EXPLANATORY NOTES

Investigatory Powers (Amendment) Act 2024

Chapter 9

tso
a Williams Lea company

Published by TSO (The Stationery Office), a Williams Lea company, and available from:

Online
www.tsoshop.co.uk

Mail, Telephone & E-mail
TSO
PO Box 29, Norwich, NR3 1GN
Telephone orders/General enquiries: 0333 202 5070
E-mail: customer.services@tso.co.uk
Textphone: 0333 202 5077

ISBN 978-0-10-560377-1

9 780105 603771

£19.35

INVESTIGATORY POWERS (AMENDMENT) ACT 2024

EXPLANATORY NOTES

What these notes do

These Explanatory Notes relate to the Investigatory Powers (Amendment) Act 2024 which received Royal Assent on 25 April 2024 (c. 9).

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

Table of Contents

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 Commissioner's Office

JC – Judicial Commissioner

ML – Machine learning

MOD – Ministry of Defence

NCA – National Crime Agency

NSN – National Security Notices

Ofcom – Office of Communications

PECR – The Privacy and Electronic Communications (EC Directive) Regulations 2003 (S.I. 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 Act

1. The Investigatory Powers (Amendment) Act 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 Act follows the publication of the Home Secretary's statutory report on the IPA 2016 in February 2023[1], and a subsequent independent review by the former Independent Reviewer of Terrorism Legislation, Lord Anderson of Ipswich KBE KC, published in June 2023[2]. 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 Act 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 Act 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) Act 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 s260 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) Act 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 its statutory functions.

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

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, 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 resources in protecting national security.

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

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 the head of an intelligence service.

23. Building on these recommendations, this Act:

    a. Amends safeguards for the retention and examination of BPDs where there is low or no reasonable expectation of privacy. This creates 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. Amends 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. Makes clear that the head of an intelligence service – the agency head – can delegate certain existing functions in relation to BPD warrants. This enables 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).

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 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 those that are generally available in order to support

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

them in carrying out their statutory functions. It may be more proportionate or practical for the intelligence service to examine *in situ* a dataset held by a third party rather than acquire and retain the data themselves.

26. The Act inserts 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).

27. The new regime introduces 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.

28. Lord Anderson's review of the IPA 2016 noted that the Investigatory Powers Commissioner's 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 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

29. 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.*

30. 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.
- 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

[6] Annual Report 2019 – IPCO

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).

31. 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.

32. 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.

33. 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.

34. 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.

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

35. The Government consultation response was published 7 November 2023. This response set out the amendments to Part 4 and Part 9 of the IPA 2016 that were made in this Act 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 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 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.

36. 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 Act, therefore, amends Section 95 and 97 to allow extraterritorial enforcement of DRNs to strengthen policy options when addressing emerging technology, bringing them in line with TCNs. This ensures that notices given to international telecommunication operators can be enforced, should they need to be. The Act also clarifies 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).

37. 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 Act 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.

38. 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 is not considered necessary to amend enforcement at this time.

Internet Connection Records (ICRs)

39. 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 the ability of investigators to discover and prosecute serious criminals would be revolutionised by better use of these ICRs.

40. The way in which the IPA 2016 was originally drafted required certain thresholds to be met on the 'known' elements of the investigation, such as when a website had been accessed. Condition A for ICR access is focused on identifying subjects relevant to **specific known event(s)** and does not permit enquiry into wider use beyond that known event(s). A significant gap existed with ICRs where, for example, analysis of a seized device identified a site serving images of child

sexual exploitation or that the device was being used for communications between threat actors. In such circumstances, ICRs could **not have** been used to detect other unknown subjects using those sites, beyond a specific *known* event.

41. This limited the ability of the intelligence services and the NCA to use ICRs to detect previously 'unknown' criminals online. The changes will 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, where previously this would not have been possible using ICRs.

42. The Act adds a new condition D to the list of existing conditions for the use of ICRs at s62 of the IPA 2016. This will enable target detection, which was not possible using the existing ICR conditions A to C. This new condition D is only available to the intelligence services and the NCA, and 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 therefore is to enable the intelligence services and the NCA to detect previously unknown individuals who are using the internet to commit high-harm crimes. The addition of condition D is a relatively small change to the Act as the intelligence services and the NCA are already permitted to use the existing ICR conditions for subject identification but were required to know the time of access and service in use to do so, which limited the utility of the capability to assist in detecting new subjects of interest.

44. The measure allows 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 ready access to children. Intelligence derived from ICR applications could assist law enforcement partners in prioritising 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. This 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. Flagging suspicious behaviour in that way can lead to action being taken to prevent criminals from defrauding their intended victims.

47. 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 should explain their reasoning with reference to tangible supporting information which is subject to the existing oversight and safeguards of the regime. Data returned as a result of a Condition D application will be subject to the safeguards as set out in the Codes of Practice, including that data may only be held for as long as the relevant public authority is satisfied that it is still necessary for a statutory purpose.

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 identified potential ways to improve the regime while maintaining this balance.

52. Firstly, given the restrictive nature of the existing 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 the Prime Minister being unable to consider a warrant application due to medical incapacitation or a lack of access to secure communications. The Act makes changes 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 does this by providing that alternative approvers of sufficient rank or office are able to approve warrant applications in urgent circumstances. Alternative approvers must have the necessary operational awareness, which will be further defined in the relevant Codes of Practice, in order to be appointed by the Prime Minister to consider warrant applications when the Prime Minister is unable to do so. In the case of Section 26 or 111 warrants, the Act makes 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 Act makes 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 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 Act therefore makes an amendment to the processes associated with the removal of a subject from a TEI warrant which removes the requirement to notify the Secretary of State at the point of the removal of the subject.

55. Fourthly, the Act makes changes to the table in Part 1 of Schedule 6 of the IPA 2016 which rectify 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. As enacted, the IPA 2016 referred 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 has been 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 Act tidies up the IPA 2016 and corrects 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 reforms to the IPA 2016 in this Act 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 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 measures 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 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 measure in the Act 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 does not give the MoD or the IPC any new powers; however, it does formalise this agreement to increase oversight.

Flexibility and resilience

61. The Act contains measures which 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 in this Act 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. This ensures clearer parameters regarding the IPC's oversight and ensures that law enforcement agencies, such as, the NCA are included in the scope of s.230, with the flexibility that would allow a rapid response to emerging oversight requirements.

