HOUSE OF LORDS

Library Note

Investigatory Powers Bill (HL Bill 40 of 2016–17)

This House of Lords Library briefing provides an overview of the provisions of the Investigatory Powers Bill. This is a government Bill introduced in the House of Commons on 1 March 2016 and carried over into the current session. Following completion of its Commons stages, it was introduced in the House of Lords on 8 June 2016. The Bill is scheduled for second reading debate on 27 June 2016.

The Bill includes the following provisions:

- Powers for the targeted interception of communications.
- Powers for targeted equipment interference (accessing computer equipment, mobile phones etc) in order to obtain stored communications and other data.
- Powers to obtain communications data (the context, but not the content of a communication) from communications service providers.
- Powers to obtain internet connection records (a proposed new form of communications data) from communications service providers.
- Powers for the security and intelligence agencies to undertake interception and equipment interference on a larger scale and to acquire communications data in bulk.
- Powers for the security and intelligence agencies to acquire and retain bulk personal datasets (datasets which contain containing information about a wide range of people, most of whom are not of interest to the agencies).
- A new system for the authorisation of warrants, whereby the approval of the Secretary of State and an independent Judicial Commissioner will be required.
- An overhaul of the oversight regime for investigatory powers, with the three current commissioners and their offices replaced by a single Investigatory Powers Commissioner.

Most of these investigatory powers are already used under existing legislation and are being consolidated and clarified in this Bill. The power to obtain internet connection records is a new power. The bulk powers, used by the security and intelligence agencies, have only recently been avowed by Government.

Matt Korris
21 June 2016
LLN 2016/032

Table of Contents

1. Introduction 1
    1.1 Second Reading in the House of Commons 1
    1.2 Committee Stage in the House of Commons 3
    1.3 Report Stage in the House of Commons 3
2. Part 1: General Privacy Protections 5
3. Part 2: Lawful Interception of Communications 6
    3.1 Judicial Review Principles 6
    3.2 Purposes for Warrants 7
    3.3 Modifications and Renewals 8
    3.4 Safeguards for Members of Parliament, Legally Privileged Material and Trade Unions 9
4. Parts 3 and 4: Authorisations for Obtaining Communications Data and Retention of Communications Data 10
    4.1 Authorisations for Communications Data 11
    4.2 Protection for Journalists and Whistleblowers 12
    4.3 Public Authorities Entitled to Access Communications Data 13
    4.4 Internet Connection Records 14
    4.5 Request Filter 15
5. Part 5: Equipment Interference 16
6. Part 6: Bulk Warrants 17
    6.1 The Operational Case for Bulk Powers 17
    6.2 Operational Purposes for Bulk Powers 19
    6.3 Modifications to Bulk Warrants 20
7. Part 7: Bulk Personal Dataset Warrants 20
    7.1 Class BPD Warrants 21
    7.2 Medical Records 22
8. Part 8: Oversight Arrangements 22
    8.1 Appointment of Judicial Commissioners 23
    8.2 Separation of Authorisation and Oversight Functions 23
    8.3 Creation of an Investigatory Powers Commission 24
    8.4 IPC Remit and Role of the ISC 24
    8.5 Protection for Whistleblowers and Notifications for Subjects of Investigatory Powers 25
9. Part 9: Miscellaneous and General Provisions 25
    9.1 Judicial Authorisation for Notices 25
    9.2 Notices and Encryption 25
10. Third Reading in the House of Commons 26

1. Introduction

This Library briefing provides an outline of the provisions of the Investigatory Powers Bill, as introduced in the House of Lords on 8 June 2016, indicating where amendments were made to the Bill in the House of Commons. It also outlines some of the amendments debated at report stage and not made to the Bill, including those on which the House divided.

