC's main oversight

functions. As such, an amendment has been made to insert a reference into s.229 to enable a JC to decide whether to approve the renewal of certain notices.

## Internet Connection Records (ICRs)

112. Internet Connection Records are data collected and retained by Telecommunications Operators (TOs) about the sites and services to which their customers connect on the internet. Certain Public Authorities are permitted to seek disclosure of that data within limited Access Conditions and upon independent authorisation by the Office for Communications Data Authorisations (OCDA) (or internal authorisation for National Security purposes by the intelligence services). The Public Authorities are laid out in Schedule 4 of the Act and include police forces, the NCA and the UK intelligence services.

113. The capability allows those specified Public Authorities to ask two primary questions of the data. Firstly, in instances where the subject of interest or device is known, the question of which internet sites or services have been connected to over a specified period (subject development) and secondly, for instances where a site or service is known, which customers have accessed that service at a specified time or times(subject identification).

114. The proposed changes concern this second 'subject identification' aspect of the legislation. The IPA 2016 as currently drafted covers this within Condition A.

> Condition A is that the person with power to grant the authorisation considers that it is necessary, for a purpose falling within section 60A(7), 61(7) or 61A(7) (as applicable), to obtain the data to identify which person or apparatus is using an internet service where—
>
> (a) the service and time of use are already known, but
>
> (b) the identity of the person or apparatus using the service is not known.

115. As drafted, Condition A is designed to assist in investigations where a specified internet site or service is known to have been accessed at a specified time or times and the public authority is seeking to determine the identity of the party or parties involved in that connection.

116. Examples of this may be where officers receive intelligence, perhaps from forensic examination of a seized device, about the use of a specified video conferencing facility, to livestream the abuse of a child or where a public figure has been subject to sustained online threats and abuse via a number of internet facilities such as an overseas hosted email facility, social media platform or constituency website. In such circumstances investigators would wish to identify subjects accessing those internet resources at relevant specified times coincidental to the abuse occurring and threats having been made.

117. There are concerns that this requirement to know the specific service and time of access limits utility of the ICR capability and prevent this TO- stored and managed data from being used to assist in some of the most serious investigations.

118. Whilst investigators may identify websites of interest in the course of their investigations, they may lack knowledge around whether a specified site has been accessed or a specific time or times of access. Where the site is itself criminal in nature then investigators are interested in access at any time.

119. The proposed addition to the legislation would allow investigators to state a service or services and a time period i.e., 'between this date/time and this date/time' within an application These stated service or services in a particular time period will be based upon subject matter expertise, analysis and existing intelligence and be indicative of behaviours that indicate serious criminality or a national security threat.

120. An example of this may be where the intelligence services identify a previously unknown site promoting terrorism, or child sexual abuse and exploitation, or the command and control infrastructure for malware, and wish to identify parties who are accessing those resources – where they may have a clear suspicion that they are being accessed but lack the requisite knowledge that they are and exactly when.

121. In circumstances where serious criminality may be denoted by a very specific pattern of connections this new provision aims to allow that pattern to be translated into the form of a question of ICR data to assist in identifying subjects of interest displaying those linked behaviours and in respect of whom it would not otherwise have been possible to detect.

122. An example of this would be in high-harm fraud which often involves online behaviour that could be identified by ICRs. ICRs could be used, for example, to search for devices which were simultaneously connecting to legitimate banking applications and to malicious control points. Such behaviour could indicate that a financial fraud is in progress. Improved access to ICRs could enable the intelligence services to detect such activity more effectively and to inform law enforcement partners the identity of the potential fraudsters and of any associated organised crime groups.

123. Whilst clearly having the potential to provide significant operational utility it is recognised that such queries are highly susceptible to imprecise construction. As a result, additional safeguards are proposed in this Bill with the intention of managing access to this new Condition and mitigating public concerns.

124. These safeguards include that the capability is to be limited solely to the intelligence service and the NCA who are assessed to possess the requisite subject matter expertise to formulate appropriate queries to derive the correct subset results. This has a significant reliance on understanding the construct of the ICR data queried, which may differ between TOs, understanding of human verses machine generated connections, and understanding of computer logic and the importance of accurate syntax.

125. The lawful purposes in respect of which this new Access Condition may be utilised are also limited, relating solely to National Security, the Economic Wellbeing of the UK so far as those interests are also relevant to the interests of national security, and for Serious Crime purposes.

126. Under the new condition proposed in this Bill, all applications would undergo review, where an appropriately trained authorising officer would consider the application. Applicants would have to address in detail within their application exactly how collateral intrusion would be managed to ensure only those persons who should be subject of investigation are so. Persons so identified would then be subject to individual development utilising established investigative capabilities to support the intelligence, all of which would need to be further and separately authorised.

127. The need for this change has been considered in depth, and supported, by Lord Anderson KC in his review of proposed IPA 2016 reforms.

# Warrantry

## Sections 26 and 111

**Section 26**

128. Where an intercepting authority makes an application to the Secretary of State for the issue of either a targeted interception warrant (where the purpose is to authorise or require the interception of communications sent by or intended for, a person who is a member of a relevant legislature) or a targeted examination warrant (where the purpose is to authorise the selection for examination of the content of such communications), the warrant must be approved by the Prime Minister.

**Section 111**

129. Where an application is made to the Secretary of State for a targeted equipment interference or examination warrant the purpose of which is to obtain or examine protected material consisting of communications sent by, or intended for, a person who is a member of a relevant legislature, or their private information, the warrant must be approved by the Prime Minister.

## Director General NCA

130. Section 106 provides the power for a "law enforcement chief" to issue TEI warrants. The power to issue a TEI warrant may be assigned to an "appropriate delegate" only if it is not practicable for the law enforcement chief to exercise it, and only in urgent cases.

131. Schedule 6 (table in Part 1) describes who is a law enforcement chief for the purposes of section 106 and, for the NCA, identifies the Director General (DG) only. The Bill proposes to add a Deputy Director General of the NCA to the list of law enforcement chiefs who are able to delegate the function of considering TEI applications under s.106 IPA 2016, to appropriate delegates (as described in the table in Part 1 of Schedule 6 IPA 2016) in urgent cases.

## Law Enforcement Equipment Interference delegation

132. Schedule 6 of the IPA 2016 refers to section 12A of the Police Act 1996 which was repealed in 2012 and replaced by s.41 of the Police Reform and Social Responsibility Act 2011 (Commencement No. 7 and Transitional Provisions and Commencement No. 3 and Transitional Provisions (Amendment)) Order 2012. The Bill proposes to correct a drafting error, by making reference to the 2011 Act, rather than the repealed section of the Police Act 1996.

## Targeted Equipment Interference, removal of a subject

133. Part 5 of the IPA 2016 is concerned with equipment interference warrantry. Warrants may be issued by, amongst others, the Secretary of State or by Scottish Ministers. Such a warrant may be modified in accordance with section 118; sections 119-122 set out how that modification process works. Section 119(1) provides that a senior official acting on behalf of the Secretary of State (or the Scottish Ministers, as the case may be) may modify a warrant.

134. Section 121 concerns the notification of modifications (this does not apply to urgent modifications, in respect of which a different regime applies). Subsection (1) provides that where a modification is made under section 118, a JC must be notified of it and of the reasons for making it, but this is subject to certain exceptions as set out in subsection (2). Subsection (3) applies where a modification is made by a senior official in accordance with section 119(1) and requires the Secretary of State (or a member of the Scottish Government, as the case may be) to be notified personally. The Bill proposes changing these provisions to remove the obligation on the Senior Official to notify the Secretary of State personally when a modification is made that removes a matter, name or description from a targeted equipment interference or targeted examination warrant.

## Targeted Examination warrants in Scotland

135. Under the IPA 2016, the Secretary of State may not issue an equipment interference warrant if the

only grounds that the warrant is necessary is for the prevention and detection of serious crime and the warrant would authorise interference with equipment that is in Scotland at time of issue. Warrants of this nature are issued by Scottish Ministers in accordance with section 103(1)(b) and 103(2)(b). Section 102(4) states that targeted examination warrants may not be issued by the Secretary of State if the warrant relates to a person who would be in Scotland at the time of issue. As section 103 only permits Scottish Ministers to issue warrants where the purpose is for prevention and detection of serious crime, this creates a gap.

136. A targeted examination warrant under section 102(3) that relates to equipment in Scotland, and which is necessary only for the purpose of the prevention and detection of serious crime, could be issued by the Scottish Ministers, but if the purpose was for national security, it could not legally be issued. The issue has been remedied through a partial commencement. Regulation 9 of The Investigatory Powers Act 2016 (Commencement No. 5 and Transitional and Saving Provisions) Regulations 2018 came into force on 27th June 2018. The Bill corrects this by amending section 102 with the effect that the Secretary of State may issue a targeted examination equipment interference warrant for National Security purposes where it relates to someone who was in Scotland at the time of the issue of the warrant.

## Investigatory Powers Commissioner Functions

137. The legal background related to Investigatory Powers Commissioner Functions is covered in the policy background.

## Amending the list of bodies dealing with security matters under s.23 FOIA

138. Section 23(1) of FOIA exempts, as a class, all information directly or indirectly supplied by, or relating to, certain bodies dealing with security matters. This provision confers an absolute exemption. Subsection (3) lists the relevant security bodies that have the benefit of the exemption. Section 23(5) of FOIA provides that the obligation to confirm or deny whether or not the authority holds the information does not arise, if compliance with that obligation would itself disclose information which is exempt by virtue of subsection (1).

139. Section 23 of FOIA (as relevant) states:

> "23. Information supplied by, or relating to, bodies dealing with security matters.
>
> (1) Information held by a public authority is exempt information if it was directly or indirectly supplied to the public authority by, or relates to, any of the bodies specified in subsection (3)
>
> (2) A certificate signed by a Minister of the Crown certifying that the information to which it applies was directly or indirectly supplied by, or relates to, any of the bodies specified in subsection (3) shall, subject to section 60, be conclusive evidence of that fact.
>
> (3) The bodies referred to in subsections (1) and (2) are—
>
> (a) Security Service …" …
>
> "(5) The duty to confirm or deny does not arise if, or to the extent that, compliance with section 1(1)(a) would involve the disclosure of any information (whether or not already recorded) which was directly or indirectly supplied to the public authority by, or relates to, any of the

bodies specified in subsection (3)."

