LIBRARY BRIEFING

HOUSE OF LORDS

HL Bill 3 of 2023–24

Investigatory Powers (Amendment) Bill [HL]

Author: Russell Taylor
Date published: 15 November 2023

The Investigatory Powers (Amendment) Bill would make changes to the Investigatory Powers Act 2016. The 2016 act provides a framework for the use of investigatory powers by the security and intelligence agencies, law enforcement and other public authorities. This includes the power to obtain and retain communications. It also created the post of investigatory powers commissioner and includes a number of safeguards for the use of such investigatory powers, including a two-stage procedure for obtaining authorisations.

Following reviews of the 2016 act, the government stated that the legislation needed updating in light of international issues and rapid technological change. It said that these issues were affecting the ability of agencies to protect the public against serious crime and terrorism. The bill proposes changes including:

- creating a new condition for the use of internet connection records to aid 'target detection'
- introducing an alternative, less stringent regulatory regime for the retention and examination of bulk personal datasets where individuals have little or no expectation of privacy (such as publicly available online telephone directories)
- a new notification requirement which can be issued to selected telecommunications operators requiring them to inform the government of proposed changes to their products or services that could negatively impact the current ability of agencies to lawfully access data

Concerns have been raised by campaigners and tech companies about the possible impact of the changes proposed. In particular, some major tech companies (such as Meta and Apple) have warned that the new notification requirement may force them to withdraw services from the UK if it unduly impacts their ability to innovate and introduce new security features. Civil liberties groups have also raised general concerns about the breadth of the investigatory powers regime and the impact on privacy.

Table of Contents

1. Background to the legislation 3

1.1 Investigatory Powers Act 2016 3

1.2 Criticism and legal challenges by privacy rights groups 4

2. Reviewing the investigatory powers legislation 6

2.1 Home Office review of the 2016 act 6

2.2 Lord Anderson Review 7

3. Details of the Investigatory Powers (Amendment) Bill 2023–24 8

3.1 Introduction of the bill 8

3.2 Provisions in the bill 9

4. Commentary on the bill's proposals 21

4.1 Consultation on the new notices regime 21

4.2 Other reaction to the bill 23

1. Background to the legislation

1.1 Investigatory Powers Act 2016

The Investigatory Powers Act 2016 (IPA 2016) provides a framework for the use of investigatory powers by the security and intelligence agencies, law enforcement and other public authorities. This includes the power to obtain and retain communications. For example, in brief, the act:[1]

- set out powers available to the state to obtain communications and communications data
- provided for statutory safeguards, clarifies which powers can be used by different authorities, and sets out how the use of powers must be authorised (for example, it may include authorisation by judicial commissioners (JCs))
- created a new investigatory powers commissioner (IPC) to oversee the use of these powers
- provided a new power for the secretary of state to require, by notice, communications services providers to retain internet connection records (ICRs)

The act includes powers for the security and intelligence agencies to acquire communications data in bulk, including the retention of bulk personal datasets (BPDs), for example electoral roll and travel data.[2] The act also requires the Home Office to undertake a review of the legislation (see section 2.1 below).

Many of the powers in the act were pre-existing and already being used by intelligence and law enforcement agencies. The government stated that one of the intentions behind introducing the 2016 act was to bring together and build upon statutory powers already available to make the regime clearer and more understandable.[3] The government explained that the act was also required to replace emergency legislation passed in July 2014 (the Data Retention and Investigatory Powers Act 2014), which was subject to a sunset clause.[4]

[1] Explanatory notes to the Investigatory Powers Act 2016, p 9.

[2] Security Service: MI5, 'Bulk personal datasets', accessed 15 November 2023. MI5 explained that, although the majority of individuals on these datasets will be of no interest to MI5, using the datasets can allow them to gain further information on individuals or groups who may come up in an investigation.

[3] Home Office, 'Report on the operation of the Investigatory Powers Act 2016', 9 February 2023, p 3.

[4] The Data Retention and Investigatory Powers Act 2014 itself had been required following a decision by the

Alongside consolidating existing powers, the government also stressed that the IPA 2016:[5]

- Overhauled how powers were authorised and overseen. For example, it did this by creating the IPC and requiring the approval of JCs before authorising the use of more intrusive powers (the "double-lock" system).
- Ensured the powers were "fit for the digital age". On this, GCHQ flagged the importance of the new powers to retain ICRs.[6]

Further information on the operation of the legislation and its provisions can be found on the Home Office webpage, 'Investigatory Powers Act', last updated on 18 October 2023. Information on the parliamentary scrutiny of the legislation,[7] which included consideration of draft bills, committee reports and debates across two parliamentary sessions, can be found in the following briefings:

- House of Lords Library, 'Investigatory Powers Bill: Briefing for Lords stages', 21 June 2016
- House of Commons Library, 'Investigatory Powers Bill', 11 March 2016; and 'Investigatory Powers Bill: Lords amendments', 28 October 2016

1.2 Criticism and legal challenges by privacy rights groups

The regime introduced by the IPA 2016 has attracted criticism from civil liberties groups, who have dubbed the act the "Snooper's Charter". For example, Liberty has raised concerns about the impact on privacy and the risks posed by the handling of people's data:

> […] the information agencies can get their hands on paints an incredibly detailed picture of who we are, who we talk to, where we go and what we think. It can reveal our health concerns, political views, religious beliefs, relationships and all of our movements—leaving nothing private.
>
> And by storing all the information in 'personal datasets' or hacking our devices and leaving them permanently damaged, they are putting our most sensitive personal data

European Court of Justice which invalidated the Data Retention Directive of 2006.

[5] As above.

[6] GCHQ, 'Investigatory Powers Act', 18 March 2019.

[7] The bill forming the act received royal assent on 29 November 2016.

at risk of attack from others.[8]

Similar concerns were raised by Big Brother Watch, who also argued that safeguards in the legislation were not strong enough and there was "no guarantee that citizens will be told if they have been put under surveillance wrongfully".[9]

Aspects of the investigatory powers regime have also been successfully challenged in the courts. For example, following a successful campaign to the European Court of Human Rights by Big Brother Watch and other groups, the government issued a remedial order in 2023 introducing additional safeguards for the bulk interception of confidential journalistic material.[10] In addition, Liberty and the National Union of Journalists have been challenging the IPA 2016 regime around protections for journalists and the ability to share BPDs with overseas states. Judgment was handed down in the Court of Appeal in August 2023. The court said its "conclusions are first, that the provisions challenged in this appeal are, with one exception, Convention compliant, and secondly, that those provisions do not violate EU law".[11] The Court of Appeal also returned one matter to the divisional court for it to determine, relating to the protection of journalistic material obtained by bulk equipment interference warrant. Further information on these legal proceedings can be found in the following sources:

- Joint Committee on Human Rights, 'Proposal for a Draft Investigatory Powers Act 2016 (Remedial) Order 2023'. 13 June 2023, HL Paper 210 of session 2022–23
- Home Office, 'Home Office response to the 13th report from the Joint Committee on Human Rights', 18 October 2023
- R (on the application of National Council for Civil Liberties) v Secretary of State for the Home Department and others (National Union of Journalists intervening) [2023] EWCA Civ 926; see paras 12 and 213 for a summary of the Court of Appeal's conclusions.

---

[8] Liberty, 'Snooper's Charter', accessed 13 November 2023.

[9] Big Brother Watch, 'Investigatory Powers Bill set to become law', 17 November 2016.

[10] Draft Investigatory Powers Act 2016 (Remedial) Order 2023. This is currently awaiting approval by Parliament; see: UK Parliament, 'Investigatory Powers Act 2016 (Remedial) Order 2023', accessed 13 November 2023.

[11] R (on the application of National Council for Civil Liberties) v Secretary of State for the Home Department and others (National Union of Journalists intervening) [2023] EWCA Civ 926; see paras 12 and 213 for a summary of the Court of Appeal's conclusions

- Liberty, 'Update on Liberty's legal challenge against the Investigatory Powers Act 2016', 4 August 2023

2. Reviewing the investigatory powers legislation

2.1 Home Office review of the 2016 act

Section 260 of the IPA 2016 required the government to publish a report on the operation of the legislation within five years and six months of its royal assent. The Home Office published its review on 9 February 2023.[12]

Explaining its approach to the review, the Home Office said it had considered whether the act remained fit for purpose. It added that, due to recent international issues such as Russia's invasion of Ukraine and rapidly developing technological change, it had "become apparent" that areas of the legislation were no longer working optimally and needed updating to improve security. The review explained:

> [S]ome elements of the oversight regime are now inhibiting the UK intelligence community's ability to work together and with partners otherwise leaving the British people vulnerable to a wide range of evolving threats. This is particularly in light of Russia's invasion of Ukraine and the threat of further conflict elsewhere. The UK intelligence community has emphasised the critical importance of updating the legislation to help catch up technologically with the increasingly sophisticated tools used by terrorists, drug smugglers, and organised criminal gangs.[13]

In its conclusion, the Home Office reasoned that the objectives to consolidate existing powers and to provide enhanced oversight and safeguards for use of powers had largely been achieved.[14] However, regarding the objective that the legislation remained "futureproof", the Home Office said that "rapid technological change and intensifying systemic competition" meant that changes were needed. It also said it was likely the legislation would need to be kept under review in anticipation of the need for substantial reform in the future. It explained this was despite the act being drafted in a "technology-neutral manner".