63. The IPA 2016 did not make 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 approve the decision of a Secretary of State to give a notice). Lord Anderson's report highlighted that this could hamper IPCO's resilience and agility, particularly in circumstances where the IPC may be unavailable to carry out their role. The Act allows for up to two Deputy IPCs to be appointed, 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 might become unavailable. The specific appointment and removal from office of Deputy IPCs would be the responsibility of the IPC.

64. The Act contains a measure which delegates 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 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 gives Deputy IPCs the power to determine such appeals when the IPC is unable or unavailable to determine them.

65. 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. 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 Act amends the IPA 2016 to remove this limitation and allows the IPC's power in respect of CD authorisation to be generally exercised by JCs.

66. This Act removes 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 was previously 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. Following the suspension of the emergency legislation, the Home Office has replicated the procedures, safeguards, and terms of appointment set out in ss. 22 and 23 of the Coronavirus Act 2020 in this Act, but removed the connection to coronavirus and widened its application to exceptional circumstances which result in a shortage of JCs. Specifically, the powers provide 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 Act includes 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 change makes 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. These amendments specifically includes these codes and legislation within the IPA 2016's error reporting regime (s.231(9)) and clarifies that such errors fall within the IPC's remit.

Personal data breaches

69. This Act includes measures that specify Telecommunications Operators (TOs) must notify certain personal data breaches to the Investigatory Powers Commissioner (IPC) who must then disclose to the Information Commissioner details of those breaches. The Act provides the IPC with the power to inform an individual if they have been affected by a personal data breach committed by a TO, if the IPC determines it is in the public interest to do so. The Act also repeals s.5A(9) of PECR, so TOs are required to notify any Personal Data Breaches that occur in relation to authorisations or notices for Communications Data under Part 3 of the Act to the Information Commissioner.

70. The Act also makes amendments to the Regulation of Investigatory Powers Act 2000 to ensure that the Investigatory Powers Tribunal has the jurisdiction to consider and determine complaints about personal data breaches committed by TOs.

Freedom of Information Act 2000

71. 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 of that Act.

72. 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 previous 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.

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

Communications Data (CD)

Section 11

74. 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 Telecommunications Operator (TO) or a Postal Operator (PO) without lawful authority. A relevant public authority is an authority listed in Schedule 4 of IPA 2016. The Act now provides examples of what will be included within the meaning of "lawful authority" under section 11.

75. 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 posed significant challenges to public authorities. This Act therefore set 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.

76. 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.

77. 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 measures in this Act aim to remove the risk of them (and other public sector organisations) 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 Act uses a similar definition to that used in the Procurement Act 2023. Not all such organisations will be TOs.

78. The sharing of CD between public authorities will still require compliance with data protection legislation and would continue to be subject to sufficient oversight. There is an agreement between the IPC and the Information Commissioner in relation to where their responsibilities may overlap.

Section 12

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

80. 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 Postal Operators or "postal powers", or as secondary data from interception and EI warrants.

81. As a result, 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, were unable to perform their statutory functions as effectively as they needed to.

82. For those regulatory or supervisory bodies with IPA 2016 powers, this issue remained extant where there was 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 fine.

83. For regulatory or supervisory bodies without IPA 2016 powers this issue remained due to the fact that some of the data for which disclosure was required by those bodies to carry out their statutory functions effectively now fell within the definition of CD and required an IPA 2016 authorisation to acquire it. The changes to legislation in this Act aim to make it easier for these organisations to carry out their lawful functions.

84. Section 12 of the IPA 2016 recognised the need for bodies with "regulatory functions" to acquire CD. This was previously limited to organisations such as the Office of Communications (Ofcom) and the Information Commissioner's Office for their regulation of TOs. This amendment to the IPA 2016 expands the definition of 'Regulatory Powers' to include those with wider, statutory 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, explicitly, where the CD is not being acquired in the course of a criminal investigation.

85. 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 or via some other judicial authorisation route.

86. 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.

87. The bodies who may be permitted to use their non-IPA 2016 powers for the purposes of regulation or supervision are the public authorities listed within Schedule 4 of the IPA 2016 together with those currently listed and who may be later added, by regulations, to new Schedule 2A.

Section 261

88. 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.

89. Insufficient clarity existed over whether subscriber and account data was CD or content, for example in the context of registration details provided in online forms when an individual was setting up an account or taking up a service over the internet.

90. Due to the complex nature of whether subscriber and account data amounted to CD or content, this Act amends 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.

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

Interception

92. 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.

93. 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 Act therefore amends 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.

94. 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 enables 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

95. 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.

96. Section 195 of Chapter 3 provided 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.

97. This Act introduces prior independent authorisation to Section 195, the effect of which is 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 also brings 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 and signed into law on 15th April 2024.

Legal background

Bulk Personal Datasets (BPDs)

98. The existing Part 7 regime in the IPA 2016 required 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 doing so. 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.

99. In order to be compatible with the ECHR, the statutory regime provides for adequate and effective safeguards against abuse. In the context of pre-IPA 2016 bulk interception, the Grand Chamber of the European Court of Human Rights 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 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."

[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 lawful 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

100. 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/

101. The changes made in this Act introduce a new regime, alongside the current Part 7 which is 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 in the Act sets 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 regime includes 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 is also *ex-post facto* oversight by the IPC, and the redress mechanism of the Investigatory Powers Tribunal.

102. The Act also makes minor changes to Part 7, extending the duration of BPD warrants from six months to twelve months. The changes also provide that certain functions that hitherto had to be performed by the head of the intelligence service – an agency head – can 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)

103. 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 with additional safeguards and formal oversight. See above policy background for further detail.

Changes to the Notices Regime

104. Notices may be given to relevant operators 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.

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

106. 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.

107. The Secretary of State must then consult the Technical Advisory Board (TAB) and a JC. 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 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.

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

108. 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. Section 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.

109. The measures in this Act 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 (Section 18).

110. Sections 90(1) and 257(1) of the IPA 2016 include regulation making powers in relation to a review of a notice. The Investigatory Powers (Review of Notices and Technical Advisory Board) Regulations 2018 (S.I. 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 pre-existing power does not give the Secretary of State the power to specify in regulations a time limit regarding the overall review process. Section 18 introduces a new regulation making power that will enable the amendment of existing regulations (S.I. 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 provides 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.