140. Amendments to section 23 of FOIA have to be made by primary legislation, as there is no power to add to the list of security bodies by regulations, as is possible for amendments to Schedule 1, by virtue of section 4 FOIA. This Bill proposes to add JCs to the list of bodies dealing with security matters with the intention of ensuring that sensitive equities contained in information provided or relating to the functions of JCs are protected.

## Communications Data (CD)

141. Section 11 of the IPA 2016 created an offence of obtaining CD without lawful authority. There is no definition of "lawful authority" in respect of CD acquisition. The objective of amending section 11 is to make clear that certain types of authority or methods of acquiring CD will amount to "lawful authority". This would include applications to request CD in line with Part 3 IPA 2016, or through a judicial authorisation or Court Order, but it is likely to include other forms of authority. To resolve this, the intention is to provide a non-exhaustive list of circumstances of what will amount to lawful authority for the purposes of section 11.

142. The Bill provides examples of authorisations that will amount to "lawful authority" and includes an IPA 2016 authorisation, a Court order or other statutory power to require or provide CD, as well as CD relating to Public Emergency call services (codes of practice paragraph 6.1) and publicly available data with the intention of providing the legal certainty for those bodies who acquire CD and wish to avoid committing the section 11 offence.

143. The purpose of section 11 was also to discourage public authorities from abusing Part 3 powers to acquire CD from private companies. The explanatory note to section 11 says: 'The offence is intended to act as a deterrent and provide reassurance that abuse of powers to acquire communications data will be punished'.

144. The "powers" in question are the power to issue a notice to a TO to compel disclosure of CD. The obligation to comply with a notice does not bind the Crown so this power logically cannot have been aimed at public sector sharing of CD. Section 11 was not intended to catch public sector sharing of data and the Data Protection Act provides sufficient safeguards to protect the sharing of CD between public sector organisations where it is necessary and proportionate to do so. The offence will continue to apply to the acquisition of CD from private sector TOs. The IPC will continue to oversee the acquisition of CD by relevant public authorities from TOs in both the public and private sectors.

145. The purpose of section 12 IPA 2016 was to provide transparency around public authority access to CD, in effect ensuring that the Act was the only route available in relation to the 'statutory purposes' at section 61(7).

146. Section 12 and Schedule 2 IPA 2016 amended general information gathering powers, so far as they enabled public authorities to secure the disclosure, by a TO, of CD without the consent of the operator; where the disclosure did not involve a court order or other judicial authorisation or warrant, was not a regulatory power, and where it was not possible for the public authority to use a power under the IPA 2016 or the RIPA 2000.

147. Regulatory powers were in turn limited, in section 12(6), to those solely exercisable in connection with the regulation of telecommunications operators, services or systems and postal operators and services.

148. The statutory purposes at section 60A(7) state that it must be necessary to obtain the data—

> "(a)in the interests of national security,
>
> (b)for the applicable crime purpose,
>
> (c)in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security,
>
> (d)in the interests of public safety,
>
> (e)for the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health,
>
> (f)to assist investigations into alleged miscarriages of justice, or
>
> (g)where a person ("P") has died or is unable to identify themselves because of a physical or mental condition—
>
> (i)to assist in identifying P, or
>
> (ii)to obtain information about P's next of kin or other persons connected with P or about the reasons for P's death or condition."

149. The statutory purposes had originally included for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department and, secondly, for the purpose of exercising functions relating to the regulation of financial services and markets or financial stability. These lawful purposes were however subsequently excluded by the Data Retention and Acquisition Regulations 2018 enacted in response to the Court of Justice of the European Union's (CJEU) Tele2/Watson Judgment.[12]

150. These specific provisions were not routinely used because bodies with regulatory or supervisory functions, such as those who regulate the Financial Markets or ensure compliance with Money Laundering and Terrorist Financing Regulations, were previously able to acquire the data they needed in pursuance of their functions by using their own information gathering powers already available to them rather than the IPA 2016 provisioned powers.

151. However, as businesses are increasingly moving their service offerings online, more of the data those business collect about their customers now falls within the definition of Communications Data as it relates to the provision of a Telecommunications Service as defined in the IPA 2016. This data was data which regulatory and supervisory bodies would have previously been able to access using their own information gathering powers, but in respect of which those businesses are now seeking IPA 2016 Part 3 authorisations, from public authorities, before agreeing to disclosure.

152. The Section 12 provisions have had the effect of preventing those regulatory or supervisory organisations from gathering the data they require because their enquiries can fail to meet the serious crime threshold, which is the only other statutory purpose available to access some types of required data.

153. The purpose of the proposed Section 12 reforms in this Bill is to allow bodies with recognised regulatory and supervisory functions, and who utilise civil proceedings as a means of enforcement, to continue to perform the roles required of them by Parliament in permitting them to acquire CD using their own information gathering powers as previously was the case.

154. This proposed reform would not diminish the existing statutory requirements for the disclosure of

---

[12] EUR-Lex - 62015CJ0203 - EN - EUR-Lex (europa.eu)

CD. The position remains that an IPA 2016 authorisation is required to obtain the disclosure of CD in the course of any criminal investigation where there is a view to initiating a criminal prosecution.

155. Proposed provisions in the Bill would require any organisation changing their approach from a civil investigation to a criminal investigation (with a view to a criminal prosecution) to satisfy both themselves and the IPCO, that their application of the legislation is right and proper at all times. This is an area that is already subject to oversight and scrutiny and these measures aim to ensure that this reform cannot be used to circumvent the safeguards in place within the IPA 2016.

156. Section 261 IPA 2016 includes the definition of CD. When the IPA 2016 was enacted, section 21 of RIPA 2000 was replaced, and the definition of CD changed. Under section 261(3) "subscriber" or "account data" were brought within a new category of CD referred to as "Entity" data. Section 261(6) of the IPA 2016 created a new definition of what the "content" of a communication is to ensure there's a clear distinction between "content" and CD on the basis of Parliamentary concern in relation to privacy by providing that anything that was "content" could not be CD. However, the section 261(6) "content" carve-out created uncertainty as to whether 'subscriber data' or 'account data' is CD or whether it might be the "content" of a communication created by the subscriber or account information. A short example is provided below:

> Your **name** may be included in an electronic form when you open an online account and when clicking 'submit', it is sent to that company's servers. The **"content"** of that communication could be argued to be the information entered in the form which includes **'subscriber'** communications data information.

157. The intention of the amendment is to provide additional clarity that subscriber data and account data fall within the scope of CD, rather than potentially being within the meaning of "content" under section 261(6) of the IPA. The change aims to achieve clarity because public authorities, the independent oversight body (IPCO) and the TOs carry a risk of having to record or report the acquisition of subscriber or account data as an error (because some TOs might consider it as content and so not disclosable under a part 3 CD authorisation). The provisions proposing the clarification of subscriber or account data as CD aim to reduce the risk of errors and provide greater legal certainty.

## Interception

158. Section 56 of the IPA 2016 prohibits the use of intercepted communication and relevant secondary data in legal proceedings. The exceptions to this principle are set out in Schedule 3 to the IPA 2016.

159. Paragraph 13 of Schedule 3 deals with disclosure to Parole Commissioners for Northern Ireland, to permit the review of intercept materials in certain circumstances.

160. Paragraph 24 of Schedule 3 permits disclosure of relevant intercept materials to a coroner or a legal advisor, the exception only covers the Coroners and Justice Act 2009 which applies to inquests in England and Wales only. The new paragraphs 25 and 26 will extend the exception to coroners and legal advisors conducting inquests and inquiries into deaths in both Northern Ireland and Scotland. This will bring parity among all administrations.

# Territorial extent and application

161. See the table in Annex A for a summary of the position regarding territorial extent and application in the United Kingdom.

162. All measures in the Bill are reserved and apply to the whole of the UK, with the exception of:

a. Clauses 7 and 8 which enable the IPC to appoint up to two deputies to whom functions conferred on the IPC may be delegated when the IPC is unable or unavailable to exercise their functions. This is likely to engage the legislative consent motion process because of the IPC's functions in overseeing the use of investigatory powers by public authorities in Scotland (e.g. policing and local authorities), which fall into devolved competence.

b. Clause 9 enables the IPC to appoint Temporary JCs in exceptional circumstances, which results in a shortage of persons able to carry out the function of Judicial Commissioners. This is likely to engage the legislative consent motion process because of the functions of JCs in assisting the IPC in the exercise of their oversight functions.

c. Clause 10(4) amends section 231(9) IPA 2016 to clarify the scope of the error-reporting obligations imposed on public authorities, to specify that a relevant error includes an error of a description identified in a code of practice issued under Schedule 7 IPA 2016 and other relevant enactments, including RIP(S)A 2000. This is likely to engage the legislative consent motion process.

d. Clause 29 amends the list of persons and bodies dealing with security matters under s.23 of FOIA. FOIA extends to the UK. However, freedom of information policy is a devolved matter, meaning that its application depends on whether devolved administrations have implemented their own freedom of information legislation. The proposed amendment to section 23 FOIA does not apply to the regime under the Freedom of Information (Scotland Act) 2002, as such, this measure does not require a legislative consent motion.

e. Clause 26 makes amendments Schedule 3 IPA 2016 in respect of the Parole Board of England and Wales; these will apply to England and Wales only. A legislative consent motion will not be required. It also creates two new paragraphs at Schedule 3 which apply to Northern Ireland coroners and Scottish sheriffs, these will apply to Northern Ireland and Scotland. A legislative consent motion will not be required, because Part 2 of the IPA 2016 is specifically mentioned in paragraph 17 of Schedule 2 of the Northern Ireland Act 1998.

# Commentary on provisions of Bill

## Part 1: Bulk Personal Datasets

### Low or no reasonable expectation of privacy

#### Clause 1: Requirement for authorisation

163. This clause makes a number of amendments to Part 7 of the IPA 2016 in consequence of the new Part 7A of that Act inserted by clause [2].