The Bill is informed by three recent reviews of investigatory powers:

- David Anderson QC, Independent Reviewer of Terrorism Legislation, *A Question of Trust: Report of the Investigatory Powers Review*, June 2015
- Intelligence and Security Committee of Parliament, *Privacy and Security: A Modern and Transparent Legal Framework*, 12 March 2015, HC 1075 of session 2014–15
- Royal United Services Institute, *A Democratic Licence to Operate: Report of the Independent Surveillance Review*, July 2015

The draft Investigatory Powers Bill[1] was subsequently published on 4 November 2015 and scrutinised by three parliamentary committees, all of which reported in February 2016:

- Joint Committee on the Draft Investigatory Powers Bill, *Draft Investigatory Powers Bill*, 11 February 2016, HL Paper 93 of session 2015–16
- Intelligence and Security Committee of Parliament, *Report on the Draft Investigatory Powers Bill*, 9 February 2016, HC 795 of session 2015–16
- House of Commons Science and Technology Committee, *Investigatory Powers Bill: Technology Issues*, 1 February 2016, HC 573 of session 2015–16

The Government published a combined response to all three committees on 1 March 2016,[2] alongside the introduction of the revised Investigatory Powers Bill to the House of Commons.

For an analysis of the pre-legislative scrutiny of the draft Bill, and the changes made by the Government subsequently, see the House of Commons Library briefing, *Investigatory Powers Bill* (11 March 2016).[3]

1.1 Second Reading in the House of Commons

Speaking during second reading, the Home Secretary, Theresa May, said that the Government "are committed to updating and consolidating our country's investigatory powers in a clear and comprehensive new law that will stand the test of time".[4] She said that the Bill "will provide world-leading legislation setting out in detail the powers available to the police and the security and intelligence services to gather and access communications and communications data. It will provide unparalleled openness and transparency about our investigatory powers, create the

[1] HM Government, *Draft Investigatory Powers Bill*, November 2015, Cm 9152.
[2] HM Government, *Investigatory Powers Bill: Government Response to Pre-Legislative Scrutiny*, March 2016, Cm 9219.
[3] House of Commons Library, *Investigatory Powers Bill*, 11 March 2016.
[4] HC *Hansard*, 15 March 2016, col 812.

strongest safeguards, and establish a rigorous oversight regime".[5] She also reminded the House that the Data Retention and Investigatory Powers Act 2014, which the Bill would replace, contained a sunset clause and would expire at the end of 2016 and that the "grave threats" faced by the country made it imperative that new legislation was passed.[6]

The Shadow Home Secretary, Andy Burnham, acknowledged that there was a widespread consensus of the need to update the laws relating to investigatory powers.[7] He said that while the Labour Party would not oppose the Bill at second reading, it was "not yet worthy" of their support as there were significant weaknesses that needed to be addressed.[8] These included: the need for a presumption of privacy, particularly in relation to sensitive professions (parliamentarians, journalists and lawyers); the thresholds and justifications for the use of the powers; the content and use of internet connection records (ICRs); greater justification for the inclusion of the bulk powers; the use of judicial review principles by the Judicial Commissioner when considering applications for a warrant; and the potential misuse of the powers.[9]

The SNP Spokesperson for Justice and Home Affairs, Joanna Cherry, also acknowledged the need for the law in this area to have a "thorough overhaul" and welcomed the attempt to consolidate a number of existing statutes in the Bill.[10] She said that, as with the Labour Party, the SNP would not vote against the Bill at second reading, but that they had significant concerns about the powers in the Bill and that it would need to be "extensively amended" if they were not to vote against it at a later stage.[11]

Nick Clegg, speaking for the Liberal Democrats, acknowledged that the Bill represented "progress in some important respects" on previous proposals, but said that it was "not yet in a fit state" and his Party would not support it.[12]

Dominic Grieve, chair of the Intelligence and Security Committee of Parliament (ISC), said that the present Committee and its predecessor were satisfied "in broad terms" with the powers in the Bill and that they were not "unnecessary or disproportionate to what we need to protect ourselves".[13] He noted with disappointment the lack of the "clear statement on overarching privacy protections" that the ISC had recommended and outlined his concerns about the different routes for obtaining communications data under the powers in the Bill.[14] He also questioned the need for bulk equipment interference warrants and class bulk personal dataset warrants.[15]

Following the debate, the second reading motion was carried by 281 votes to 15.[16] The programme motion and a carry-over motion were subsequently agreed without division.[17]

---

[5] HC *Hansard*, 15 March 2016, col 813.
[6] ibid, col 813.
[7] ibid, col 824.
[8] ibid, col 825.
[9] ibid, cols 828–35.
[10] ibid, col 839.
[11] ibid, col 840.
[12] ibid, col 850.
[13] ibid, col 836.
[14] ibid, col 837.
[15] ibid, cols 837–9.
[16] ibid, col 904.
[17] ibid, col 908.