In particular, the Home Office review highlighted limitations of the BPD regime and the complexity of the communications data definitions. It contained a number of proposals to

[12] Home Office, 'Report on the operation of the Investigatory Powers Act 2016', 9 February 2023.
[13] As above, p 5.
[14] As above, pp 23–4.

strengthen these and other areas of the legislation, which were then considered further during Lord Anderson of Ipswich's (Crossbench) review (see section 2.2 below).

2.2 Lord Anderson Review

In anticipation of the need for legislative changes, in January 2023 the government appointed Lord Anderson of Ipswich to carry out an independent review of the IPA 2016.[15] Lord Anderson had previously held the post of independent reviewer of terrorism legislation for six years.

The Home Office said the review should assess the case for legislative change, with a focus on the BPD regime, criteria for obtaining ICRs, the suitability of various definitions within the act, and the flexibility of warrantry processes and the oversight regime. It said that the review would involve consultation with law enforcement, intelligence agencies, and other public and external bodies.

Lord Anderson's review was published in June 2023 and considered some of the reform proposals raised by the Home Office. For example, it addressed Home Office proposals to:[16]

- Amend part 7 of the act (relating to warrants for BPDs) to create a new, "light-touch" regulatory regime for the retention and examination by UK intelligence agencies of BPDs of which individuals have a "low or no expectation of privacy". Lord Anderson's review endorsed this if the datasets (or class of datasets) were agreed upon by an independent JC.
- Amend one of the three conditions in s 62 of the act (setting out the restrictions for obtaining ICRs) so as to facilitate the use of ICRs for "target discovery" (for example, tracking down users of child sexual abuse websites). Lord Anderson agreed with this principle, but believed it would be "better achieved" by creating a fourth condition only available to intelligence agencies and only for "national security-related and serious crime purposes".
- Amend s 87 of the act (on powers to require retention of certain data) so that a mechanism continues to exist whereby UK telecommunications operators (TOs) can be required, upon agreement by the government and a JC, to retain the communications data of 'inbound roamers' with foreign SIM cards. Lord Anderson's report explained that this issue relates to methods of

[15] Home Office, 'Lord Anderson appointed to review the Investigatory Powers Act', updated 13 February 2023.
[16] Lord Anderson, 'Independent review of the Investigatory Powers Act 2016', 30 June 2023.

> "delivering international roaming services that will see 4G voice calls and messaging not being handled by the UK operator but being automatically routed via the home [non-UK] networks over a dedicated IP link".[17] This proposal was endorsed by Lord Anderson.

Other proposals focused on clarifying certain definitions in the IPA 2016 and giving greater flexibility to the oversight and warrantry processes. Further detail and analysis of the proposals, including a full list of recommendations, can be found in Lord Anderson's report: 'Independent review of the Investigatory Powers Act 2016', 30 June 2023.

In summary, Lord Anderson believed the recommended changes would leave the central themes of the legislation intact, including the "strong independent scrutiny" at its core, whilst giving the intelligence agencies, law enforcement and the IPC the "extra agility" they need.[18] His report also commented on the potential need for wholesale reform in the future (bearing in mind technological developments including artificial intelligence) and how this process might be started.

3. Details of the Investigatory Powers (Amendment) Bill 2023–24

3.1 Introduction of the bill

The Investigatory Powers (Amendment) Bill was formally announced as part of the King's Speech on 7 November 2023. In the background briefing to the King's Speech the government again set out its views that the investigatory powers regime needed to be updated in light of technological change and evolving threats. It said that this was important to give the security and intelligence agencies and law enforcement bodies the tools they needed to "keep us safe, prevent terrorism and take on hostile states.[19]

[17] As above, p 52.
[18] As above, executive summary.
[19] Prime Minister's Office, 'King's Speech 2023: Background briefing notes', 7 November 2023, p 69.

The government stated that the bill would make targeted changes to improve public safety and that it would be "recalibrating" aspects of the regime rather than creating "new powers":

> The Investigatory Powers (Amendment) Bill will update the Investigatory Powers Act 2016 to deliver the urgent changes needed to protect the British people, enabling the intelligence agencies to keep up-to-date in tackling a range of evolving threats and accelerating technological advancements that provide new opportunities for terrorists, hostile state actors, child abusers and criminal gangs.
>
> These limited and targeted reforms to the 2016 act do not create new powers but, instead, recalibrate certain elements of the current regime to ensure that it remains fit-for-purpose to respond to modern threats.[20]

The bill received its first reading in the House of Lords on 8 November 2023.