164. Subsection (2) amends section 199 (bulk personal datasets: interpretation) so that the definition of when an intelligence service retains a bulk personal dataset (BPD) in that section applies to the new Part 7A as well as Part 7.

165. Subsection (3) amends the heading above section 200 (requirement for authorisation by warrant: general). The heading is amended from "requirement for warrant" to "requirement for authorisation". Subsection (4) amends section 200 so that retention and examination of a bulk personal dataset may be authorised under Part 7A as well as under Part 7.

166. Subsection (5) amends section 201 (exceptions to section 200(1) and (2)) to cross refer to new exceptions introduced to accommodate the changes made by the new Part 7A. Subsection (6) provides a new heading to be inserted after s201.

167. Subsection (7) makes substantial changes to section 220 (initial examination: time limits) so that the procedure that currently applies to sets of information obtained by intelligence services, and to which Part 7 applies, accommodates authorisations under the new Part 7A.

168. Subsection (8) amends section 225 (application of Part to BPDs obtained under this Act) so that a direction under subsection (3) of that section can permit a bulk dataset to which it applies to be retained, or retained and examined, pursuant to an authorisation under the new Part 7A as well as Part 7.

#### Clause 2: Low or no reasonable expectation of privacy

169. This clause inserts new Part 7A (Bulk personal dataset authorisations, low or no reasonable expectation of privacy) after Part 7 of the IPA 2016.

#### New section 226A of the IPA 2016: Bulk personal datasets: low or no reasonable expectation of privacy

170. Section 226A is concerned with the application of Part 7A and sets out the test and factors that determine whether a bulk personal dataset is within its scope.

171. Subsection (1) sets out test which must be applied. The test is whether the nature of the personal data contained within the dataset is such that the individuals to whom the personal data relates could have no, or only a low, reasonable expectation of privacy in relation to that data.

172. Subsection (2) requires that regard must be had to all the circumstances when considering the test in subsection (1), including, in particular, certain factors listed in subsection (3).

173. Subsection (3) lists the factors to which, in particular, regard must be had when considering the test in subsection (1). These are: the nature of the data; the extent to which the data has been made public (either by the individuals to whom the data relates themselves, or with their consent); the extent to which data that has been published has been subject to editorial control or by a person acting in accordance with professional standards; the extent to which the data is widely known about if it has been published or is in the public domain, and; the extent to which the data has

already been used in the public domain.

## New Section 226B of the IPA 2016: Individual authorisation

174. Subsection (1) sets out that, for the purposes of Part 7A, an "individual authorisation" is an authorisation that authorises an intelligence service to retain, or retain and examine, any dataset described in that authorisation. Subsection (2) is self-explanatory.

175. Subsection (3) allows the head of an intelligence service, or a person acting on their behalf, to grant an individual authorisation where certain conditions are met. These conditions are set out in subsections (4) and (5).

176. The conditions in subsection (4) require that the person granting the authorisation considers that s226A applies to the dataset (it is a dataset in respect of which there is no, or only a low, reasonable expectation of privacy), the authorisation is necessary for the exercise of the intelligence services functions and the conduct being authorised is proportionate to what is sought to be achieved by it, and that there are appropriate arrangements in force (approved by the Secretary of State) for storing and protecting the data. Subsections (5) and (6) require that the decision to grant the authorisation has been approved by a Judicial Commissioner (JC), unless the bulk personal dataset falls within an existing category authorisation, or the head of an intelligence service granting the authorisation (or person acting on their behalf) considers there is an urgent need to grant it.

177. Subsection (7) sets out that the head of the intelligence service (or person acting on their behalf) may, if they consider it appropriate to do so, still seek JC approval of their authorisation even if the dataset falls within an authorised category authorisation.

178. Subsection (8) sets out that an individual authorisation relating to a BPD may also authorise the retention or examination of BPDs that do not exist at the time of the authorisation, but which may be reasonably regarded as replacements for the dataset that was authorised. For example, this could include circumstances where a publicly available dataset (that the intelligence service holds under an authorisation) is periodically updated with new information of a type that is already contained within the dataset. In such a case the intelligence service would not need to obtain a new authorisation to retain or examine the newest version of a dataset that it already holds under an authorisation.

## New section 226BA of the IPA 2016: Category authorisation

179. This section provides for "category authorisations", which permit the head of an intelligence service, or a person acting on their behalf, to authorise a category of bulk personal datasets for the purposes of Part 7A if they consider that s226A applies to any dataset that falls within the category described in the authorisation (e.g. by reference to the use to which the datasets will be put). The decision to grant the authorisation must be approved by a JC.

## New section 226BB of the IPA 2016: Approval of authorisations by Judicial Commissioners

180. This section makes provision for the approval of category or individual authorisations by JCs.

181. Subsection (1)(a) sets out that in deciding whether to approve a decision to grant an individual authorisation, a JC must review the conclusions of the decision maker in regards to whether section 226A applies to the bulk personal dataset described in the authorisation. Subsection (1)(b) sets out that in respect of a category authorisation, the JC must review the conclusions of the decision maker as to whether section 226A applies to any dataset that falls within the category of datasets described by the authorisation.

182. Subsection (2) sets out that in deciding whether or not to approve a category or individual

authorisation, the JC must apply the same principles that would be applied by a court on an application for judicial review and ensure that the duties imposed by section 2 IPA 2016 (general duties in relation to privacy) are complied with.

183. Subsection (3) sets out that when refusing to approve a decision to grant a category or individual authorisation, JC must give written reasons for their refusal to the person who decided to grant the authorisation.

184. Subsection (4) sets out that the head of an intelligence service (or person acting on their behalf) may ask the IPC to decide whether to approve the decision to grant an individual or category authorisation that has been refused by a JC.

## New section 226BC of the IPA 2016: Approval of individual authorisations granted in urgent cases

185. This section provides that where an individual authorisation has been granted in urgent circumstances without prior approval from a JC because of an urgent need to grant it, a JC must be informed by the person that granted it. Subsection (3) provides that the JC has three working days (commencing from the day after the urgent authorisation was granted) to decide whether or not to approve the decision to grant the authorisation and to inform the person who granted the authorisation of that decision.

186. Subsection (4) and (5) sets out that where a JC refuses to approve an urgent authorisation, the urgent authorisation ceases to have effect unless already cancelled, may not be renewed and that the head of the intelligence service (or person acting on their behalf) may not ask the IPC to overturn the JC's decision.

187. Subsection (6) provides that where JC has refused to approve the decision to grant an urgent authorisation, the head of the intelligence service must, as far as reasonably practicable, ensure that use of the dataset stops as soon as possible.

188. Subsection (7) provides that where a JC refuses to approve a decision to grant the urgent authorisation, section 220 (Part 7 initial examinations: time limits) applies to that dataset as if intelligence service had obtained that dataset at the time they were notified of the decision to refuse to approve the grant of the urgent authorisation.

189. Under subsection (8), the lawfulness of things done at specified points in reliance on an authorisation that ceases to have effect under this section is not affected by the authorisation ceasing to have effect.

## New section 226C of the IPA 2016: Duration of authorisation

190. This section sets out that the duration of authorisations under Part 7A, unless renewed or cancelled, is, for urgent authorisations, the end of five working days from the day after the day the authorisation was granted, and, in all other cases, is 12 months.

## New section 226CA of the IPA 2016: Renewal of authorisation

191. This section sets out that if certain renewal conditions are met, the head of an intelligence service (or a person acting on their behalf) may renew a category or individual authorisation.

192. Subsection (2) and (3) set out the renewal conditions for an individual authorisation.

193. Subsection (4) sets out the renewal conditions for a category authorisation.

194. Subsection (5) sets out the renewal periods in three specific circumstances. For urgent individual authorisations, the renewal period is the fifth working day after the day on which the authorisation was granted. For an individual authorisation which is part of a category

authorisation that has not been renewed, the renewal period is three months ending with the day at the end of which the authorisation would cease to have effect. In any other case, the renewal period is 30 days ending with the day at the end of which the authorisation would cease to have effect. Subsection (6) sets out that the decision to renew individual and category authorisations must be approved by a JC.

### New section 226CB of the IPA 2016: Cancellation of authorisation

195. This section sets out that the head of an intelligence service (or another Crown servant acting on their behalf) may cancel a category or individual authorisation at any time during its duration and must do so where certain cancellation conditions are met.

196. Subsection (3) provides the cancellation conditions for individual authorisations. These are that: the dataset described in the authorisation no longer meets the test in section 226A, the authorisation is no longer necessary, the conduct authorised is no longer proportionate, or that the intelligence service no longer has arrangements approved by the Secretary of State for the storage of BPDs or for protecting them from unauthorised disclosure.

197. Subsection (4) provides that the cancellation condition for category authorisations is that the test in section 226A no longer applies to any dataset that falls within the category described in the authorisation.

### New section 226CC of the IPA 2016: Non-renewal or cancellation of individual authorisation

198. This section concerns where an individual authorisation ceases to have effect because it has expired without being renewed or because it is cancelled.

199. Subsection (2) provides that the head of an intelligence service (or another Crown servant on their behalf) may decide to grant a new individual authorisation to retain or retain and examine any material held in reliance on an authorisation that has ceased to have effect. In such circumstances a new authorisation must be granted before the end of five working days, beginning with the day on which the authorisation ceased to have effect.

200. Subsection (3) provides that an intelligence service is not in breach of section 200 (1) of (2) (requirement for authorisation) for certain periods where an individual authorisation has ceased to have effect. These periods are five working days beginning with the day on which the authorisation ceases to have effect, or in the case where a new authorisation is granted, the period in which a JC is deciding whether to approve the decision.

### New section 226CD of the IPA 2016: Non-renewal or cancellation of category authorisation

201. This section concerns where a category authorisation ceases to have effect (because it has expired without being renewed or is cancelled) and an individual authorisation has been granted for a dataset that falls within that category, but that authorisation has not been approved by a JC.

202. Subsections (2) and (3) set out that the authorisation ceases to have effect after 3 months unless it is renewed, cancelled or otherwise ceases to have effect before then.