111. 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. Section 18 gives 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 made outside these timelines. This ensures the JC has the appropriate power to deal with non-compliance and provides clarity to all parties regarding timelines and expectations.

112. 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 was previously no equivalent enforcement provision for TCNs or NSNs. Provisions in this Act 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.

113. 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 Act imposes 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.

114. 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 Act creates 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 was required to the IPC's main oversight functions. As such, this Act makes an amendment 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)

115. Internet Connection Records are data collected and retained by 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 Investigatory Powers Commissioner's Office (IPCO) (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.

116. 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).

117. The change in the Act concerns this second 'subject identification' aspect of the legislation. The IPA 2016 as drafted cover 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.

118. 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. To that end this Condition is event (s) specific.

119. 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.

120. There were concerns that this requirement to know the specific service and time of access limited utility of the ICR capability and prevented this TO stored and managed data from being used to assist in the detection of some of the most serious offenders and National Security threats.

121. 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.

122. The addition by this Act of new Condition D to the legislation allows 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. All such applications must be both necessary and proportionate before they can be authorised.

123. An example of where a Condition D ICR may be appropriate would 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.

124. 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 discovering subjects of interest displaying those linked behaviours and in respect of whom it would not otherwise have been possible to detect.

125. An example of this would be in high-harm fraud which often involves online behaviour that could be identified by ICRs. ICRs can now be used, for example, to search for devices which are 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 will enable the intelligence services to detect such activity more effectively and to inform law enforcement partners of the identity of the potential fraudsters and of any associated organised crime groups.

126. 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 introduced in this Act with the intention of managing access to this new Condition and mitigating public concerns.

127. 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.

128. The lawful purposes for 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.

129. Under this new condition, 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 the subject of an 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. Data returned as a result of a Condition D application will be subject to the safeguards as set out in the Codes of Practice, including that data may only be held for as long as the relevant public authority is satisfied that it is still necessary for a statutory purpose.

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

Warrantry

Sections 26 and 111

Section 26

131. 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

132. 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

133. 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.

134. 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 Act adds 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

135. 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 Act corrects 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

136. 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.

137. 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 Act changes 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

138. 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.

139. 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 Act 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

140. 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

141. 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).

142. 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)."

143. 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 Act adds 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)

144. Section 11 of the IPA 2016 created an offence of obtaining CD without lawful authority. There was no definition, in the original Act, of "lawful authority" in respect of CD acquisition. The objective of amending section 11 has been to make clear that certain types of authority or methods of acquiring CD will amount to "lawful authority". This includes applications to request CD in line with Part 3 IPA 2016, or through a judicial authorisation or Court Order as well as those included ina non-exhaustive list detailing circumstances which will amount to lawful authority for the purposes of section 11.

145. The Act 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.

146. 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'.

147. 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.

148. 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).

149. 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.

150. 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.

151. 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."

152. 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

153. 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.

[12] EUR-Lex - 62015CJ0203 - EN - EUR-Lex (europa.eu) - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62015CJ0203

154. 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.

155. The Section 12 provisions had the effect of preventing those regulatory or supervisory organisations from gathering the data they require where their enquiries failed to meet the serious crime threshold, which was the main remaining statutory purpose available to them to access some types of required data.

156. The purpose of the Section 12 reforms in this Act are 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.

157. These reforms do not diminish nor expand upon the existing statutory requirements for the disclosure of 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.

158. Provisions in the associated Codes of Practice will 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.

159. 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 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, when they complete an online application form, for example. A practical 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.

160. The amendment provides 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). These provisions, providing clarification of subscriber or account data as CD, aim to reduce the risk of errors and provide greater legal certainty.

Interception

161. 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.

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

163. 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

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

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

    a. Sections 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 engages the legislative consent motion process in Scotland 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. The LCM was granted 14 March 2024.

    b. Section 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 engages the legislative consent motion process in Scotland because of the functions of JCs in assisting the IPC in the exercise of their oversight functions. The LCM was granted 14 March 2024.

    c. Section 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 engages the legislative consent motion process in Scotland. The LCM was granted 14 March 2024.

    d. Section 28 makes amendments to 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 was not required; this is because Part 2 of the IPA 2016 is specifically mentioned in paragraph 17 of Schedule 2 of the Northern Ireland Act 1998.

    e. Section 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 amendment to section 23 FOIA does not apply to the regime under the Freedom of Information (Scotland Act) 2002, as such, this measure did not require a legislative consent motion.

Commentary on provisions of the Act

Part 1: Bulk Personal Datasets

Low or no reasonable expectation of privacy

Section 1: Requirement for authorisation

166. This section makes a number of amendments to Part 7 of the IPA 2016 in consequence of the new Part 7A of that Act inserted by section 2.

167. 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.

168. 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 BPD may be authorised under Part 7A as well as under Part 7.

169. 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.

170. 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, also accommodates authorisations under the new Part 7A.

171. Subsection (8) amends section 225 (application of Part [7] to BPDs obtained under this Act) so that a direction under subsection (3) of that section can permit a 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.

Section 2: Low or no reasonable expectation of privacy

172. This section 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

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

174. Subsection (1) sets out test which must be applied. The test is whether the nature of the BPD 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.

175. 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).

176. 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

177. 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 a cross-reference to section 200 as amended by this Act and is self-explanatory.

178. 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).

179. 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.

180. Subsections (5) requires that decisions to grant an individual authorisation must be approved by a Judicial Commissioner (JC). This is subject to the exceptions set out in subsection (6): the approval of a JC is not required if the BPD falls within an existing category authorisation granted under section 226BA, or the person granting the authorisation considers there is an urgent need to grant it.

181. Subsection (7) sets out that a person granting an individual authorisation in respect of a BPD that falls within an existing category authorisation may nevertheless, , still seek JC approval if they consider it appropriate to do so..

182. 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 retains under an individual 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 individual authorisation to retain or examine an updated version of a dataset that is already the subject of an authorisation.

New section 226BA of the IPA 2016: Category authorisation

183. 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 (including by reference to the use to which the datasets will be put). The decision to grant the authorisation must be approved by a JC.

184. A category authorisation is different to an individual authorisation. An individual authorisation authorises the retention, or retention and examination, of a BPD to which section 226A applies. A category authorisation effectively disapplies – per section 226A(6)(a) – the requirement for judicial approval where an individual authorisation pertains to a dataset that falls within a category authorisation. That is because a decision will already have been made, and approved by a JC, that any dataset that falls within the description in the category authorisation is a dataset to which section 226A would apply.