3.2 Provisions in the bill

The bill contains 31 clauses and two schedules. In broad terms, the bill would do the following:[21]

- introduce changes to the BPD regime intended to improve the intelligence services' ability to use less sensitive datasets (such as publicly and commercially available data)
- place the intelligence services' examination of BPDs held by third parties (external organisations 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)
- introduce changes to the notices regimes intended to 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"
- create a new condition for the use of ICRs by the intelligence services and the National Crime Agency (NCA) for 'target detection'

---

[20] As above.

[21] Explanatory notes, p 6.

- adjust the oversight regime to support the IPC in their role, including powers to enable the IPC to delegate some functions to JCs, appoint deputies and put certain functions on a statutory basis
- introduce measures to make the warrantry authorisation processes more flexible for the intelligence services, as well as for the NCA
- provide for changes to the communications data regime to provide greater certainty on the circumstances for lawful data acquisition

Further details on these provisions are set out below.

3.2.1 Part 1: Bulk personal datasets

As stated above, the government believes the current IPA 2016 framework is restricting the ability for intelligence agencies to adequately use BPDs to protect national security.

The explanatory notes (EN) to the bill highlight Lord Anderson's endorsement for changes to this regime, adding:

> 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.[22]

Clauses 1 and 2 would introduce an alternative less stringent regulatory regime for BPDs where there is "low or no reasonable expectation of privacy". The EN provide the examples of online encyclopaedias and news media.[23] BPDs in this category would need authorisations rather than warrants for their use. The new regime would operate alongside the existing part 7 regime. The clauses would set out the tests for whether a BPD should be considered in this category and how the authorisation regime would work. For example, it would generally include a requirement for JC approval.[24]

Clause 3 would extend the duration of a part 7 BPD warrant from six months to 12 months. The government explained that BPDs are "often used to support long-term

[22] As above, p 8.
[23] As above, p 9.
[24] As above, p 32.

strategic intelligence activities rather than short-term tactical actions" and this change would allow the BPDs' value to be better demonstrated.[25]

Clause 4 would allow agency heads to delegate certain functions in relation to BPD warrants to an appropriate Crown servant acting on their behalf. However, the EN specified that agency heads would still be accountable for decisions taken on their behalf and they would still need to personally carry out functions where risks are higher (for example, actioning the urgent cessation of BDP activity where required).[26]

Clause 5 would create a new regime for third party BPDs. These are datasets which would fall within part 7 of IPA 2016 if an intelligence service were to retain it, but which are actually held by a third party (such as government departments or commercial entities). The new regime would set a framework for the intelligence agencies to examine it "in situ" (therefore, on the third party's system), rather than requiring acquisition and retention of it. The EN gave the following example:

> [A]n 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 support them in carrying out their statutory functions. It may be more proportionate or practical for the intelligence service to examine a dataset held by a third party rather than acquire and retain the data themselves.[27]

The new regime would use the "double-lock" system, therefore requiring approval from the secretary of state and a JC, and would include statutory oversight by the IPC. The EN also explained that these provisions build upon recommendations from the Investigatory Powers Commissioners Office (IPCO).[28]

Clause 6 consists of miscellaneous drafting amendments.

---

[25] As above, p 9.
[26] As above.
[27] As above, p 10.
[28] As above.

3.2.2 Part 2: Oversight arrangements

The bill would seek to make changes to the operation and arrangement of the IPC's functions. The EN set out the current setup as follows:

> 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.[29]

However, the government contends that the IPA 2016 makes it hard to make changes to the regime and therefore intended the provisions in the bill to provide more flexibility and to provide "greater legislative clarity" of the oversight regime.[30] As noted by the EN, these changes are supported by the IPCO and, where relevant, Lord Anderson's review.

Clauses 7 and 8 would allow the IPC to appoint up to two deputy IPCs to carry out certain functions when the IPC is not available. The appointment of the deputy IPCs would be the responsibility of the IPC.

Clause 9 would allow the IPC to appoint temporary JCs in exceptional circumstances. The EN explained that this power was available during the coronavirus pandemic and had proved "vital" to the continued operation of the oversight regime during that time.[31] However, the legislation enabling this has now expired. The government contends that these powers would be a useful long-term option, stating that:

> The powers proposed would specify that: the IPC may appoint temporary JCs to carry out the functions conferred on JCs by any enactment; a temporary JC would be appointed for one or more terms not exceeding six months each and not exceeding three years in total; and the secretary of state and the IPC must also agree that an exceptional circumstance which results in a shortage of JCs exists before these powers are exercised.[32]

---

[29] As above, p 15.
[30] As above.
[31] As above, p 16.
[32] As above, pp 16–17.