### New section 226D of the IPA 2016: Section 226A ceasing to apply to bulk personal dataset

203. This section provides that where an individual authorisation is granted and in the course of examining the dataset the head of an intelligence service (or person acting on their behalf) believes that section 226A no longer applies to the BPD, or part of the dataset, any activity being carried in relation to that part of the bulk personal dataset must stop as soon as possible. Subsection (3)

provides that in such circumstances, section 220 (Part 7 initial examinations: time limits) applies in relation to the bulk personal dataset as if the set was obtained when that belief was formed. Subsection (4) provides that the individual authorisation in relation to part of the bulk personal dataset to which section 226A no longer applies, is to be treated as if it had been cancelled. Subsection (5) sets out that the lawfulness of certain activity is not affected by this section.

### New section 226DA of the IPA 2016: Annual report

204. This section provides that the head of each intelligence service must provide an annual report to the Secretary of State about the BPDs that were authorised to be retained, or retained and examined, under Part 7A by the intelligence service. The first such report must relate to no less than one year and no more than two years, beginning with the date from which Part 7A is fully brought into force. Subsequent annual reports should cover no more than one year, beginning from the end of the period to which the previous report relates.

### New section 226DB of the IPA 2016: Report to Intelligence and Security Committee

205. This section provides that the Secretary of State must provide an annual report to the Intelligence and Security Committee of Parliament setting out information about category authorisations and renewals of category authorisations granted during the preceding twelve months. The first such report must relate to no less than one year and no more than two years, beginning with the date from which Part 7A comes fully into force. Subsequent annual reports should cover no more than one year, beginning from the end of the period to which the previous report relates.

### New section 226DC of the IPA 2016: Part 7A: Interpretation

206. This section clarifies that within Part 7A and section 199 (bulk personal datasets: interpretation), section 263 (general definitions) and section 265 (index of defined expressions), use of the terms 'category authorisation' and 'individual authorisation' has the same meaning as those provided under section 226B(1). Subsection (3) provides that for Part 7A, only a person holding office under the Crown may act on behalf of the head of an intelligence service.

## Bulk personal dataset warrants

### Clause 3: Duration of bulk personal dataset warrants

207. This clause amends section 213 in Part 7 of the Act so that BPD warrants would have a duration of twelve months rather than six as is currently the case. The proposed change would apply to both class BPD warrants and specific BPD warrants, and would apply to all warrants that are issued or renewed on or after the date that the clause comes into force.

### Clause 4: Agency head functions

208. This clause will make amendments to a number of provisions in Part 7 of the Act in which a function is conferred on the head of an intelligence service. The amendment aims to provide that such functions can be carried out by a Crown Servant on behalf of the head of the intelligence service, as is currently the case in respect of a number of other functions elsewhere in the Act (e.g. making an application for a warrant).

## Third party bulk personal datasets

### Clause 5: Third party bulk personal datasets

209. Clause 5 insets a new Part, Part 7B, into the IPA 2016.

### New section 226E of the IPA 2016: Third party bulk personal datasets: interpretation

210. This section defines when an intelligence service examines a third party bulk personal dataset for the purposes of Part 7B. The requirements are that the intelligence service has relevant access to a

dataset held electronically, by a third party, which includes personal data relating to a number of individuals. The nature of the set must be that the majority of the individuals are not, and are unlikely to become, of interest to the intelligence services. Finally, after an initial inspection, the intelligence service examines the set electronically in situ for the purpose of the exercise of its functions.

211. Subsection (2) defines when an intelligence service has relevant access to a set of information.

### New section 226F of the IPA 2016: Requirement for authorisation by warrant

212. This section prohibits an intelligence service from exercising the power to examine a third party dataset unless that examination is authorised by a warrant under Part 7B ("a 3PD warrant"). A 3PD warrant may authorise the examination to datasets where the content may change over time and future datasets that do not exist when the warrant is authorized.

### New section 226FA of the IPA 2016: Exceptions to section 226F(1)

213. This section provides that the prohibition in s226F(1) does not apply to the exercise of a power to examine a third party bulk personal dataset if done so under any other warrant or authorisation issued or given under the IPA 2016, or to an initial inspection under Part 7B.

### New section 226G of the IPA 2016: Application for third party BPD warrant

214. This section permits the head of an intelligence service or a person acting on their behalf to apply to the Secretary of State. The application must include a general description of the dataset or datasets in the application (a general description may describe more than one dataset provided that the general description applies to each dataset). The requirement to provide a general description is different from the requirement to provide a description for a warrant under Part 7, reflecting the extent to which the intelligence service is able to describe the set given it does not hold a set examined under Part 7B.

215. Where the person making the application knows the dataset consists of protected data or health records, a substantial proportion of it consists of sensitive personal data or the nature of the set, or the circumstances in which it was created, are such that its examination under Part 7B is likely to cause novel or contentious issues, the application must include a statement to that effect.

216. The Secretary of State may issue the warrant if it is considered necessary for specified purposes, the conduct to be authorised is proportionate to what is sought to be achieved by it, there are satisfactory arrangement sin place for the examination of the set and, unless it is urgent, the decision to issue the warrant has been approved by a JC.

217. The application may only be made on behalf of the head of an intelligence service by a person holding office under the Crown.

### New section 226GA of the IPA 2016: Approval of warrants by Judicial Commissioners

218. This section outlines the factors which the JCs must use to decide whether to approve the decision to issue a 3PD warrant. They must review the Secretary of State's conclusions on whether the warrant is necessary and proportionate. The JCs must apply the principles which would be applied by a court on application for judicial review and ensure that the JC complies with the duties imposed by section 2 IPA 2016.

219. If a JC refuses to approve the decision to issue a warrant, written reasons must be provided to the Secretary of State and the Secretary of State may ask the IPC to decide whether to approve to issue the warrant.

## New section 226GB of the IPA 2016: Approval of third party BPD warrants issued in urgent cases

220. This section describes the process for the approval of 3PD warrants issued in urgent cases. This applies when a 3PD warrant is issued without JC prior approval and the Secretary of State considered that there was an urgent need for it to be issued.

## New section 226GC of the IPA 2016: Decisions to issue warrants to be taken personally by Secretary of State

221. This section specifies the Secretary of State must make the decision to issue a 3PD warrant personally. Unless it is not reasonably practicable to do so, the Secretary of State must sign the 3PD warrant. If the Secretary of State does not sign the warrant, it may be signed by a senior official if the relevant conditions are met.

## New section 226GD of the IPA 2016: Requirements that must be met by warrants

222. This section states that a 3PD warrant must be addressed to the head of an intelligence service by whom or on whose behalf the application was made, and it must include a general description of the dataset to which the warrant relates.

## New section 226H of the IPA 2016: Duration of warrants

223. This section outlines the duration of a warrant issued under Part 7B. Generally, a 3PD warrant will last 12 months although a shorter period is provided for in respect of warrants that fall under the urgent approval procedure.

## New section 226HA of the IPA 2016: Renewal of warrants

224. This section states if the renewal conditions are met a 3PD warrant may be renewed by an instrument issued by the Secretary of State.

## New section 226HB of the IPA 2016: Cancellation of warrants

225. This section states the Secretary of State or senior official acting on their behalf may cancel a warrant at any time should the cancellation conditions be met in relation to the warrant. These conditions are that the warrant is no longer necessary on any of the specified grounds or that the conduct authorised is no longer proportionate to what is sought to be achieved by the conduct.

## New section 226HC of the IPA 2016: Non-renewal or cancellation of third party BPD warrant

226. This section outlines where a 3PD warrant is no longer valid as it has expired without being renewed or because it has been cancelled. The head of the intelligence service to whom the warrant was addressed must ensure relevant activity carried out in reliance on the warrant stops as soon as possible, although the lawfulness of certain activity already done or in process is not affected.

## New section 226I of the IPA 2016: Initial inspection

227. This section makes provision for an initial inspection period before a 3PD warrant is required. This initial inspection period allows, amongst other things, an intelligence service to determine whether Part 7B applies to their examination of the set.

### New section 226IA of the IPA 2016: Safeguards relating to examination of third party bulk personal datasets

228. This section outlines safeguards relating to the examination of 3PD warrants. The Secretary of State is required to ensure arrangements are in force to secure that any examinations necessary and proportionate.

### New section 226IB of the IPA 2016: Additional safeguards for items subject to legal privilege: examination

229. This section applies where protected data within a 3PD is to be examined in reliance of a 3PD warrant were the purpose of using criteria for the examination of the data is to identify items subject to legal privilege, or the use of the criteria is likely to have that effect.

### New section 226IC of the IPA 2016: Additional safeguards for items subject to legal privilege: retention following examination

230. This section outlines where, as part of a 3PD examination, an intelligence service examines and retains an item subject to legal privilege (not under Part 7 of the IPA 2016), the person to whom the warrant is addressed must inform the IPC as soon as reasonably practicable after retaining the item. The IPC then has certain powers, including to direct that the item must be destroyed or to impose conditions as to its retention or use.

### New section 226ID of the IPA 2016: Offence of breaching safeguards relating to examination of material

231. This section creates a new offence that applies where a person deliberately examines a third party bulk personal dataset in reliance on a 3PD warrant, knowing or believing that the examination is not necessary and proportionate. This clause brings in an offence for breaching safeguards to examine 3PD material. An offence is committed.

### New section 226IE of the IPA 2016: Part 7B: interpretation

232. This section provides definitions for terms used in Part 7B.

## Minor and consequential amendments

### Clause 6: Minor and consequential amendments

233. This section makes minor and consequential amendments to sections 1 and 2 of the IPA 2016 (oversight and general duties in relation to privacy) to reflect the inclusion of the new Parts 7A and 7B within the Act, as well as making necessary amendments to the Regulation of Investigatory Powers Act 2000 to include conduct carried out under Parts 7A and 7B within the list of activities for which the Investigatory Powers Tribunal is the appropriate forum for complaints.