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

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

186. 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.

187. 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.

188. 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.

189. 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

190. 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.

191. Subsection (4) explains that subsections (5) to (7) set out what happens if a judicial commissioner refuses to approve the decision to grant an urgent individual authorisation.

192. Subsection (5) provides that 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 revisit the JC's decision under section 226BB(4).

193. 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.

194. 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 it was notified of the decision to refuse to approve the grant of the urgent authorisation. This has the effect of restarting the time limit for the intelligence service to carry out an initial examination of the dataset so that it can decide whether it wishes to continue to retain, or retain and examine, the dataset in whole or in part and can make such consequential arrangements as are necessary (e.g, granting a further individual authorisation under section 226B).

195. Under subsection (8), the lawfulness of things done in reliance on an urgent individual authorisation that a JC subsequently refuses to approve is not affected by the authorisation ceasing to have effect.

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

196. This section sets out that the duration of authorisations under Part 7A, unless renewed or cancelled, is, twelve months for all authorisations other than urgent individual authorisations. Urgent individual authorisations are valid until the end of five working days from the day after the day the authorisation was granted.

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

197. This section sets out the process for the renewal of individual and category authorisations (including urgent individual authorisations) and the conditions that must be met.

198. Subsection (1) provides that the head of an intelligence service (or a person acting on their behalf) may renew a category or individual authorisation at any time during the renewal period provided the renewal conditions are met.

199. Subsection (2) and (3) set out the renewal conditions for an individual authorisation, including a requirement that the renewal of individual authorisations must be approved by a JC unless the dataset is one that falls within a category of datasets authorised by a category authorisation (see section 226BA).

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

201. Subsection (5) defines what is meant by the expression "renewal period":

- For urgent individual authorisations, the renewal period is the "relevant period" (per section 226C) i.e. the fifth working day after the day on which the authorisation was granted.
- For an individual authorisation which was authorised in reliance on a category authorisation that has ceased to have effect because it has been cancelled or 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.

202. 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

203. 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 (subsection (1)) and must do so where certain cancellation conditions are met (subsection (2)).

204. 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 datasets authorised under Part 7A or for protecting them from unauthorised disclosure.

205. 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

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

207. 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.

208. 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

209. This section provides for circumstances in which 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.

210. 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. This is also the "renewal period" for the purposes of renewing such an individual authorisation, as opposed to the 30 days that would otherwise apply (see section 226CA(5)(b)).

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

211. This section provides for circumstances in which 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) forms the belief that section 226A either does not apply *or* no longer applies to part of the dataset This is to be distinguished from circumstances in which it is considered that section 226A no longer applies to the dataset as a whole. In that case a cancellation condition is met and the authorisation must be cancelled (see section 226CB).

212. Subsection (2) provides that the head of the intelligence service must, as far as reasonably practicable, ensure that any activity that is being carried in relation to that part of the dataset stops as soon as possible.

213. Subsection (3) provides that section 220 (Part 7 initial examinations: time limits) applies in relation to the relevant part of the dataset as if that part of the dataset was obtained when the necessary belief referred to in subsection (1) was formed. This has the effect of restarting the time limit for the intelligence service to carry out an initial examination of the relevant part of the dataset so that it can decide whether it wishes to continue to retain, or retain and examine that part of a the dataset as a separate dataset and can make such consequential arrangements as are necessary (e.g, granting a further individual authorisation under section 226B).

214. 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 at the point in time at which the relevant belief was formed. Subsection (5) sets out that the lawfulness of certain activity carried out before the relevant part of the authorisation cased to have effect is not affected by this section.

New section 226DA of the IPA 2016: Annual report

215. This section provides that the head of each intelligence service must provide an annual report to the Secretary of State. This is a report about the BPDs that were authorised to be retained, or retained and examined, under Part 7A by the intelligence service.

216. 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. Reports must be provided to the Secretary of State as soon as reasonably practicable after the end of the relevant reporting period.

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

217. This section provides that the Secretary of State must provide an annual report to the Intelligence and Security Committee of Parliament. This is a report setting out information about category authorisations and renewals of category authorisations granted during the preceding twelve months.

218. 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. Reports must be provided to the Secretary of State as soon as reasonably practicable after the end of the relevant reporting period.

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

219. This section state that within Part 7A, use of the terms ‘category authorisation’ and ‘individual authorisation’ has the same meaning as those provided under section 226B(1) and section 226BA(1) respectively. Subsection (2) provides a cross-reference to and section 199 (bulk personal datasets: interpretation), section 263 (general definitions) and section 265 (index of defined expressions) to assist with interpretation. 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

Section 3: Duration of bulk personal dataset warrants

220. This section amends section 213 in Part 7 of the Act so that BPD warrants will have a duration of twelve months rather than six. The change applies to both class BPD warrants and specific BPD warrants, and applies to all warrants that are issued or renewed on or after the date that the section comes into force.

Section 4: Agency head functions

221. This section makes amendments to a number of provisions in Part 7 of the IPA 2016 in which a function is conferred on the head of an intelligence service. The amendment aims to make clear 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 IPA 2016 (e.g., making an application for a warrant).

Third party bulk personal datasets

Section 5: Third party bulk personal datasets

222. Section 5 insets a new Part, Part 7B, into the IPA 2016.

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

223. This section sets out the circumstances in which an intelligence service examines a third party bulk personal dataset for the purposes of Part 7B and therefore requires a warrant. Subsection (1) sets out the circumstances which are that:

- the intelligence service has "relevant access" to a set of information 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;
- after an initial inspection, the intelligence service examines the set electronically *in situ* for the purpose of the exercise of its functions.

224. Subsection (2) defines when an intelligence service has "relevant access" to a set of information. Access must be made available as a result of arrangements made directly between the intelligence service and the third party, the type and extent of the access must be such that it is not generally available (whether on a commercial basis or otherwise), and the access must be electronic.

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

225. 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 authorised.

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

226. 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 (see section 226I(5)).

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

227. This section permits the head of an intelligence service or a person acting on their behalf to apply to the Secretary of State for a 3PD warrant.

228. Subsection (2) provides that 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 retain a set examined under Part 7B.