1.2 Committee Stage in the House of Commons

The Bill was considered at a public bill committee of MPs, over the course of 16 sittings held between 24 March and 3 May 2016. The amendments made were largely technical or minor drafting changes, although the Security Minister, John Hayes, made commitments to consider a number of the issues raised ahead of report stage.

Particularly controversial areas included:

- The process for judicial authorisation of warrants.
- The retention of internet connection records.
- The need for an independent review of bulk powers.
- The extent to which the Bill makes adequate provision for the protection of privacy.
- Protection for sensitive and confidential communications, including those of journalists and MPs, and material subject to legal professional privilege.

A summary of proceedings at committee stage has been provided by the House of Commons Library in its briefing *Investigatory Powers Bill: Committee Stage Report*.[18]

1.3 Report Stage in the House of Commons

Report stage of the Investigatory Powers Bill took place over two days on 6 and 7 June 2016. During the first day of report stage, the Government passed amendments inserting new clauses on:

- Privacy principles and protections.
- Civil liability for certain unlawful interceptions.
- The modification of warrants.
- Approval of national security notices and technical security notices by Judicial Commissioners.

Numerous minor and consequential government amendments were also passed.

The Government accepted a Labour amendment to include additional protection for the legitimate activities of trade unions. Additionally the Government accepted two amendments proposed by Dominic Grieve, chair of the ISC, on behalf of the Committee. These require the Investigatory Powers Commissioner (IPC) to review the privacy safeguards for warrants issued under the Bill and allow the Prime Minister to refer oversight matters to the IPC for review on behalf of the ISC.

[18] House of Commons Library, *Investigatory Powers Bill: Committee Stage Report*, 2 June 2016.

Five amendments proposed by the SNP were pushed to division, all unsuccessfully. In each case the SNP and Liberal Democrats voted in favour, the Conservatives against and Labour abstained.

On the second day of report stage Government amendments were passed to strengthen the safeguards on accessing communications data related to journalistic material and on bulk personal datasets containing medical records. Consequential amendments were passed on the modification of warrants.

SNP amendments to remove parts 6 and 7 of the Bill (bulk powers and bulk personal datasets) and a Liberal Democrat amendment to remove internet connection records from part 3 of the Bill were all defeated at division.

During report stage both government and opposition Members spoke of a constructive approach towards consideration of the Bill. The Security Minister, John Hayes, said: "I do not want to indulge in hyperbole, but consideration of the Bill has been characterised by an unusual degree of co-operation to get it right across the House".[19] He added that "the SNP made an incredibly helpful contribution, because it tested the Government, held us to account and made a number of useful and thought-through proposals. The Opposition […] equally added immense value to our consideration".[20]

The Shadow Immigration Minister, Kier Starmer, noted that "there have been significant movement and concessions from the Government; again, that has been constructive. Important moves in the right direction, which will improve the Bill, have been achieved through that dialogue".[21] The chair of the Joint Committee on Human Rights (JCHR), Harriet Harman, congratulated the Government, the Labour and SNP front and backbenchers for "working constructively"[22] and ISC chair Dominic Grieve said that "the Government have moved substantially on some key issues, providing greater protection, for which we should be grateful".[23]

Alistair Carmichael (Liberal Democrat MP for Orkney and Shetland) was more sceptical: "one thing that I have learned to recognise is a well-rehearsed line exchanged between the two Front-Bench teams. I think we saw that when the shadow Home Secretary was getting his assurances from the Minister for Security".[24]