# Part 2: Oversight Arrangements

### Clause 7: Deputy Investigatory Powers Commissioner

234. Clause 7(2) inserts two new subsections into section 227 of the IPA 2016, as follows.

235. Subsection (6A) sets out that the Investigatory Powers Commissioner (IPC) may formally appoint up to two persons who are Judicial Commissioners (including Temporary Judicial Commissioners) to become Deputy Investigatory Powers Commissioners (DIPC).

236. Subsection (6B) clarifies that a Deputy Investigatory Powers Commissioner continues to be a Judicial Commissioner (JC).

237. Clause 7(3) clarifies the circumstances when a person will cease to be a Deputy Investigatory Powers Commissioner (DIPC). This will be for the following reasons:

> (a) the person ceases to be a Judicial Commissioner,
> (b) the Investigatory Powers Commissioner removes the person from being a Deputy Investigatory Powers Commissioner, or
> (c) the person resigns as a Deputy Investigatory Powers Commissioner."

238. Clause 7(4) will insert the definition of a DIPC and refers to appointment of a DIPC under 227(6A) and the expression is also read in accordance with section 227(13)(b)),".

239. Clause 7(5) will insert the term "Deputy Investigatory Powers Commissioner" into the index of defined expressions.

## Clause 8: Delegation of functions

240. This clause gives the IPC the ability to delegate the exercise their functions to a DIPC, in addition to other JCs, and specifies the scope of delegations to DIPCs and (JCs). This is achieved by amending section 227(8) and inserting new subsections (8A) - (8D).

241. Clause 8(2) inserts subsection (8A) into section 227 IPA, which specifies that certain personal functions conferred on the IPC, such as deciding an appeal against, or a review of, a decision made by a JC, may only be delegated to DIPCs when the IPC is unable or unavailable to exercise their functions for any reason.

242. Subsection (8B) of section 227 clarifies that the IPC's functions, as listed in subsection (8A) may not be delegated to JCs who are not DIPCs.

243. Subsection (8C) of section 227 clarifies that the IPC's functions, as listed in subsection (8A) may not be delegated to JCs who are not DIPCs.

244. Subsection (8D) of section 227 specifies that where there are two DIPCs, the power under section 227(8)(a) may be used to delegate to one DIPC the function of the IPC in deciding an appeal against, or a review of, a decision made by the other DIPC.

245. Subsection (10A) of section 227 specifies that where the exercise of the IPCs functions under section 227(8)(c) (deciding an appeal against, or a review of, a decision made by a JC is delegated to DIPCs and the DIPC decides the appeal or review, no further appeal or request for a further review may be made to the IPC in relation to the decision of the DIPC.

## Clause 9: Temporary Judicial Commissioners

246. This clause inserts new section 228A into the IPA 2016 and gives the IPC and the Secretary of State the power to appoint Temporary JCs in exceptional circumstances, which result in a shortage of persons able to carry out the functions of JCs. In the event of a temporary JC being appointed, the IPC must notify certain persons including the Prime Minister, the Secretary of State and the Scottish Ministers as soon as practicable after the appointment. These provisions are based on section 22 of the Coronavirus Act 2020 and regulation 3 of S.I. 2020/360.

## New section 228A of the IPA 2016: Temporary Judicial Commissioners

247. Subsection (1) sets out when the power to appoint Temporary JCs can be exercised.

248. Subsections (2) and (3) specifies that the IPC may appoint one or more persons to carry out the functions of JCs and that such persons shall be known as Temporary JCs.

249. Subsection (4) specifies the term of a Temporary JC.

250. Subsection (5) sets out who the IPC must notify when a new Temporary JC is appointed.

251. Subsection (6) clarifies that a reference in any enactment is to be read (so far as context allows) as referring also to a Temporary JC.

252. Subsection (7) specifies that certain provisions relating to the appointment of JCs, under section 227 and 228 IPA 2016, are disapplied in relation to the appointment of Temporary JCs. This includes the requirement for the Prime Minister to appoint JCs, for JCs to be appointed on the recommendation of the Lord Chancellor and other senior judges in the three legal jurisdictions and the requirement for the Prime Minister to consult with the Scottish Ministers (section 227(1) and (4)- (6). Section 228(2) IPA 2016 is also disapplied to allow for Temporary JCs to be appointed for one or more terms not exceeding six months each and not exceeding three years in total.

253. Subsection (8) clarifies that in section 228A, the term "Judicial Commissioner functions" means the functions conferred on JCs by any enactment (including the IPA 2016).

## Clause 10: Main functions of the Investigatory Powers Commissioner

254. This clause removes from the investigatory powers main oversight, functions relating to the oversight of prevention or restriction of use of communication devices by prisoners etc.

255. The clause 10(2)(b) places certain MoD oversight functions on a formalised footing, which are currently overseen on a non- statutory footing. To achieve this, this clause inserts into the Act that the IPC must keep under review (including by way of audit, inspection and investigation) compliance by any part of His Majesty's forces, or by any part of the Ministry of Defence, with policies governing the use of surveillance and the use and conduct of covert human intelligence sources outside the UK.

256. This clause 10(3) inserts a provision specifying that the Prime Minister may direct the IPC to carry out additional oversight functions in respect of any public authority not mentioned in section 230(1)(a) - (c), so far as engaging in intelligence activities.

257. This clause 10(4) replaces the reference to a "code of practice under Schedule 7" with a reference to a "relevant code of practice". This is then defined in a new subsection to mean a code of practice under Schedule 7, the Police Act 1997, Regulation of Investigatory Powers Act 2000 or the Regulation of Investigatory Powers (Scotland) Act 2000. This amendment is intended to clarify the scope of "relevant errors" under the IPA 2016.

## Clause 11: Personal data breaches

258. Clause 11(1) inserts a provision into the Investigatory Powers Act (s.235A) for the Investigatory Powers Commissioner to notify affected individuals of serious personal data breaches relating to warrants issued under the Investigatory Powers Act 2016, if the IPC determines it is in the public interest to make such a notification.

259. Subsection (1) sets out the circumstances in which the provision applies, namely where a Telecommunications Operator is prevented from reporting a personal data breach to the Information Commissioner due to a relevant restriction.

260. Subsection (2) sets out that a Telecommunications Operator must report such a personal data breach to the Investigatory Powers Commissioner.

261. Subsection (3) confirms that where a Telecommunications Operator has reported a personal data breach to the Investigatory Powers Commissioner, a Judicial Commissioner must then disclose information about the breach to the Information Commissioner. This will ensure that the Information Commissioner can appropriately investigate such a breach.

262. Subsection (4) sets out that where a Judicial Commissioner discloses information about a personal data breach to the Information Commissioner, the Information Commissioner must consider whether the breach is serious and if such a consideration is made, the Information Commissioner

must notify the Investigatory Powers Commissioner.

263. Subsection (5) confirms that the Investigatory Powers Commissioner must inform an individual of any personal data breach relating to that individual of which the Commissioner is notified by the Information Commissioner, if the Commissioner considers that it is in the public interest for the individual to be informed of the breach.

264. Subsection (6) sets out the factors the Investigatory Powers Commissioner must consider in deciding whether it is in the public interest to notify an individual who has been affected by a personal data breach.

265. Subsection (7) confirms that the Investigatory Powers Commissioner must ask the Secretary of State and any public authority the Commissioner considers appropriate for submissions before making a decision regarding the public interest in notifying the affected individual of a breach.

266. Subsection (8) sets out the information the Investigatory Powers Commissioner must provide when notifying an individual who has been affected by a personal data breach of the breach.

267. Subsection (9) provides that the Investigatory Powers Commissioner may not inform an individual who has been affected by a personal data breach of a breach notified by the Information Commissioner, except as provided by section 235A.

268. Subsection (10) sets out that a personal data breach is considered to be serious if the breach is likely to result in a high risk to the rights and freedoms of individuals.

269. Subsection (11) defines the key terms used throughout this section, covering "the 2003 Regulations" (i.e. the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI/2003/2426) - "PECR"), "personal data breach" and "relevant restriction".

270. Clause 11(2) repeals regulation 5A(9) of PECR to enable Telecommunications Operators to report certain personal data breaches to the Information Commissioner.

271. Clause 11(3) repeals paragraph 14 of Schedule 10 IPA 2016, in consequence of the amendment at Clause 11(2).

# Part 3: Communications Data etc

## Communications data

### Clause 12: Offence of unlawfully obtaining communications data

272. Clause 11 amends section 11. Subclause (2) amends section 11(1) with the effect that public authorities which acquire communications data from another public authority acting as a Telecommunications Operator (TO) which is not wholly or mainly funded out of public funds will not commit a section 11 offence in relation to that acquisition.

273. Subclause (3) inserts a list of examples of cases which will amount to "lawful authority" in subsection (3A) of section 11 in respect of communications data acquisition from a TO or Postal Operator. This is a non-exhaustive list of authorities that will amount to "lawful authority" and which includes the following; where the relevant person has obtained communications data under section 81(1) IPA 2016, where communications data is obtained in the exercise of a statutory power of the relevant public authority (including other authorisations available under the IPA 2016), where the operator lawfully provides the communications data to the relevant public authority, any judicial authorisation e.g. a court order, where the data has been obtained after it has been published and where the communications data has been obtained by the relevant person when responding to a call made to the emergency services.

274. Subclause (3B) sets out the meaning of 'emergency services' and 'publish' as referred to in Subclause (3A).

275. This clause also makes a consequential change to the heading of section 6 with the insertion of 'in relation to interceptions' in order to distinguish it from "lawful authority" for communications data.

## Clause 13: Meaning of "communications data": subscriber details

276. This clause makes clear "communications data" includes entity data that comprises the content of a communication made for the purpose of initiating or maintaining an entity's access to a telecommunications service. It is also the content about an entity to which that telecommunications service is provided or will be provided. It is not the data comprised in the recording of speech, for example voicemails. This proposal would have the practical effect of clarifying that this data is communications data rather than content.

## Clause 14: Powers to obtain communications data

277. This Clause amends Section 12 of the IPA 2016. Currently Section 12 (2) of the Act states that any 'general information gathering power' which would have previously enabled a public authority to secure disclosure of Communications Data from a Telecommunications Operator or Postal Operator,

i. without the consent of the operator,

ii. does not involve a court order or other judicial authorisation or warrant,

iii. and *is not a regulatory power,*

would cease to have effect.