229. Subsection (3) provides that where the person making the application knows that:

- the dataset consists of protected data or health records,
- a substantial proportion of the dataset 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 (see subsection (6)).

230. Subsection (4) sets out the test that the Secretary of State must apply when deciding whether or not to issue a warrant. The Secretary of State may issue the warrant if he or she considers that the warrant is necessary for specified purposes, the conduct to be authorised is proportionate to what is sought to be achieved by it, there are satisfactory arrangements in place for the examination of the set and, unless it is urgent, the decision to issue the warrant has been approved by a JC. Subsection (5) provides that the fact that a 3PD warrant would authorise the examination of bulk personal datasets relating to activities in the British Islands of a trade union is not in itself sufficient to establish that it is necessary. Subsections (7) and (8) are concerned with the definition of health records for the purposes of section 226G.

231. 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

232. 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.

233. 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

234. 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.

235. Subsection (2) provides that the Secretary of State must inform the JC that the warrant has been issued. The JC must then, before the end of the third working day after the day on which the warrant was issued – the "relevant period" –decide whether to approve the decision to issue the warrant and notify the Secretary of State of the Judicial Commissioner's decision.

236. Subsection (4) explains that subsections (5) to (7) set out what happens if a judicial commissioner refuses to approve the decision to grant an urgent individual authorisation.

237. Subsection (5) provides that if a Judicial Commissioner refuses to approve the decision to issue a 3PD warrant, the warrant ceases to have effect (unless already cancelled), and may not be renewed. The Secretary of State may not asked the Investigatory Powers Commissioner to revisit the JC's decision under section 226GA(4).

238. Subsection (6) provides that the head of the intelligence to which the warrant was issued, must ensure, as far as reasonably practicable, that any processes being done in reliance on the warrant stops as soon as possible.

239. Under subsection (7), the lawfulness of things done in reliance on an urgent individual authorisation that a JC subsequently refuses to approve is not affected by the authorisation ceasing to have effect.

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

240. This section specifies the Secretary of State must make the decision to issue a 3PD warrant personally. The Secretary of State must also sign the 3PD warrant unless it is not reasonably practicable to do so.

241. If the Secretary of State cannot sign the warrant, it may be signed by a senior official instead (i.e., a member of the Senior Civil Service or a member of the Senior Management Structure of His Majesty's Diplomatic Service – see section 226IE). In these cases, the warrant must contain a statement that (a) it is not reasonably practicable for the warrant to be signed by the Secretary of State, and (b) the Secretary of State has personally and expressly authorised the issue of the warrant.

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

242. 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 (or datasets) to which the warrant relates.

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

243. This section sets out that the duration of 3PD warrants, unless renewed or cancelled, is, twelve months. Urgent 3PD warrants are valid until the end of five working days from the day after the day the warrant was issued.

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

244. This section sets out the process for the renewal of 3PD warrants (including urgent 3PD warrants), which may be renewed by an instrument issued by the Secretary of State, at any time during the "renewal period", if the renewal conditions are met.

245. Subsection (2) sets out the renewal conditions: the Secretary of State considers that the warrant continues to be necessary and proportionate, and the decision to renew has been approved by a JC. In making their decision, the JC must take the same approach as is taken when a warrant is first issued (see subsection (5) and section 226GA (approval of warrants by Judicial Commissioners)).

246. Subsection (3) provides that the "renewal period" means (a) in the case of an urgent warrant, the relevant period, (b) any other case, the period of 30 days which ends with the day the warrant would otherwise cease to have effect. The decision to renew must be taken personally by the Secretary of State and signed by the Secretary of State.

247. Subsection (4) provides that, as with the decision to issue a warrant, the decision to renew a warrant must be taken by the Secretary of State personally and must also be signed by the Secretary of State (see section 226GC (decision to issue warrants to be taken personally by Secretary of State) in respect of the requirements that apply to the issuing of a warrant).

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

248. This section states the Secretary of State or senior official acting on their behalf may cancel a warrant at any time and must cancel the warrant should the cancellation conditions be met. The cancellation 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

249. This section is concerned with what happens when a 3PD warrant ceases to have effect either because it has expired without being renewed or because it has been cancelled (see section 226HB (cancellation of warrants). Subsection (2) provides that the head of the intelligence service to whom the warrant was addressed must, as far as reasonably practicable, ensure that any activity that is being 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

250. This section makes provision for an initial inspection period before a 3PD warrant is required. The initial inspection process is an important preliminary step which enables the intelligence service to inspect the contents of the dataset in order to determine whether access to the dataset would engage Part 7A and to consider whether to make an application for a 3PD warrant in respect of it. This section enables that process to be carried out in the absence of a 3PD warrant, making it a limited exception to the requirement in section 226F(requirement for authorisation by warrant). Subsection (1) sets out the circumstances in which it can be said that an initial inspection is being carried out and subsection (2) sets out the purposes for which the initial inspection may be carried out.

251. Subsection (3) and (4) make clear that the initial inspection process will lead to a decision by the intelligence service as to whether to apply for an 3PD warrant. Subsection (5) provides that the intelligence service may examine the dataset after the end of the initial examination process for the specific purpose of making an application for a warrant.

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

252. This section is concerned with safeguards. It places an obligation on the Secretary of State to ensure that arrangements are in force to secure that any examination of data contained in a 3PD is necessary and proportionate in all the circumstances. The arrangements must take account of the information that is reasonably available to the intelligence service in relation to the data.

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

253. This section is concerned with safeguards for "protected data" that is legally privileged. It makes provision for the approval of "relevant criteria" to be used for the examination of data. The expression "protected data" is defined in section 203 in Part 7 of the IPA 2016: in broad terms, protected data is likely to be content as opposed to metadata.

254. Subsections (2) to (8) set out a regime for the approval of the use of criteria where either a purpose of using the criteria is to identify items subject to legal privilege, or the use of the criteria is likely to do so.

255. Where the criteria are referrable to an individual known to be in the British Islands, the approval of the Secretary of State is required and, per subsection (4), this approval must also be approved by a JC. When deciding whether to give approval the JC must apply the same principles as a court on application for judicial review and consider with a degree of care to ensure the JC complies with duties imposed by section 2.

256. In all other cases, the approval may be given internally by a senior official. The senior official's approval does not need to be approved by a JC.