The SNP Spokesperson for Justice and Home Affairs, Joanna Cherry, said that she recognised that the Government had made "significant concessions", but added that the "amendments tabled by the Government for debate today are only a partial response to our legitimate concerns. The Government need to pay more than lip service to the importance of privacy and to the principles of necessity and proportionality".[25]

---

[19] HC *Hansard*, 6 June 2016, cols 879–80.
[20] ibid, col 881.
[21] ibid, col 883.
[22] ibid, col 972.
[23] ibid, col 973.
[24] HC *Hansard*, 7 June 2016, cols 1134–5.
[25] HC *Hansard*, 6 June 2016, cols 897–8.

She also raised concerns about the number of amendments that had been tabled, most of which could not be debated or considered:

> My issue is that other Members—the people sitting behind me, the Labour Members and Government Members—will not get a chance to speak and that we will not get a chance to vote on more than a handful of amendments. Given the degree of concern expressed about the Bill, it is frankly ridiculous that we will get to vote only on maybe eight or nine amendments over the next couple of days out of the hundreds of amendments that have been tabled. I am not ashamed to say that that is no way to legislate. We need to look at the way we go about things.[26]

In total 498 amendments and 27 new clauses were tabled for report stage. Solicitor General Robert Buckland acknowledged that:

> It is a large group, which some hon. Members have described to me as "unprecedented". I would not be so bold as to say that, having served a mere six years in this place. I concede, however, that the group is considerable. That perhaps reflects the huge and legitimate interest of Members of all parties in these particular parts of the Bill.[27]

2. Part 1: General Privacy Protections

Part 1 of the Bill sets out the protections for privacy that underpin the powers in the rest of the Bill. It provides a definition of interception and introduces new offences of unlawful interception and of unlawfully obtaining communications data. It also includes restrictions on requests for interception by overseas authorities and on the assistance that may be provided under mutual assistance agreements.

The protection of privacy has been a central issue in the scrutiny of the Bill. The Intelligence and Security Committee of Parliament (ISC) in its scrutiny of the draft Bill recommended that the Bill set out "universal privacy protections which apply across the full range of investigatory powers".[28] The chair of the ISC, Dominic Grieve, reiterated his call for an overarching privacy clause at second reading[29] and it was subsequently raised by Labour and the SNP during committee stage.[30]

At report stage the Government introduced a new clause entitled "General Duties in Relation to Privacy" in response to these calls. Security Minister John Hayes said that the clause "puts privacy at the heart of the Bill in precisely the overarching way that those who scrutinised it prior to and during committee recommended".[31] He acknowledged that the new clause was "inspired by the ISC" and based on the amendment tabled by Kier Starmer during committee.[32]

---

[26] HC *Hansard*, 6 June 2016, col 899.
[27] ibid, col 948.
[28] Intelligence and Security Committee of Parliament, *Report on the Draft Investigatory Powers Bill*, 9 February 2016, HC 795 of session 2015–16, p 3.
[29] HC *Hansard*, 15 March 2016, col 837.
[30] See House of Commons Library, *Investigatory Powers Bill: Committee Stage Report*, 2 June 2016, pp 7–8; and HC *Hansard*, 6 June 2016, col 879.
[31] HC *Hansard*, 6 June 2016, col 879.
[32] ibid, col 880.

Labour proposed its own privacy clause at report stage. Kier Starmer acknowledged that that the differences between the two were "very slender indeed"[33] and related to the wording of whether public authorities "must have regard to" the requirements of the Human Rights Act 1998 or "give effect to" them.[34] John Hayes said that he was happy to "continue to have a discussion about the fine details" of the privacy clause.[35] The Government's privacy clause was accepted without division.