278. Section 12(6) of the Act then narrowly defined a 'regulatory power' as meaning any power to obtain information or documents – but only those exercisable in connection with the regulation of TOs, services or systems or postal operators or services.

279. Clause 14(4) inserts new subsections (2B) to (2D) into section 12 with the effect of disapplying section 11(2)'s limitation of general information powers in certain circumstances. New subsection (2B) provides that subsection (2) does not apply in relation to the exercise of regulatory or supervisory powers, unless those powers are exercised in the course of a criminal investigation. New subsection (2C) defines "criminal investigation". New subsection (2D) provides that an investigation is not in the course of a "criminal investigation" if, at the time of the acquisition of the CD, it is not being done with a view to seeking a criminal prosecution.

280. Clause 14(6) replaces the term 'regulatory power' with the definition of 'regulatory or supervisory power.' and defines this new term as being one exercisable in connection with

i. the regulation of persons or activities,

ii. the checking or monitoring of compliance with requirements, prohibitions or standards imposed by or under an enactment, or

iii. the enforcement of any requirement or prohibition imposed by or under an enactment,

281. This definition of 'regulatory or supervisory power' is designed to capture organisations such as the Financial Conduct Authority and HMRC and their respective regulation of the financial sector and supervision of anti-money laundering regulations.

282. Clause 14(7) introduces a Schedule which reverses certain of the changes made by Schedule 2 to

the IPA 2016 with the effect of reinstating powers available to public authorities which confer regulatory and supervisory powers on those authorities. Those changes made by Schedule 2 to the IPA 2016 relate to powers which can only be used for criminal investigations are unchanged by the Schedule to this Bill.

283. In effect this means that the public authority can only acquire Communications Data from a TO using a regulatory or supervisory power, rather than those conferred under the IPA 2016, if at the time of acquisition their intention is to use the information in support of a civil function or civil penalty and not a criminal prosecution.

## Internet connection records

### Clause 15: Internet connection records

284. The new Clause adds an additional access condition 'D' which stipulates who may use this new condition and under what circumstances. The condition is split into two parts. Condition 'D1' covers the Lawful Purposes for which the new condition may be used when authorisation is by the Investigatory Powers Commissioner. Condition 'D2' covers the more limited Lawful Purposes for which the new condition may be used when internal authorisation is permitted.

285. Clause 15 (1) makes clear that the following clause relates to section 62 of the Act and restrictions in relation to internet connection records.

286. Clause 15(2) and (3) simply amend sections in the Act which mention all conditions to ensure they now also reference the new condition D.

287. Clause 15(4) inserts new subsections 5A, 5B and 5C into the Act which define the new condition D and provides interpretation of the term 'specified.'

288. New subsection (5A) introduces a table which makes clear that condition D1 only applies to the intelligence services and the NCA.

289. It defines Condition D1 as being when the Investigatory Powers Commissioner considers that it is necessary, for a purpose referenced within the table (see below), to obtain data to identify which persons or apparatuses are using one or more specified internet services in a specified period, where "specified" means specified in the application.

290. This is similar to Condition A save that it removes the requirement to possess unequivocal knowledge about the service(s) and time(s) of use and instead permits that these factors be stated within the application, based upon analysis and subject matter expertise.

291. The table relevant to condition 'D1' sets out the limited lawful purposes for which the intelligence services and the NCA may use this provision;

292. For the intelligence services this is:

i. in the interests of national security,

ii. in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security

iii. for the purpose of preventing or detecting serious crime.

293. For the NCA this is;

i. for the purpose of preventing or detecting serious crime.

294. New subsection 5B introduces a further table relevant to condition 'D2.' This sets out the more limited circumstances where a designated senior officer may authorise use of this provision.

295. For the intelligence services this is limited to;

i. in the interests of national security,

ii. in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security

And in urgent cases only;

i. for the purpose of preventing or detecting serious crime.

296. For the NCA condition D2 permits a designated senior officer to authorise use of the provision, in urgent cases only, for the purpose of preventing or detecting serious crime.

297. New subsection 5C explains that the term 'specified' means specified within the application for the authorisation.

# Part 4: Notices

## Retention notices

### Clause 16: Powers to require retention of certain data

298. Clause 16 amends section 87 of the IPA 2016. That section limits what types of relevant communications data can be required to be retained by a TO under a data retention notice under section 87.

299. Subclause (2) inserts wording into section 87(4) to disapply the effect of s87(4) in relation to data that;

a. is, or can only be obtained by processing internet connection records. The effect of this is that such data can be retained under a data retention notice.

b. does not relate to a relevant roaming service.

300. Clause 16(3) inserts new subsection (4A) which defines "relevant roaming service". The effect of this definition read with the exclusion of relevant roaming services from s87(4) is that relevant communications data relating to a relevant roaming service can be subject to a data retention notice under section 87.

### Clause 17: Extra-territorial enforcement of retention notices etc

301. This clause amends section 95(5) and 97 to allow extraterritorial enforcement of data retention notices to strengthen policy options when addressing emerging technology, bringing it in line with technical capability notices (TCNs).

## Retention, national security and technical capability notices

### Clause 18: Review of notices by the Secretary of State

302. When a notice is formally given to a TO by the Secretary of State, its obligations become binding on them. If at this point the operator is dissatisfied with the terms of the notice, they have a statutory right to refer the notice (or part of it) to the Secretary of State for review.

303. Section 90(4)(a) (data retention notices) specifies that during that review period the TO is not required to make any changes to specifically comply with the notice. This requirement is replicated in section 257(3)(a) (national security and technical capability notices). This ensures consistency across all notice types.

304. Section 90(4A) specifies that the TO must not make any relevant changes which relates to

obligations within the notice. Subsection (4B) defines "relevant change", This proposal would preserve the status quo during the review period, meaning if the TO was providing assistance in relation to warrants, authorisations or notices under the IPA 2016 then this assistance must continue during the review period. This requirement is replicated in section 257(3A) and (3B) to ensure consistency across all notice types.

305. Section 90(5) (data retention notices) is amended to specify that the Secretary of State must review a notice before the end of the review period and decide what action to take under subsection (10). This requirement is replicated in section 257(4) (national security and technical capability notices) to ensure consistency across all notice types.

306. Section 90(5A) (data retention notices) defines the "review period". This amendment introduces a new regulation making power, enabling the Secretary of State to specify in regulations the overall length of time a review of a notice can take. This requirement is replicated in section 257(4A) (national security and technical capability notices) to ensure consistency across all notice types.

307. Section 90(9A) and (9B)(data retention notices) make provisions for a JC to give a direction to the operator and Secretary of State specifying the time period within which both parties may provide evidence or representations and the power to disregard any submissions provided outside these timescales. This requirement is replicated in Section 257(8A) and (8B) (national security and technical capability notices) to ensure consistency across all notice types.

308. The amendment to Section 90(10) (data retention notices) ensures the Secretary of State must, after considering the conclusions of the TAB and JC, decide what action to take before the end of the "relevant period". This requirement is replicated in section 257(9) (national security and technical capability notices) to ensure consistency across all notice types.

309. Section 90(11A) (data retention notices) defines the "relevant period". This amendment introduces a new regulation making power, enabling the Secretary of State to specify in regulations the length of time the Secretary of State can take to reach a decision. This requirement is replicated in section 257(10A) (national security and technical capability notices) to ensure consistency across all notice types.

310. Section 90(14)-(16) (data retention notices) makes provision for the Secretary of State to include in regulations made pursuant to these clauses, provisions to extend any period of time provided for by the regulations, the circumstances in which the Secretary of State may extend the review period and the relevant period and the associated requirements if an extension is sought. These requirements are replicated in Section 257(13)-(15) (national security and technical capability notices) to ensure consistency across all data types.

311. The amendment to 267(3) applies the affirmative procedure to regulations made under these sections.

312. The amendment to section 95(5) ensures (data retention notices) that the new duty under section 90(4A) is enforceable by current mechanisms specified in this section. This requirement is replicated in section 255(10) (national security and technical capability notices) in relation to the new duty under section 257(3A).

313. The further amendment to section 255(10) ensures subsection (8), the prohibition of revealing the existence of notices, is enforceable by current mechanisms specified in this section, just as subsection already 9 is. This is to ensure consistency across all notice types.

## Clause 19: Meaning of "telecommunications operator" etc

314. As companies increasingly have multiple entities spread across the globe involved in the delivery of their services, this clause amends the definition of a TO out of an abundance of caution to ensure the IPA 2016 continues to apply to all those it was intended to.

315. Section 261(10)(c) provides additional clarification ensuring that large companies with complex corporate structures are covered in their totality by the IPA 2016. This amendment is not seeking to bring additional companies within scope.

316. The amendment to section 253(1)(a) makes clear that a TCN may be issued to one entity in relation to another entity's capability.

### Clause 20: Renewal of notices

317. Section 87(6A) (data retention notices) introduces a new obligation for a notice to be renewed, if it has not been varied so as to require additional obligations, renewed or revoked, within the relevant period. Subsection (6B) defines the "relevant period" as a period of two years beginning with the day a notice comes into force (if the notice has not previously been varied) or in the case of a notice that has been varied or renewed, the day after the day the notice would have ceased to have effect, had it not been varied or renewed. This requirement is replicated in section 255(5A) and (5B) (national security and technical capability notices) to ensure consistency across all notice types.

### New sections 94A and 256A of the IPA 2016: Renewal of notices

318. Section 94A(2) sets out the renewal conditions which the Secretary of State must take into account for the purposes of determining the necessity and proportionality justifications of the notice. The provision also specifies that the decision to renew a notice is subject to the approval of a JC. This requirement is replicated in section 256A(2) for national security notices and subsection (3) for TCNs to ensure consistency across all notice types.

319. Section 94A(3)-(5) make clear the renewal period, the manner in which the Secretary of State may bring the renewal to attention of the operator and ensuring that the current processes regarding the issuing of a data retention notice, under sections 87(10), 88, 89 and 90, apply to renewals. This is replicated in section 256A subsections (4)-(7) to ensure that current processes for issuing national security and technical capability notices apply to renewals.