Clause 10 makes various changes relating to the IPC's powers; namely:

- To remove the IPC's oversight functions relating to telecommunications restriction orders (TROs) for prisoners. The government argues that TROs are already subject to judicial approval in the county court, providing "the necessary degree of assurance and oversight", and that it had "not identified any additional benefit in the IPC overseeing this process after the event".[33]
- To place the IPC's oversight of compliance by the Ministry of Defence (MoD) onto a statutory footing. The EN explained that the "IPC currently provides oversight of the MoD's overseas covert human intelligence sources and surveillance operations on a non-statutory basis.[34] The government said that the changes in the bill would not grant new powers; instead, it would formalise them in response to a recommendation from the current IPC, Sir Brian Leveson.
- To extend the power of the prime minister to issue directions requiring the IPC to carry out additional oversight functions in respect of any public authority not mentioned in s 230(1) of the IPA 2016, so far as they are engaging in intelligence activities. The EN stated that the aim of this was to "ensure clearer parameters regarding the IPC's oversight and that law enforcement agencies such as the NCA would be included in the scope of s 230".[35] It also said it would improve flexibility.
- To clarify the scope of error reporting to the IPC to include "errors of a description identified in codes of practice issued under the Regulation of Investigatory Powers Act 2000, Regulation of Investigatory Powers (Scotland) Act 2000 and the Police Act 1997 (in addition to the IPA 2016)".[36] This relates to serious errors made in the use of investigatory powers. The EN explained that, in practice, these errors are already reported to the IPC by public authorities. However, the amendment is intended to clarify that these fall under the IPC's remit and make the reporting mandatory.

3.2.3 Part 3: Communications data

In the context of the bill, the EN described communications data (CD) as metadata attached to communications that can indicate the "'who', 'when', 'where' and 'how'".[37]

---

[33] As above, p 16.
[34] As above, p 15.
[35] As above, p 16.
[36] As above, p 17.
[37] As above, p 11.

Clause 11 of the bill relates to s 11 of the IPA 2016, which provides for an offence when a relevant person within a relevant public authority "knowingly or recklessly" obtains CD from a TO or a postal operator (PO) without lawful authority.[38] The government has highlighted concerns with the drafting of this section in terms of its impact and complexity for public authorities and public sector bodies. As such, clause 11 seeks to amend s 11 in the 2016 act to provide examples of what would constitute "lawful authority" and to exclude public authorities from being deemed a TO. However, the EN stated that "the sharing of CD between public authorities would still be required to comply with data protection legislation and would continue to be subject to sufficient oversight".[39]

Clause 12 aims to provide clarity on how certain CD is considered under various provisions of the IPA 2016 regime. The EN detailed these provisions as follows:

> 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.
>
> At present, there is insufficient clarity over whether subscriber and account data is CD or content, for example in the context of registration details provided in online forms when an individual is setting up an account or taking up a service over the internet.
>
> Due to the complex nature of whether subscriber and account data amount to CD or content, this bill proposes amending s 261 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.[40]

Clause 13 relates to s 12 of the IPA 2016. As explained by the EN, s 12 restricts the information gathering powers of CD by public authorities:

---

[38] As above, p 17.
[39] As above, p 18.
[40] As above, p 19.

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

As a result, the government contends that this has led to potential issues with public authorities being able to perform their statutory functions as they need to:

> [T]here are concerns that several bodies with regulatory or supervisory functions, such as those with responsibility for supervising the financial sector and ensuring compliance with money laundering and terrorist financing regulations, may be unable to perform their statutory functions as effectively as they need to.[41]

Clause 13 aims to adjust these rules to make it easier for certain public authorities to exercise information gathering powers. For example, it would amend the definition of 'regulatory power' to 'regulatory or supervisory power' so as to include bodies such as the Financial Conduct Authority. However, certain restrictions and IPC oversight would still apply where it was pursued for criminal investigations or criminal prosecutions.

Clause 14 relates to ICRs. These are records, held by a TO, about the service to which a device has connected on the internet, for example that someone has accessed 'illegalsite.com'.[42] The clause aims to expand the rules for the use of ICRs to improve 'target detection'; for example, discovering people who may be involved in serious crime. The EN provide the following further detail:

> The way in which the IPA 2016 is currently drafted requires certain thresholds to be met on the 'known' elements of the investigation, such as when a website has been accessed. This limits the ability of the intelligence services and NCA to use ICRs to detect previously 'unknown' criminals online. The proposed changes would help the intelligence services and NCA to detect and locate individuals involved in serious

---

[41] As above, p 18.

[42] As above, p 12.