257. Where the purpose of the examination is to identify items subject to legal privilege (as opposed to only being likely to do so), the decision maker is required to balance the need to use the relevant criteria against the public interest in the confidentiality of items subject to legal privilege. Use of the criteria may only be authorised if there are exceptional and compelling circumstances that make it necessary to do so.

258. The "exceptional and compelling" test is further explained in subsection (7) which provides that there cannot be exceptional and compelling circumstances unless (a) public interest in obtaining the information outweighs public interest in confidentiality of items subject to legal privilege, (b) there are no other means to reasonably obtain the data, and (c) obtaining the information is necessary in the interests of national security or for the purpose of preventing death or significant injury.

259. Subsections (9) to (13) set out a regime for the approval of the use of criteria where a purpose of the using the criteria is to examine data (or underlying material i.e. other data from which that data was derived – see subsection (13)) that would be legally privileged but where the intelligence services considers it likely that it was created or held with the intention of furthering a criminal purpose (often called the iniquity exception to legal privilege).

260. Where the criteria are referrable to an individual known to be in the British Islands, the approval of the Secretary of State is required – this approval does not need to be approved by a JC (see subsection (10)).

261. In all other cases, the approval may be given internally by a senior official. The senior official's approval does not need to be approved by a JC (see subsection (11)).

262. Approval may be given only if the decision maker considers that the targeted data or the underlying material is likely to have been created or to be held with the intention of furthering a criminal purpose.

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

263. This section explains the process that must be followed if an intelligence service examines legally privileged material in a 3PD and retains it (otherwise than under a warrant issued under Part 7 of the IPA 2016).

264. The intelligence service 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.

265. If the IPC considers that the (a) the public interest retaining the item outweighs the public interest in confidentiality of items subject to legal privilege, and (b) retaining the item is necessary in the interests of national security or for the purpose of preventing death or significant injury (see subsection (5)), then the intelligence service may continue to retain the item, subject to such conditions as the IPC may impose (see subsection (4)).

266. If the IPC does not agree that the item may be retained, then he or she must direct either that the item be destroyed or that it be subject to one or more conditions as to its use or retention. In deciding whether to require destruction or impose conditions, the IPC may require an affected party (either the Secretary of State or the intelligence service the 3PD warrant was addressed) to make representation and must have regard to any such representations made.

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

267. 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. An offence is committed if a person examines a 3PD with reliance on a 3PD warrant, the person knows the examination is a breach of the requirement specified in subsection (2) and the person deliberately examines that data in breach of that requirement.

268. This section also sets out the penalties for a person found guilty of this offence, and makes clear that proceedings in relation to an offence under this section may only be instituted by or with the consent of the Director of Public Prosecutions in England and Wales or the Director of Public Prosecutions for Northern Ireland in Northern Ireland.

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

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

270. Personal and protected data has the same meaning as in Part 7. Senior official means a member of the Senior Civil Service or a member of the Senior Management Structure of His Majesty's Diplomatic Service; and third party BPD warrant is defined in section 226F.

Minor and consequential amendments

Section 6: Minor and consequential amendments

271. 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

Section 7: Deputy Investigatory Powers Commissioner

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

273. 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).

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

275. Section 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.

276. Section 7(4) inserts 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)).

277. Section 7(5) inserts the term "Deputy Investigatory Powers Commissioner" into the index of defined expressions.

Section 8: Delegation of functions

278. This section 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).

279. Section 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.

280. 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.

281. Subsection (8C) of section 227 clarifies that the IPC's functions, as listed in subsection (6A) [appointment of DIPCs] may not be delegated.

282. 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.

283. 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.

Section 9: Temporary Judicial Commissioners

284. This section 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

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

286. 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.

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

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

289. 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.

290. 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, per section 228A(4).

291. 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).

Section 10: Main functions of the Investigatory Powers Commissioner

292. This section amends the IPC's main oversight functions.

293. Section 10(2)(a) removes the IPC's functions relating to the oversight of prevention or restriction of use of communication devices by prisoners etc., as telecommunications restriction orders are already subject to judicial approval in the county court.

294. Section 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 section inserts a provision into the IPA 2016 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.

295. Section 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) of the IPA 2016, so far as engaging in intelligence activities.

296. Section 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 of the IPA 2016, 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.

Section 11: Personal data breaches

297. Section 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 IPA 2016, if the IPC determines it is in the public interest to make such a notification.

298. 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.

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

300. 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.

301. 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.

302. 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.

303. 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.

304. 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.

305. 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.

306. 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.

307. 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.

308. 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 (S.I. 2003/2426) - "PECR"), "personal data breach" and "relevant restriction".

309. Section 11(2) amends RIPA 2000 to clarify that the Investigatory Powers Tribunal is the appropriate forum for to determine complaints relevant personal data breaches specified in section 235A of the Act.

310. Section 11(3) amends RIPA 2000 in consequence of the amendments made at section 11(2) regarding the Tribunal's jurisdiction.

311. Section 11(4) amends section 68(8) RIPA 2000 to add the Information Commissioner to the list of relevant Commissioners who may be required to provide assistance to the Tribunal.

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

313. Section 11(6) repeals paragraph 14 of Schedule 10 IPA 2016, in consequence of the amendment at Section 11(5).

Part 3: Communications Data etc

Communications data

Section 12: Offence of unlawfully obtaining communications data

314. Section 12 amends section 11 of the IPA 2016. Subsection (2) amends section 11(1) of the IPA 2016 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.

315. Subsection (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.

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

317. This section 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.

Section 13: Meaning of "communications data": subscriber details

318. This section 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 will have the practical effect of clarifying that this data is communications data rather than content.

Section 14: Powers to obtain communications data

319. This section 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 without:

    i. the consent of the operator,

    ii. a court order or other judicial authorisation or warrant, and

    iii. being *a regulatory power,*

    no longer enables the public authority to secure such discloser.

320. Section 12(6) of the IPA 2016 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.

321. Section 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 and to certain specified public authorities. 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.

322. Section 14(5A) and (5B) provide a definition for 'specified public authority' as one listed in either new Schedule 2A or Schedule 4, and states that either the Secretary of State or the Treasury may, by regulations, modify new Schedule 2A.

323. Section 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,

324. 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.

325. Section 14(7) introduces a Schedule which reverses certain of the changes originally 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. The changes made by Schedule 2 to the IPA 2016 which relate to powers that can only be used for criminal investigations are unchanged by this Act.