320. A consequential amendment to section 229(8)(e)(i) is required to bring notices requiring renewal, pursuant to sections 94A and 256A, under the main oversight functions of the IPC. This ensures JCs are able to carry out their functions in deciding whether to approve the renewal of a notice.

## Notification of changes to telecommunications services etc

### Clause 21: Notification of proposed changes to telecommunications services etc

321. This clause amends the IPA 2016 by inserting section 258A into the Act.

### New section 258A of the IPA 2016: Notification of proposed changes to telecommunications services etc

322. Section 258A(1) introduces a notification requirement. This is an obligation that the Secretary of State can place on an operator that requires them to notify the Secretary of State of relevant changes that the operator is intending to make.

323. Subsection (2) and (3) defines the term "relevant change", which is a change to a service or system provided by the operator and that is specified in regulations.

324. Subsection (4) makes provisions for regulations, which will set out thresholds for the notification requirement to ensure that it does not disproportionately or unnecessarily affect operators who do not hold or provide operationally relevant data.

325. Subsection (5) and (6) sets out what the Secretary of State must consider before issuing a notice to an operator under this section.

326. Subsection (7) requires the Secretary of State to consult the operator before giving them a notice under this section. The proposed provisions would require the Government to discuss during the consultation the Government the specifics of the obligation with the operator before the Secretary of State issues the notice. These individualised and confidential specifics will be included in the formal notice issued by the Secretary of State.

327. Subsections (8)-(10) ensures that the new duty under 258A and the non-disclosure of the existence of a notice under this section is enforceable by civil proceedings.

328. Subsection (11) and (12) defines the term "relevant operator". This is to ensure that the notification requirement can be placed on operators that provide lawful access of significant operational value and who currently provide assistance with warrants, authorisations or notices under the IPA 2016. This is to ensure the notification requirement does not disproportionality affect all operators.

329. A consequential amendment to sections 65, 67 and 68 of RIPA 2000 is required to bring notices issued pursuant to section 258A under the Investigatory Power Tribunal's jurisdiction (consistent with other similar notices issued under the IPA). This is a minor and technical amendment.

### New section 258B of the IPA 2016: Variation and revocation of notices given under section 258A

330. Section 258B introduces a provision that allows the Secretary of State to vary or revoke a notice under this section if required. This is to ensure that the notification requirement remains necessary and proportionate and continues to accurately reflect the systems and services the operator provides and are in scope of the thresholds.

# Part 5: Miscellaneous

## Members of Parliament

### Clause 22: Interception and examination of communications: Members of Parliament etc

331. Subsection (1) sets out that the clause amends section 26 of the IPA 2016. Section 26 sets out the additional safeguards that apply to the issue of a targeted interception warrant or a targeted examination warrant, where the purpose of that warrant relates to the acquisition of communications sent by, or intended for, a member of relevant legislature (such as an MP). The safeguard in section 26 is sometimes referred to as the "triple lock".

332. Subsection (2) amends section 26(2) IPA 2016 to provide, that where conditions A and B are met, a Secretary of State designated under the amended s26 may approve the issue of the warrant instead of the Prime Minister. The approval decision may not be made by the Secretary of State to whom the warrant application is made.

333. Subsection (3) inserts new subsections (2A) - (2E) at the end of section 26. New subsection (2A) provides condition A, which is that the Prime Minister is unable to decide whether to give approval under subsection (2), due to incapacity or an inability to access secure communications. New subsection (2B) sets out condition B, which is that there is an urgent need for the approval decision to be made. Both conditions A and B must be met for a designated Secretary of State to be able to give approval in place of the Prime Minister.

334. New subsection (2C) and (2D) specify that the Prime Minister may only designate individuals holding the office of Secretary of State and only five such individuals may be designated. Subsection (2D) also specifies that an individual Secretary of State may only be designated if they are required in their "routine duties" to issue warrants under sections 19 or 102. . New subsection

(2E) provides for the duration of such a designation under s26, which is that it will end when the individual ceases to hold the office of Secretary of State or when the Prime Minister revokes the designation. Subsection (2F) provides a definition of "senior official" for the purposes of that section, as amended.

### Clause 23: Equipment interference: Members of Parliament etc

335. Subclause (1) sets out that the following sections amend Section 111 of the IPA 2016. The subsequent sections set out which sections will be amended and how.

336. Subclause (2) provides, that where conditions A and B are met, a Secretary of State, other than the original authorising Secretary of State, may provide the final authorisation in the triple lock mechanism in relation to a targeted equipment interference warrant or a targeted examination warrant. Subclause (3) inserts wording into section 111(6) to the same effect but in relation to a targeted equipment interference warrant from a law enforcement chief.

337. Subclause (4) inserts new subsections (7A) - (7E) into section 111. New subsection (7A) provides condition A, which is that the Prime Minister is unavailable to decide whether to approve the issue of the warrant due to incapacity or an inability to access secure communications. New subsection (7B) sets out condition B, which is that there is an urgent need for the approval decision to be made. Both conditions A and B must be met for a designated Secretary of State to be able to give approval in place of the Prime Minister.

338. New subsections (7C) and (7D) specify that the Prime Minister may only designate individuals holding the office of Secretary of State and only five such individuals may be designated. Subsection (2D) also specifies that an individual Secretary of State may only be designated if they are required in their "routine duties" to issue warrants under sections 19 or 102. only a Secretary of State can be designated under section 111. New subsection (7D) provides for the duration of such a designation under section 111, which is that it will end when the individual ceases to hold the office of Secretary of State or when the Prime Minister revokes the designation.

## Equipment interference

### Clause 24: Issue of equipment interference warrants

339. Subsection 1 describes the location within the Act that the relevant changes will be made to – Part 1 of the table in Schedule 6.

340. Subsection 2 substitutes the reference to section 12A(1) and (2) of the Police Act 1996, (which is referenced to allow for the delegation from the Chief Constable to Deputy and Assistant Chief Constables in urgent cases), now repealed, to instead reference section 41(1) and (5) of the Police Reform and Social Responsibility Act 2011.

341. Subsections 3 and 4 allows for Deputy Director Generals at the NCA to be able to issue Targeted Equipment Interference warrants and delegate their authorisation functions to designated senior officers in the NCA in urgent cases.

342. Amend process of removal of subjects from a TEI or TXEI warrant.

343. This clause removes the requirement to notify the Secretary of State where a modification is to remove any matter, name or description included in the warrant in accordance with section 115(3) to (5).

### Clause 26: Issue of targeted examination warrants to intelligence services

344. This clause amends section 102(4) IPA 2016 to allow the Secretary of State to issue warrants for Scottish applications for national security purposes.

### Clause 27: Bulk equipment interference: safeguards for confidential journalistic material etc

345. This clause improves journalistic safeguards within the IPA's bulk equipment interference regime (Section 195).

346. It will replace the existing Section 195 provisions with a requirement for prior independent authorisation by the Investigatory Powers Commissioner before criteria can be used to select material for examination (from that acquired under a bulk equipment interference warrant) for the purpose of finding confidential journalistic material or finding or identifying a source of journalistic information, or where the finding or identifying of such material is highly likely.

347. The clause provides a new urgency process (Section 195A) for dealing with requests which need to be approved out of hours, for authorisations to use criterial to select material for examination. These authorisations will be undertaken by a senior official (under Section 195(2)) rather than the Investigatory Powers Commissioner, and will be subject to subsequent judicial authorisation as soon as reasonably practicable.

348. The clause also provides a consequential amendment to section 229(8) which includes references to the new functions of the Investigatory Powers Commissioner in sections 195 and 195A to ensure consistency within the IPA.

## Exclusion of matters from legal proceedings etc: exceptions

### Clause 28: Exclusion of matters from legal proceedings etc: exceptions

349. This clause creates exceptions to the prohibition on disclosing intercept materials to be used as evidence under s.56. The exception is being extended to proceedings before the Parole Board of England and Wales and will also affect any subsequent proceedings that arise out of those proceedings (such as an appeal). The clause also provides the limits on the disclosure of intercept material for this purpose.

350. An exception is also being introduced to permit disclosure to certain coroners who conduct inquiries or inquests in Northern Ireland and relevant sheriffs who conduct inquiries or inquests into a person's death in Scotland. New paragraph 25 of Schedule 3 to the IPA 2016 makes it clear that a disclosure can be made to a relevant coroner or, in certain circumstances, to a legal adviser working with them. New paragraph 26 of Schedule 3 to the IPA 2016 permits disclosures to relevant persons conducting an inquiry under the Inquiries into Fatal Accidents and Sudden Deaths etc. (Scotland) Act 2016 or a lawyer appointed under section 24 of that Act to assist the relevant person.

## Freedom of information

### Clause 29: Freedom of information: bodies dealing with security matters

351. This clause inserts JCs into s.23 of the Freedom of Information Act 2000 to ensure that the bodies that support JCs can rely on the s.23 exemption to protect sensitive information from disclosure in response to FOIA requests.

# Part 6: General

## General

### Clause 30: Power to make consequential provision

352. This Clause allows for the Secretary of State to amend or repeal a provision of the Bill. The

Secretary of State can only do this by laying a statutory instrument which must be approved by both Houses of Parliament in relation to changes to an instrument which changes primary legislation. If the instrument makes consequential changes which are to legislation other than to primary legislation, the instrument will be subject to annulment by a resolution of either House of Parliament.

### Clause 31: Extent

353. This clause sets out the territorial extent of the Act. Subsection (3) provides for the Act to be extended to (with or without modifications) to the Isle of Man or any of the British overseas territories, by Order in Council.

### Clause 32: Commencement

354. Part 6 (this part) comes into force on the day on which the Bill is passed. The other provisions of the Bill come into force on such day as is appointed by regulations made by the Secretary of State.

355. Regulations under this clause may include provision of the sort mentioned in subsection (3) and (4), namely transitional and saving provision and different provisions for different purposes. They are to be made by statutory instrument but are not subject to the negative or affirmative Parliamentary procedure.