> 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.
>
> The bill seeks to achieve this by adding a new condition to the list of existing conditions for the use of ICRs at s62 of the IPA 2016. The intention of this is to improve target detection, enhancing the usefulness of the power without disproportionately increasing the level of intrusion. This new condition would only be available to the intelligence services and the NCA for a more limited set of lawful purposes relating solely to national security, the economic wellbeing of the UK (so far as those interests are also relevant to the interests of national security), and for serious crime purposes.[43]

The new condition would set out who may use the condition and under which circumstances. For example, condition D1 would be that the IPC considers that it is necessary 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".[44] Designated senior officers may also authorise use of the provision in "urgent cases only".

3.2.4 Part 4: Amendments to the notices regime

This part of the bill relates to requirements for TOs (or POs) to comply with different types of notices to assist with the UK's national security and law enforcement. As set out in the EN, the IPA 2016 provides for three different types of notice:

- 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 TOs.
- Technical capability notices (TCNs) require TOs to provide and maintain technical capabilities enabling them to respond to relevant IPA 2016 authorisations or warrants allowing access to communications data, the content of a communication (the 'what'), or to enable equipment interference. A notice does not itself authorise the activity that the technical capability is intended to enable.

---

[43] As above, pp 12–13.

[44] As above, pp 43–4.

- National security notices (NSNs) require the TO 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).[45]

All of these notices require the 'double-lock' procedure to be followed before they can be issued to the operator in question.[46] The secretary of state must also consider factors including the likely benefit, the technical feasibility, and the potential cost of complying with the notice. The notice itself does not grant access to data; authorisations or warrants must be obtained as set out under the IPA 2016.

The government contends that changes, as set out in the following clauses, to the notices regime are needed in light of the significant technological change which has occurred since 2016. It ran a consultation on its proposals for change over the summer of 2023 and published the outcome of the consultation on 8 November 2023 (the same day as the bill's first reading).[47]

Clause 15 would amend s 87 of the IPA 2016, which limits what types of communications data can be required to be retained by a TO under a DRN. The new clause would provide that data which can only be obtained by processing ICRs and relevant communications data relating to a relevant roaming service be part of a DRN.[48] The clause defines a relevant roaming service as follows: "a telecommunications service provided by the system operator under an agreement with a TO outside the UK (the "non-UK operator") which facilitates the use by persons in the United Kingdom of the system operator's telecommunication system to access one or more telecommunications services of the non-UK operator". The EN explained that this related to a provision in the IPA 2016 to bar the retention of 'third party data', and stated:

> There is no intention to revisit the point of principle; however, the bill contains measures seeking to amend s 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.[49]

---

[45] As above, p 11.
[46] As above.
[47] Home Office, 'Government response to the Home Office consultation on revised notices regimes', updated 8 November 2023.
[48] Explanatory notes, p 44.
[49] As above, p 12.

Clause 16 would bring the provisions for extraterritorial enforcement of DRNs in line with those of TCNs. The government explains the rationale for these changes as follows:

> 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 DRN is enforceable by civil proceedings against a person in the UK, but there is no express provision permitting the enforcement of a DRN against a person outside the UK. The bill therefore seeks to amend sections 95 and 97 to allow extraterritorial enforcement of DRNs to strengthen policy options when addressing emerging technology, bringing them in line with TCNs.[50]

The government contends that these broader enforcement provisions are needed in the light of the increasing volume of data of interest now held by international companies.

Clause 17 is intended to ensure the status quo is retained when a notice issued to a TO is being reviewed. As explained by the EN:

> 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. Section 90(4)(a) (data retention notices) specifies that during that review period the TO is not required to make any changes to specifically comply with the notice.[51]

The bill seeks to add to this by requiring the TO to also not make any "relevant changes" relating to obligations in their notice. Therefore, 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".[52]

Clause 18 seeks to clarify the meaning of TO in order to ensure "large companies with complex corporate structures are covered in their totality by the IPA 2016". [53]

---

[50] As above.

[51] As above, p 22.

[52] As above, p 45.

[53] As above.

Clause 19 would provide for the renewal of notices where those notices have not been varied or revoked within a relevant period (two years from certain proscribed dates). It would also set out conditions for the renewal of a notice; for example, that the secretary of state still deems the notice necessary and that the decision to renew is approved by a JC.

Clause 20 would introduce a notification requirement which can be issued to relevant operators requiring them 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".[54] Regulations would set out what kind of changes would be covered and thresholds to ensure the notification requirement "does not disproportionately or unnecessarily affect operators who do not hold or provide operationally relevant data".[55] The clause would also set out what the secretary of state must consider before issuing a notice and would require consultation with the operator. In addition, the clause sets out rules for the variation or revocation of the notice by the secretary of state.

The clause specifies that the notice would be enforceable by civil proceedings under the following scenarios:

- A person to whom a notice is given under this section, or any person employed or engaged for the purposes of that person's business, must not disclose the existence or contents of the notice to any other person without the permission of the secretary of state.
- A relevant operator to whom a notice is given under this section must comply with the notice a reasonable time before making any relevant changes to which the notice relates.