Additional government amendments to part 1 were approved at report stage to add references to privacy rights under other legislation and to prevent the powers in other legislation from being used to acquire communications data. A new government clause was added to introduce a civil liability for certain unlawful interceptions, which was welcomed by SNP Spokesperson for Justice and Home Affairs, Joanna Cherry, who thanked the Minister for acknowledging that it reflected an amendment she had proposed at committee stage.[36]

3. Part 2: Lawful Interception of Communications

Part 2 of the Bill would allow for targeted interception to be undertaken by law enforcement and the security and intelligence agencies. Interception is the accessing of the content of a communication during its transmission.[37]

The Bill introduces a new authorisation system for the use of investigatory powers, which the Government refers to as the 'double lock'. Under this system an application for a warrant for targeted interception must be approved by both the Secretary of State[38] and by a Judicial Commissioner (see part 8) before it can be issued. In urgent situations a warrant can be issued without a commissioner's involvement, although it must be retrospectively approved by a commissioner within three working days or it will cease to have effect.

This authorisation system also applies to targeted equipment interference warrants (part 5), bulk warrants (part 6) and bulk personal dataset warrants (part 7). It also applies to targeted examination warrants (in parts 2 and 5) which would authorise searching the contents of material acquired using the bulk powers. Amendments at report stage extended the involvement of Judicial Commissioners to include the issuing of national security notices and technical capability notices (part 9).

3.1 Judicial Review Principles

At report stage, debate continued about the role of Judicial Commissioners when authorising warrants. The Bill said that Judicial Commissioners would use 'judicial review principles' when assessing applications for warrants, which led to concerns from opposition parties about the scope of the role of the commissioners; whether it would be a narrow approach, focused purely on assessing whether the Secretary of State had acted properly in authorising a warrant, or whether it would allow for a full assessment of the merits of the application. The Government had consistently said that Judicial Commissioners would receive the same information as the Secretary of State when assessing the application for a warrant and that the

[33] ibid, col 892.
[34] ibid, col 888.
[35] ibid, col 889.
[36] ibid, col 897.
[37] Home Office, *Investigatory Powers Bill Factsheet—Targeted Interception*, March 2016.
[38] If the application for a warrant applies to the communications of an individual in Scotland, it requires the authorisation of a Scottish Minister instead of the Secretary of State.

judicial review principles allowed for the commissioners to take a flexible approach to the task based on a well-understood approach.[39]

In order to allay concerns about the clarity of the judicial review test, the Government introduced a manuscript amendment at report stage stating that a commissioner when assessing a warrant application must do so "with a sufficient degree of care" to ensure that they comply with the duties imposed by the new privacy clause in part 1 of the Bill; such that the action is both necessary and proportionate.

This amendment was welcomed by Keir Starmer, who said: "The test for the judges is now crystal clear: look at necessity and proportionality, and review the Home Secretary's decision with a sufficient degree of care to make sure that the Judicial Commissioner complies with the duties imposed by the general provision in relation to privacy".[40] Andy Burnham concluded that "it will require much closer scrutiny of the initial decision of the Home Secretary and, significantly, bring greater clarity than the Government's initial judicial review test would have done. We believe that that does indeed amount to a real double lock".[41]

The amendment was not enough to satisfy the SNP. While acknowledging that the amendment was an improvement, Joanna Cherry said that the Bill should require the Secretary of State to give reasons for his or her decision, such that the Judicial Commissioner can assess those reasons. She said: "As long as it remains a judicial review standard, I do not see what it is that the Judicial Commissioner is reviewing, in the absence of reasons for the original decision".[42]

The amendment was accepted without division.

3.2 Purposes for Warrants

The Bill sets out in clause 20 that targeted interception warrants may be sought if it is necessary:

a) in the interests of national security,

b) for the purposes of preventing or detecting serious crime,

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

The SNP sought to amend the Bill to remove economic well-being as an acceptable purpose for a warrant. Joanna Cherry argued that:

> The Joint Committee on the Bill said that economic wellbeing should be defined, but the Intelligence and Security Committee went further and said that it should be subsumed within the national security definition and that otherwise it was "unnecessarily confusing and complicated". It was basically saying that if economic harm to the wellbeing of the UK was so serious that it amounted to a threat to national security, it would be covered

[39] HC *Hansard*, 6 June 2016, col 886.
[40] ibid, col 887.
[41] HC *Hansard*, 6 June 2016, col 952.
[42] ibid, col 965.