326. 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 regulatory or supervisory statutory function and not for a criminal investigation or prosecution.

Internet connection records

Section 15: Internet connection records

327. The new section 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.

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

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

330. Section 15(4) inserts new subsections 5A, 5B and 5C into the IPA 2016 which define the new condition D and provides interpretation of the term 'specified.'

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

332. 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.

333. 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.

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

335. 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.

336. For the NCA this is;

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

337. 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.

338. 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

339. And in urgent cases only;

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

340. 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.

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

Part 4: Notices

Retention notices

Section 16: Powers to require retention of certain data

342. Section 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.

343. Subsection (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.

344. Section 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 of the IPA 2016.

Section 17: Extra-territorial enforcement of retention notices etc

345. This section amends section 95(5) and 97 of the IPA 2016 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

Section 18: Review of notices by the Secretary of State

346. 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.

347. Section 90(4)(a) of the IPA 2016 (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.

348. Section 90(4A) of the IPA 2016 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.

349. Section 90(5) of the IPA 2016 (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.

350. Section 90(5A) of the IPA 2016 (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.

351. Section 90(9A) and (9B) of the IPA 2016 (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.

352. The amendment to Section 90(10) of the IPA 2016 (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.

353. Section 90(11A) of the IPA 2016 (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.

354. Section 90(14)-(16) of the IPA 2016 (data retention notices) makes provision for the Secretary of State to include in regulations made pursuant to these sections, 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.

355. The amendment to 267(3) of the IPA 2016 applies the affirmative procedure to regulations made under these sections.

356. The amendment to section 95(5) of the IPA 2016 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).

357. The further amendment to section 255(10) of the IPA 2016 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.

Section 19: Meaning of "telecommunications operator" etc

358. As companies increasingly have multiple entities spread across the globe involved in the delivery of their services, this section 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.

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

360. 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.

Section 20: Renewal of notices

361. Section 87(6A) of the IPA 2016 (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

362. 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.

363. 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.

364. 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

Section 21: Notification of proposed changes to telecommunications services etc

365. This section 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

366. 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.

367. 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.

368. 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.

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

370. Subsection (7) requires the Secretary of State to consult the operator before giving them a notice under this section. The provision would require the Secretary of State to discuss, during the consultation with the operator, the specifics of the obligation to be imposed on 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.

371. 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.

372. 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.

373. 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

374. 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

Section 22: Interception and examination of communications: Members of Parliament etc

375. Subsection (1) sets out that the section 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 a relevant legislature (such as an MP). The safeguard in section 26 is sometimes referred to as the "triple lock".

376. 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.

377. Subsection (3) inserts new subsections (2A) - (2F) 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.

378. 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 have the necessary operational awareness to decide whether to give approvals under subsection (2). New subsection (2E) provides for the duration of such a designation under section 26, 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.

Section 23: Equipment interference: Members of Parliament etc

379. Subsection (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.

380. Subsection (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. Subsection (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.

381. Subsection (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.

382. 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 have the necessary operational awareness to decide whether to give approvals under subsection (2) 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

Section 24: Issue of equipment interference warrants

383. Subsection 1 describes the location within the Act that the relevant changes will be made i.e. Part 1 of the table in Schedule 6.

384. 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.

385. 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.

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

Section 25: Modification of equipment interference warrants

387. This section 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) of the IPA 2016.

Section 26: Issue of targeted examination warrants to intelligence services

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

Section 27: Bulk equipment interference: safeguards for confidential journalistic material etc

389. This section improves journalistic safeguards within the IPA 2016's bulk equipment interference regime (Section 195).

390. It will replace the existing Section 195 IPA 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.

391. The section provides a new urgency process (Section 195A) for dealing with requests which need to be approved out of hours, for authorisations to use criteria 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.

392. The section also provides a consequential amendment to section 229(8) of the IPA 2016 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

Section 28: Exclusion of matters from legal proceedings etc: exceptions

393. This section creates exceptions to the prohibition on disclosing intercept materials to be used as evidence under section 56 of the IPA. 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 section also provides the limits on the disclosure of intercept material for this purpose.

394. 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

Section 29: Freedom of information: bodies dealing with security matters

395. This section amends section 23 of the Freedom of Information Act 2000 to add JCs to the list of bodies dealing with security matters, to ensure that the exemption at section 23 may be applied by public authorities to protect sensitive information from disclosure in response to FOIA requests.

Part 6: General

General

Section 30: Power to make consequential provision

396. This section allows for the Secretary of State to amend or repeal a provision of the Act. 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.

Section 31: Extent

397. This section 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.

Section 32: Commencement

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

399. Regulations under this section 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.

Section 33: Short title

400. The Act is to be referred to as the Investigatory Powers (Amendment) Act 2024.

Schedule: Disclosure powers

401. Section 14 of this Act amends section 12 of the IPA 2016 and the powers to obtain communications data reverses the effect of certain repeals of disclosure powers and makes consequential provision to schedule 2 of the IPA 2016.

Part 1: Restoration of disclosure powers

Health and Safety at Work etc Act 1974

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

Criminal Justice Act 1987

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

Consumer Protection Act 1987

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

Environment Protection Act 1990

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

Financial Services and Markets Act 2000

406. 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

407. 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

408. Section 32 makes provision regarding when measures in this Act will come into force.

Environment Act 2021: Section 20

409. The Rt Hon James Cleverly MP, Secretary of State for the Home Department, is of the view that the Act 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.

European Union (Withdrawal) Act 2018: Section 13C

410. The Rt Hon James Cleverley MP, Secretary of State for the Home Department, is of the view that the Act does not contain provision which, if enacted, would affect trade between Northern Ireland and the rest of the United Kingdom. Accordingly, no statement under section 13C of the European Union (Withdrawal) Act 2018 has been made.