3.2.5 Part 5: Warrants and other provisions

Clause 21 relates to the authorisation of warrants to intercept or examine communications sent to or from an MP or member of a devolved legislature. Currently, the IPA 2016 requires these to be authorised under the 'triple-lock' procedure, which involves the secretary of state, a JC and the prime minister. Clause 21 would amend this so that the prime minister could designate an additional secretary of state to authorise in their place when the prime minister is unavailable and if the authorisation request is deemed urgent.

---

[54] As above, p 12.

[55] As above, p 46.

Clause 22 would make a similar change to clause 21 regarding warrants for equipment interference authorisations involving MPs or members of devolved legislatures. Equipment interference authorisation allows the security and intelligence agencies, law enforcement and the armed forces to "interfere with equipment to obtain electronic data".[56] This includes computers, tablets, smartphones, cables and storage devices. Again, the clause would mean that the prime minister could designate an additional secretary of state to authorise the application when they were unavailable, and the request was deemed urgent.

Clause 23 would make the general authorisation of warrants for targeted equipment interference (TEI) applications under s 106 of the IPA 2016 more flexible. It would add deputy director generals of the NCA to the list of law enforcement officials who are able to delegate the decisions on TEI applications to "appropriate delegates" in urgent cases.[57]

Clause 24 would amend the processes linked to the removal of a subject from a TEI warrant so as to remove the requirement to notify the secretary of state at the point of the removal of the subject. The government argues that, as no privacy rights were impacted at this stage, notifying the secretary of state is an unnecessary step.[58]

Clause 25 seeks to rectify drafting issues relating to equipment interference provisions in the IPA 2016.

Clause 26 would amend the IPA 2016 so that intercepted communications and relevant secondary data could be considered in proceedings involving the Parole Board of England and Wales. The government argued that the panel members of the 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".[59] The EN noted that this was already the case in Northern Ireland proceedings.

Clause 27 would exempt further material from being available through freedom of information requests. The EN set out the rationale for this provision as follows:

> The Freedom of Information Act 2000 (FOIA) provides a general right of access to recorded information held by 'public authorities', as defined by s 3 with reference to

[56] As above, p 14.
[57] As above.
[58] As above.
[59] As above, p 19.

bodies listed in schedule 1, or companies as defined within s 6.

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

This bill seeks to add JCs (a term that includes the IPC) to the list of bodies dealing with security matters at s 23 of FOIA. Section 23 is an absolute exemption, thereby protecting information held by other public authorities which relates to the activities of JCs.[60]

3.2.6 Part 6: General provisions

Clauses 28 to 31 contain miscellaneous provisions, including commencement provisions and the territorial extent of the bill. The legislation would apply to the whole of the UK.

4. Commentary on the bill's proposals

4.1 Consultation on the new notices regime

As mentioned above, the government ran a consultation over the summer of 2023 on its proposals for a new notices regime. The outcome of the consultation was then published by the Home Office on 8 November 2023.[61]

Overall, the government stated that the majority of the concerns related to end-to-end encryption (E2EE)[62], and the proposed clause 20 power allowing a notification requirement

[60] As above, p 17.

[61] Home Office, 'Government response to the Home Office consultation on revised notices regimes', updated 8 November 2023.

[62] TechTarget defines end-to-end encryption (E2EE) as a "method of secure communication that prevents third parties from accessing data while it's transferred from one end system or device to another. In E2EE, the data is encrypted on the sender's system or device, and only the intended recipient can decrypt it. As it travels to its

to be issued to TOs requiring them to notify the secretary of state of relevant changes to their products or services. Regarding the clause 20 power, the Home Office reported the following concerns had been raised by consultation respondents:[63]

- The "predominant objection" was that it would allow the Home Office to block the rollout of new technologies and that "this would subsequently stifle innovation".
- It would empower the Home Office to "pre-emptively direct the design of products and services intended for the UK consumer market and make the Home Office the de facto global arbiter of what level of data security and encryption are permissible".
- The proposals were not proportionate and not enough weight was given in the legislation to the necessity and proportionality of proposed notices.
- At-risk groups could be put in danger because of the proposal and "bad actors could exploit vulnerabilities during any delay".
- The proposal may be "unreasonable and unworkable as operators do not necessarily know what changes to a service could affect lawful access". On this, respondents said that further details about how the powers would operate in practice would be useful.