> by clause 18(2)(a). That was the point the ISC made. We do not need a separate category.[43]

In an intervention, ICR chair Dominic Grieve said "the Committee had the opportunity to hear considerable further evidence provided by the Government, and as a result we were unanimously persuaded that keeping "economic wellbeing" as a separate category was justified".[44] He went on to say:

> The most persuasive argument of the lot was that listing economic wellbeing separately added transparency as to the purposes for which an investigatory power was being sought. We came to the conclusion that it would probably assist the Judicial Commissioners in their consideration of the necessity and proportionality of the warrant, precisely because it highlighted that it fell within a category in which economic wellbeing was present; it was therefore in practice likely to be subject to very detailed scrutiny.[45]

The SNP's amendment was defeated at division by 66 votes to 272.[46]

Joanna Cherry also argued that it was necessary to define national security in the Bill and that the test of preventing or detecting serious crime should state that there is "reasonable suspicion" that a serious criminal offence has or will take place, in order for the Bill to comply with the European Convention on Human Rights.[47] An amendment on this latter point was not reached.

3.3 Modifications and Renewals

The Government introduced new clauses and amendments to strengthen the safeguards relating to the modification and renewal of warrants. For warrants targeted at a group of suspects, sometimes referred to as 'thematic warrants', major modifications—such as adding a name to the warrant—will have to be notified to a Judicial Commissioner. Harriet Harman argued that this change was insufficient:

> The Government have gone such a long way to ensure that warrants are properly issued, so why are they driving a coach and horses through the proposal by saying, "After the warrant has been issued, If you feel like it, you can have a major modification"? Trust me, such modifications will not narrow the scope of warrants, they will only widen them. The Government have moved to an extent and have said that major modifications will be notified to the Judicial Commissioners, but it is not good enough just to tell them; there needs to be a proper approval process. The Government should look again at the proposal.[48]

Summing up, Security Minister John Hayes acknowledged the point and said:

> I entirely accept the point that it would be completely unacceptable to have a robust system for issuing warrants and a less robust system for modifying them. Warranting has

[43] ibid, cols 963–4.
[44] ibid, col 964.
[45] HC *Hansard*, 6 June 2016, col 976.
[46] ibid, col 990.
[47] ibid, cols 963–4.
[48] ibid, col 969.

> to be consistent throughout, and there can be no back-door way of weakening the process. That is not what the Government intend and not what we would allow. We have made those changes but, as I have said, we are happy to consider those matters carefully—I have heard what has been said tonight by Members on both sides of the House about what more might be done.[49]

The SNP were not content with the breadth of the scope of thematic warrants and pressed an amendment to restrict their usage. It was defeated at division by 67 votes to 271.[50]

On the renewal of warrants, John Hayes concluded that:

> Amendments 19 to 23, also tabled on behalf of the Intelligence and Security Committee, seek to prohibit a targeted or bulk interception warrant being renewed for more than 30 days. I do not foresee any circumstance where such a renewal application would be approved by the Secretary of State or Judicial Commissioner, but this is another matter that I agree could be clearer in the Bill. As with the previous amendment, we will revisit this and table an amendment in the other place.[51]

3.4 Safeguards for Members of Parliament, Legally Privileged Material and Trade Unions

Part 2 of the Bill would provide for additional safeguards in relation to the interception of the communications of Members of Parliament[52] and material subject to legal privilege.