Related documents

411. The following documents are relevant to the Act 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	Extends to E & W and applies to England?	Extends to E & W and applies to Wales?	Extends and applies to Scotland?	Extends and applies to Northern Ireland?
Part 1				
Section 1	Yes	Yes	Yes	Yes
Section 2	Yes	Yes	Yes	Yes
Section 3	Yes	Yes	Yes	Yes
Section 4	Yes	Yes	Yes	Yes
Section 5	Yes	Yes	Yes	Yes
Section 6	Yes	Yes	Yes	Yes
Part 2				
Section 7	Yes	Yes	Yes	Yes
Section 8	Yes	Yes	Yes	Yes
Section 9	Yes	Yes	Yes	Yes
Section 10	Yes	Yes	Yes	Yes
Part 3				
Section 11	Yes	Yes	Yes	Yes
Section 12	Yes	Yes	Yes	Yes
Section 13	Yes	Yes	Yes	Yes
Section 14	Yes	Yes	Yes	Yes
Section 15	Yes	Yes	Yes	Yes
Part 4				
Section 16	Yes	Yes	Yes	Yes
Section 17	Yes	Yes	Yes	Yes
Section 18	Yes	Yes	Yes	Yes
Section 19	Yes	Yes	Yes	Yes
Section 20	Yes	Yes	Yes	Yes
Section 21	Yes	Yes	Yes	Yes
Part 5				
Section 22	Yes	Yes	Yes	Yes
Section 23	Yes	Yes	Yes	Yes
Section 24	Yes	Yes	Yes	Yes

Provision	Extends to E & W and applies to England?	Extends to E & W and applies to Wales?	Extends and applies to Scotland?	Extends and applies to Northern Ireland?
Section 25	Yes	Yes	Yes	Yes
Section 26	Yes	Yes	Yes	Yes
Section 27	Yes	Yes	Yes	Yes
Section 28	Yes	Yes	Yes	Yes
Section 29	Yes	Yes	No	Yes
Part 6				
Section 30	Yes	Yes	Yes	Yes
Section 31	Yes	Yes	Yes	Yes
Section 32	Yes	Yes	Yes	Yes
Section 33	Yes	Yes	Yes	Yes

Annex B - Hansard References

412. The following table sets out the dates and Hansard references for each stage of the Act's passage through Parliament.

Stage	Date	Hansard Reference
House of Lords		
Introduction	08 November 2023	Vol. 834 Col. 21
Second Reading	20 November 2023	Vol. 834 Col. 620
Committee of the Whole House	11 December 2023 13 December 2023	Vol. 834 Col. 1724 Vol. 834 Col. 1898
Report	23 January 2024	Vol. 835 Col. 681
Third Reading	30 January 2024	Vol. 835 Col. 1116
House of Commons		
Introduction	31 January 2024	Votes and Proceedings, No.42
Second Reading	19 February 2024	Vol. 745 Col. 520
Public Bill Committee	07 March 2024	Col. 1 Col. 27
Report and Third Reading	25 March 2024	Vol. 747 Col. 1302
Lords Consideration of Lords Amendments	23 April 2024	Vol. 837 Col. 1377
Royal Assent	25 April 2024	House of Commons Vol. 748 Col. 1160 House of Lords Vol. 837 Col. 1579

Annex C - Progress of Bill Table

413. This Annex shows how each section and Schedule of the Act was numbered during the passage of the Bill through Parliament.

Section of the Act	Bill as Introduced in the Lords	Bill as amended in Committee in the Lords	Bill as amended on Report in the Lords	Bill as introduced in the Commons	Bill as amended in Committee in the Commons
Section 1	Clause 1	Clause 1	Clause 1	Clause 1	Clause 1
Section 2	Clause 2	Clause 2	Clause 2	Clause 2	Clause 2
Section 3	Clause 3	Clause 3	Clause 3	Clause 3	Clause 3
Section 4	Clause 4	Clause 4	Clause 4	Clause 4	Clause 4
Section 5	Clause 5	Clause 5	Clause 5	Clause 5	Clause 5
Section 6	Clause 6	Clause 6	Clause 6	Clause 6	Clause 6
Section 7	Clause 7	Clause 7	Clause 7	Clause 7	Clause 7
Section 8	Clause 8	Clause 8	Clause 8	Clause 8	Clause 8
Section 9	Clause 9	Clause 9	Clause 9	Clause 9	Clause 9
Section 10	Clause 10	Clause 10	Clause 10	Clause 10	Clause 10
Section 11			Clause 11	Clause 11	Clause 11
Section 12	Clause 11	Clause 11	Clause 12	Clause 12	Clause 12
Section 13	Clause 12	Clause 12	Clause 13	Clause 13	Clause 13
Section 14	Clause 13	Clause 13	Clause 14	Clause 14	Clause 14
Section 15	Clause 14	Clause 14	Clause 15	Clause 15	Clause 15
Section 16	Clause 15	Clause 15	Clause 16	Clause 16	Clause 16
Section 17	Clause 16	Clause 16	Clause 17	Clause 17	Clause 17
Section 18	Clause 17	Clause 17	Clause 18	Clause 18	Clause 18
Section 19	Clause 18	Clause 18	Clause 19	Clause 19	Clause 19
Section 20	Clause 19	Clause 19	Clause 20	Clause 20	Clause 20
Section 21	Clause 20	Clause 20	Clause 21	Clause 21	Clause 21
Section 22	Clause 21	Clause 21	Clause 22	Clause 22	Clause 22
Section 23	Clause 22	Clause 22	Clause 23	Clause 23	Clause 23
Section 24	Clause 23	Clause 23	Clause 24	Clause 24	Clause 24
Section 25	Clause 24	Clause 24	Clause 25	Clause 25	Clause 25
Section 26	Clause 25	Clause 25	Clause 26	Clause 26	Clause 26
Section 27			Clause 27	Clause 27	Clause 27
Section 28	Clause 26	Clause 26	Clause 28	Clause 28	Clause 28
Section 29	Clause 27	Clause 27	Clause 29	Clause 29	Clause 29
Section 30	Clause 28	Clause 28	Clause 30	Clause 30	Clause 30
Section 31	Clause 29	Clause 29	Clause 31	Clause 31	Clause 31

Section of the Act	Bill as Introduced in the Lords	Bill as amended in Committee in the Lords	Bill as amended on Report in the Lords	Bill as introduced in the Commons	Bill as amended in Committee in the Commons
Section 32	Clause 30	Clause 30	Clause 32	Clause 32	Clause 32
Section 33	Clause 31	Clause 31	Clause 33	Clause 33	Clause 33
Schedule	Schedule	Schedule	Schedule	Schedule	Schedule

Printed and published in the UK by The Stationery Office Limited under the authority and superintendence of Jeff James, Controller of His Majesty's Stationery Office and King's Printer of Acts of Parliament.