Responding to these concerns, the government stated that a form of these notification requirements was already set out in the notification regime. It highlighted various parts of the Investigatory Powers (Technical Capability) Regulations 2018.[64] Ministers said the government was intending to isolate this requirement so as to "formalise the expectations we have of relevant operators with regards to existing lawful access capabilities".[65]

The government also explained that the notification regime would not block a TO from

---

destination, the message cannot be read or tampered with by an internet service provider, application service provider, hacker or any other entity or service" (TechTarget, 'End-to-end encryption', accessed 10 November 2023).

[63] Home Office, 'Government response to the Home Office consultation on revised notices regimes', updated 8 November 2023.

[64] Namely schedule 1, part 1, paragraph 13; schedule 2, part 1, paragraph 13; and schedule 3, paragraph 11 of the Investigatory Powers (Technical Capability) Regulations 2018.

[65] As above.

making changes to a new or existing service:

> The notification requirement will not allow the secretary of state to prevent a technical change to an existing service, rollout of a new service or any other relevant change. Equally, it is not intended as an approval mechanism. There will be no method within the notification requirement itself for the secretary of state to intervene in any way with the decision the operator has chosen. The requirement will be just to notify the secretary of state.
>
> The notification requirement is intended to ensure law enforcement and other relevant public authorities have time to adjust accordingly and mitigate the impacts wherever possible to continue to keep the public safe.[66]

It also clarified that operators would be informed of notification requirements, that further details would be set out in the regulations, and that the secretary of state would consider necessity and proportionality in the same way as they would for any of the other investigatory powers. In practice, the government said it only expected the provisions to apply to a small number of companies "who routinely provide exceptional lawful access under the IPA".[67]

Although it stressed that E2EE was not an issue being consulted on in its proposals, the government did set out its position on the matter. It highlighted its support for private and secure communications, but it said that this must be balanced with the need for law enforcement and intelligence agencies to prevent, investigate and act on serious crimes and threats to national security. It stated:

> We fully support the responsible use of strong encryption, including end-to-end encryption, where public safety is designed in. We know it is possible to implement end-to-end encrypted services in a way which is consistent with public safety.[68]

4.2 Other reaction to the bill

A number of statements were published upon the bill's announcement in the King's Speech, but prior to the actual publication of the bill, raising concerns about its potential impact. For

---

[66] As above.
[67] As above.
[68] As above.

example, reports indicated that various tech firms had raised concerns about the proposed powers in the bill and how far they could go. In particular, the Financial Times reported that several firms, including Meta and Apple, had signalled they may withdraw from the UK market if the legislation affects their ability to offer encryption and other privacy features to consumers.[69]

Similarly, the Open Rights Group (an online privacy campaign group), feared the proposals could mean that global tech companies would need "permission" from the UK government if they wanted to make changes to security features to their services.[70] Big Brother Watch also raised concerns about the potential reach of the bill. Issuing a statement on 7 November 2023 its director, Silkie Carlo, stated:

> The King's Speech revealed plans to add yet more spying powers to the Snoopers' Charter. The government says it will give them the power to veto private tech companies' privacy and security features. Such powers would be more extreme than even the world's most despotic regimes.
>
> This would be yet another bill that would exert extraordinary control to treat private companies as extensions of the state in order to conduct mass surveillance of millions of law-abiding citizens. It would be a major blow to the population's security.[71]

[69] Anna Gross and Cristina Criddle, 'Tech groups fear new powers will allow UK to block encryption', Financial Times (£), 7 November 2023.
[70] Open Rights Group, 'King's Speech: Investigatory Powers Act reforms threaten security', 7 November 2023.
[71] Big Brother Watch, 'Big Brother Watch response to the King's Speech', 7 November 2023.

About the Library

A full list of Lords Library briefings is available on the Library's website.

The Library publishes briefings for all major items of business debated in the House of Lords. The Library also publishes briefings on the House of Lords itself and other subjects that may be of interest to members.

Library briefings are produced for the benefit of Members of the House of Lords. They provide impartial, authoritative, politically balanced information in support of members' parliamentary duties. They are intended as a general briefing only and should not be relied on as a substitute for specific advice.

Every effort is made to ensure that the information contained in Lords Library briefings is correct at the time of publication. Readers should be aware however that briefings are not necessarily updated or otherwise amended to reflect subsequent changes.

Disclaimer

The House of Lords or the authors(s) shall not be liable for any errors or omissions, or for any loss or damage of any kind arising from its use, and may remove, vary or amend any information at any time without prior notice. The House of Lords accepts no responsibility for any references or links to, or the content of, information maintained by third parties.

This information is provided subject to the conditions of the Open Parliament Licence.

Authors are available to discuss the contents of the briefings with Members of the House of Lords and their staff but cannot advise members of the general public.

Any comments on Library briefings should be sent to the Head of Research Services, House of Lords Library, London SW1A 0PW or emailed to hlresearchservices@parliament.uk.