In relation to Members of Parliament, the Bill stated that not only would the Secretary of State and a Judicial Commissioner have to approve the issuing of a warrant, but the Prime Minister must also be consulted. The Government proposed an amendment at report stage to require that the Prime Minister not just be consulted but also agree to the interception of a parliamentarian's communications.[53]

Sir Edward Leigh (Conservative MP for Gainsborough) proposed an amendment that would require that the Speaker also be consulted in relation to any warrant intercepting an MP's communications.[54] This suggestion was supported by Harriet Harman on behalf of the JCHR[55] and Alistair Carmichael for the Liberal Democrats.[56] The Solicitor General responded that:

> While I can see the merit in seeking to protect the privileges of parliamentarians through the office of the Speaker, my concern is that involving the Speaker in approving a particular warrantry process or not puts us at risk of confusing Executive action with the roles of this place and of the Speaker in terms of the legislature.[57]

---

[49] ibid, col 982.
[50] ibid, col 987.
[51] HC *Hansard*, 6 June 2016, cols 982–3.
[52] This includes Members of both Houses of Parliament, Members of the Scottish Parliament, National Assembly for Wales, Northern Ireland Assembly and UK Members of the European Parliament.
[53] HC *Hansard*, 6 June 2016, col 950.
[54] ibid, col 958.
[55] ibid, col 971.
[56] ibid, col 977.
[57] ibid, col 950.

The Security Minister, John Hayes, suggested that this proposal would "draw the Speaker into issues of national security […] highly sensitive matters of a kind that Speakers have not historically been involved in. It would be a radical change".[58]

The amendment was not considered further.

The Government was pressured by Members from all sides to improve the safeguards on legally privileged material, with concerns raised that the Bar Council, the Law Society of England and Wales, the Law Society of Scotland and the Faculty of Advocates were all yet to be persuaded that the protections were strong enough.[59] The Solicitor General said that he would be meeting with the Law Society that same week to discuss the Bill further and said that "If clear proposals come forward—I am sure that they will—they can be subject to full, proper scrutiny in the other place".[60]

Labour proposed an amendment at report stage to give explicit protection from interception to the legitimate activities of trade unions,[61] which was supported by the SNP.[62] In response, John Hayes said:

> It would neither be proportionate nor lawful for the security or intelligence agencies to investigate legitimate trade union activity. However, there are good reasons for seeking to put the matter beyond doubt […] I have already praised the Opposition and commended the way they have gone about their scrutiny of the Government's proposals; now I am going to accept the amendment that stands in the name of the Opposition.[63]

The amendment was accepted without division.

4. Parts 3 and 4: Authorisations for Obtaining Communications Data and Retention of Communications Data

Part 3 of the Bill deals with authorisations for obtaining communications data from communications service providers (CSPs). Part 4 sets out the powers for the Secretary of State to issue data retention notices to CSPs to retain and make accessible such data.

The Government explains that "Communications data is the context, but not the content of a communication: who was communicating, when, from where, and with whom. For example it can be a person's mobile phone number or email addresses used to send and receive emails, but not what is said in a telephone conversations or written in an email".[64]

Communications data is currently accessed under powers in the Data Retention and Investigatory Powers Act 2014 which expires at the end of 2016 and which has been the subject of legal challenge.[65]

---

[58] ibid, col 960.
[59] See ibid, col 965 and col 970.
[60] ibid, col 949.
[61] HC *Hansard*, 6 June 2016, cols 884–5.
[62] ibid, cols 964–5.
[63] ibid, col 983.
[64] Home Office, *Investigatory Powers Bill Factsheet—Communications Data*, March 2016.
[65] *Davis et al* v *SSHD [2015] EWHC 2092*.

Part 3 of the Bill allows for the acquisition of internet connection records (ICRs)—a proposed new form of communications data—from CSPs. ICRs are "the name used to describe communications data that can be used to identify, or assist in identifying, internet services that have been accessed by a device".[66] They would include records of source and destination IP (internet protocol) addresses and port numbers, and other information necessary to identify the service a customer has been using, though not what they have been doing on that service.[67]

4.1 Authorisations for Communications Data

Unlike the other powers in the Bill, accessing communications data would not require the approval of a Judicial Commissioner, except in instances where it is being sought in order to identify or confirm the source of journalistic information.