### Clause 33: Short title

356. The Bill, once passed, is to be referred to as the Investigatory Powers (Amendment) Act 2024.

## Schedule: Disclosure powers

357. The clause to amend section 12 and the powers to obtain communications data reverses the effect of certain repeals of disclosure powers and makes consequential provision to schedule 2.

### Part 1: Restoration of disclosure powers

358. Health and Safety at Work etc Act 1974

a. In section 20 of the Health and Safety at Work etc Act 1974 (powers of inspectors), omit subsections (9) and (10).

359. Criminal Justice Act 1987

a. In section 2 of the Criminal Justice Act 1987 (investigation of powers of the Director of Serious Fraud Office), omit subsections (10A) and (10B).

360. Consumer Protection Act 1987

a. In section 29 of the Consumer Protection Act 1987 (powers of search etc), omit subsections (8) and (9).

361. Environment Protection Act 1990

a. In section 71 of the Environment Protection Act 1990 (obtaining of information from persons and authorities), omit subsections (5) and (6).

362. Financial Services and Markets Act 2000

a. In section 175 of the Financial Services and Markets Act 2000 (information gathering and investigations: supplemental provision), omit subsections (5A) and (5B).

### Part 2: Consequential amendments

363. In consequence of the above, paragraphs 1 to 4 and 9 of Schedule 2 to the IPA 2016 (abolition of disclosure powers) will be omitted.

# Commencement

364. Clause 32 makes provision regarding when measures in this Bill will come into force.

# Financial implications of the Bill

365. There will be increased resource cost to IPCO, these costs are from where changes to the legislation requires IPCO to change their current activity and increase resource to ensure the correct oversight or to engage with changes to the IPA 2016. It is not possible to monetise this increased resource cost due to data issues around the time IPCO takes to ensure oversight for individual areas of the IPA 2016.

366. The Bill will result in some increased costs for the intelligence service and Law Enforcement Agencies, in the form of additional resource. The cost of this increased resource cannot be estimated due to the current level of resource being allocated to IPA 2016 related activities being unknown, and in some cases classified.

# Parliamentary approval for financial costs or for charges imposed

367. A money resolution is required where a Bill authorises new charges on the public revenue (broadly speaking, new public expenditure). This Bill requires a money resolution because it confers new functions on the Secretary of State, the intelligence services and the Judicial Commissioners, which might result in an increase in costs. In particular, Part 1 establishes new regimes in relation to bulk personal datasets and Part 4 establishes a new notification requirement, and includes provisions about the renewal of certain other notices, under the Investigatory Powers Act 2016.

# Compatibility with the European Convention on Human Rights

368. The Rt Hon James Cleverly MP, Secretary of State for the Home Department, , has made the following statement under section 19(1)(a) of the Human Rights Act 1998:

> "In my view the provisions of the Investigatory Powers (Amendment) Bill are compatible with the Convention rights".

369. The Government has published a separate ECHR Memorandum with its assessment of the compatibility of the Bill's provisions with the Convention rights. This Memorandum is available on the Government website.

370. The Government considers that the safeguards in this regime are appropriate to the potential intrusion associated with the retention, or retention and examination, by the intelligence services of the datasets to which it is intended to apply.

# Environment Act 2021: Section 20

371. The Rt Hon James Cleverly MP, Secretary of State for the Home Department, is of the view that the Bill as brought from the House of Lords does not contain provision which, if enacted, would be environmental law for the purposes of section 20 of the Environment Act 2021. Accordingly, no

statement under that section has been made.

# Related documents

372. The following documents are relevant to the Bill and can be read at the stated locations:

- A question of trust: report of the investigatory powers review[13]
- Annual Report of the Investigatory Powers Commissioner 2019[14]
- Annual Report of the Investigatory Powers Commissioner 2021[15]
- EUR-Lex - 62015CJ0203 - EN - EUR-Lex[16]
- Home Office report on the operation of the Investigatory Powers Act 2016[17]
- Home Secretary response to Lord Anderson review of Investigatory Powers Act[18]
- Independent review of the Investigatory Powers Act 2016[19]
- Investigatory Powers Act 2016 Investigatory Powers Act 2016[20]
- Investigatory Powers Bill: bulk powers review[21]
- IPA Factsheet[22]
- Revised Investigatory Powers Act notices regimes consultation[23]
- The Data Retention and Acquisition Regulations 2018[24]
- The Investigatory Powers Act 2016 (Commencement No. 12) Regulations 2020[25]

---

13 https://www.gov.uk/government/publications/a-question-of-trust-report-of-the-investigatory-powers-review

14 Annual Report of the Investigatory Powers Commissioner 2019 (ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com)

15 HC 910 – Investigatory Powers Commissioner's Office – Annual Report of the Investigatory Powers Commissioner 2021 (ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com)

16 EUR-Lex - 62015CJ0203 - EN - EUR-Lex (europa.eu)

17 Home Office report on the operation of the Investigatory Powers Act 2016 (accessible version) - GOV.UK (www.gov.uk)

18 Lord Anderson publishes review of Investigatory Powers Act - GOV.UK (www.gov.uk)

19 Independent review of the Investigatory Powers Act 2016 - GOV.UK (www.gov.uk)

20 Investigatory Powers Act 2016 (legislation.gov.uk)

21 Investigatory Powers Bill: bulk powers review - GOV.UK (www.gov.uk)

22 Investigatory Powers (Amendment) Bill: factsheets - GOV.UK (www.gov.uk)

23 Revised Investigatory Powers Act notices regimes consultation - GOV.UK (www.gov.uk)

24 The Data Retention and Acquisition Regulations 2018 (legislation.gov.uk)

25 The Investigatory Powers Act 2016 (Commencement No. 12) Regulations 2020 (legislation.gov.uk)

# Annex A – Territorial extent and application in the United Kingdom

| Provision | England | Wales | | Scotland | | Northern Ireland | |
|---|---|---|---|---|---|---|---|
| | **Extends to E & W and applies to England?** | **Extends to E & W and applies to Wales?** | **Legislative Consent Motion process engaged?** | **Extends and applies to Scotland?** | **Legislative Consent Motion process engaged?** | **Extends and applies to Northern Ireland?** | **Legislative Consent Motion process engaged?** |
| Part 1 | | | | | | | |
| Clause 1 | Yes | Yes | No | Yes | No | Yes | No |
| Clause 2 | Yes | Yes | No | Yes | No | Yes | No |
| Clause 3 | Yes | Yes | No | Yes | No | Yes | No |
| Clause 4 | Yes | Yes | No | Yes | No | Yes | No |
| Clause 5 | Yes | Yes | No | Yes | No | Yes | No |
| Clause 6 | Yes | Yes | No | Yes | No | Yes | No |
| Part 2 | | | | | | | |
| Clause 7 | Yes | Yes | No | Yes | Yes | Yes | No |
| Clause 8 | Yes | Yes | No | Yes | Yes | Yes | No |
| Clause 9 | Yes | Yes | No | Yes | Yes | Yes | No |
| Clause 10 | Yes | Yes | No | Yes | Yes | Yes | No |
| Part 3 | | | | | | | |
| Clause 11 | Yes | Yes | No | Yes | No | Yes | No |
| Clause 12 | Yes | Yes | No | Yes | No | Yes | No |
| Clause 13 | Yes | Yes | No | Yes | No | Yes | No |
| Clause 14 | Yes | Yes | No | Yes | No | Yes | No |
| Clause 15 | Yes | Yes | No | Yes | No | Yes | No |
| Part 4 | | | | | | | |
| Clause 16 | Yes | Yes | No | Yes | No | Yes | No |
| Clause 17 | Yes | Yes | No | Yes | No | Yes | No |
| Clause 18 | Yes | Yes | No | Yes | No | Yes | No |
| Clause 19 | Yes | Yes | No | Yes | No | Yes | No |
| Clause 20 | Yes | Yes | No | Yes | No | Yes | No |
| Clause 21 | Yes | Yes | No | Yes | No | Yes | No |
| Part 5 | | | | | | | |
| Clause 22 | Yes | Yes | No | Yes | No | Yes | No |
| Clause 23 | Yes | Yes | No | Yes | No | Yes | No |
| Clause 24 | Yes | Yes | No | Yes | No | Yes | No |
| Clause 25 | Yes | Yes | No | Yes | No | Yes | No |

| Provision | England | Wales | | Scotland | | Northern Ireland | |
|---|---|---|---|---|---|---|---|
| | **Extends to E & W and applies to England?** | **Extends to E & W and applies to Wales?** | **Legislative Consent Motion process engaged?** | **Extends and applies to Scotland?** | **Legislative Consent Motion process engaged?** | **Extends and applies to Northern Ireland?** | **Legislative Consent Motion process engaged?** |
| Clause 26 | Yes | Yes | No | Yes | No | Yes | No |
| Clause 27 | Yes | Yes | No | Yes | No | Yes | No |
| Clause 28 | Yes | Yes | No | Yes | No | Yes | No |
| Clause 29 | Yes | Yes | No | No | No | Yes | No |
| Part 6 | | | | | | | |
| Clause 30 | Yes | Yes | No | Yes | No | Yes | No |
| Clause 31 | Yes | Yes | No | Yes | No | Yes | No |
| Clause 32 | Yes | Yes | No | Yes | No | Yes | No |
| Clause 33 | Yes | Yes | No | Yes | No | Yes | No |

## Subject matter and legislative competence of devolved legislatures

373. In the opinion of the UK Government, this Bill has areas within the devolved competence of Scotland. This includes amendments relating to the IPC's powers to appoint deputies and delegate functions to Judicial Commissioners, where they provide oversight arrangements for devolved authorities and bodies exercising devolved functions. The rest of the content of the Bill relates to national security matters that are reserved to the UK Government.

# INVESTIGATORY POWERS (AMENDMENT) BILL [HL]

## EXPLANATORY NOTES

These Explanatory Notes relate to the Investigatory Powers (Amendment) Bill [HL] as brought from the House of Lords on 31 January 2024 (Bill 157).

---

Ordered by the House of Commons to be printed, 31 January 2024

---



**PUBLISHED BY AUTHORITY OF THE HOUSE OF COMMONS**