Gavin Newlands (SNP MP for Paisley and Renfrewshire North) argued that there was insufficient protection and oversight for access to communications data. He tabled amendments on behalf of the SNP so that public authorities would require the approval of a Judicial Commissioner for obtaining communications data and that there would need to be a reasonable suspicion of serious crime to authorise such acquisition.[68] He said that:

> The arguments on judicial warrantry have already been rehearsed at length [at committee stage] and I do not intend to detain the House long on this issue […] Suffice it to say, I think hon. Members should pause and reflect on the lack of oversight. Decisions concerning necessity and proportionality can only be made properly by someone who is truly independent from the operations of the organisation.[69]

The amendments were defeated at division by 68 votes to 285.[70]

The Bill would make provision for authorising access to communications data in exceptional circumstances. In such instances, the person seeking to access communications data can also authorise the request themselves, rather than requiring the approval of a designated senior official.

Dominic Grieve tabled amendments on behalf of the ISC to tighten the authorisation regime for such circumstances. He acknowledged that such a provision was necessary but said that the ISC believed it was "too vague and potentially too broad".[71] He explained that:

> The amendment would limit exceptional circumstances to those where the operation is so sensitive that knowledge of it must be kept to an absolute minimum, or where there is an unplanned, time-critical but very significant opportunity to obtain information that might be lost owing to any delay in obtaining a separate approval.[72]

Mr Grieve acknowledged the progress made in a related government amendment, but said further improvement was still necessary. In response, the Solicitor General said: "in principle,

---

[66] Home Office, *Investigatory Powers Bill Factsheet—Internet Connection Records*, March 2016, p 1.
[67] Home Office, *Operational Case for the Retention of Internet Connection Records*, March 2016, p 7.
[68] HC *Hansard*, 7 June 2016, col 1126.
[69] ibid, col 1126.
[70] ibid, col 1140.
[71] HC *Hansard*, 7 June 2016, col 1124.
[72] ibid, col 1124.

we accept the amendment. We will commit to returning with a technically adequate amendment in the other place".[73]

The government amendment was accepted without division and the ISC amendment was not pressed to a vote.

4.2 Protection for Journalists and Whistleblowers

Despite the involvement of Judicial Commissioners in considering warrants for accessing communications data in connection with journalist material, Andy Burnham said that "many journalists and the National Union of Journalists have real concerns" that the Bill weakened existing protections for journalists.[74] He explained that:

> Under PACE [Police and Criminal Evidence Act 1984], journalists are notified when the authorities want to access material and sources, so that they have the ability to challenge that in open court. The worry is that the Bill removes those protections. The National Union of Journalists makes the point that there is no real difference between physical notebooks and communications data held electronically; both could reveal the identity of a source.[75]

Mr Burnham welcomed the amendments tabled by the Government to ensure that Judicial Commissioners must have regard to the public interest of protecting journalists' sources when considering such applications for communications data, but he said that they did not go far enough.[76] He spoke in support of amendments tabled by JCHR chair Harriet Harman to ensure that the level of protection for journalists in the Bill was the same as exists under the Police and Criminal Evidence Act 1984.[77]

Mr Burnham concluded that:

> We accept that this is a difficult area to get right, particularly when the definition of who is and who is not a journalist is changing in the digital world. We accept the difficulty facing ministers. However, we think that the general principle, enshrined in PACE, of allowing journalists to challenge in open court any attempt to access material that could reveal sources is a good one. It would allow those public interest arguments to be heard and tested in court. We hope that the Government will today commit to working with us and the NUJ to find a wording that in the end does the job.[78]

In response, the Security Minister, John Hayes, said that discussions were ongoing between the Government, the National Union of Journalists (NUJ) and Society of Editors on the protections for journalists.[79] He said that "a solution needs to be found, and I am happy to say that we will look at this issue with him and others in greater detail as the Bill enjoys its passage through this House and the other place".[80]

---

[73] ibid, col 1124.
[74] ibid, col 1116.
[75] ibid, col 1116.
[76] ibid, col 1116.
[77] ibid, col 1117 and col 1131.
[78] HC *Hansard*, 7 June 2016, col 1117.
[79] ibid, col 1118.
[80] ibid, col 1117.

The Solicitor General, Robert Buckland, concluded:

> We have listened to the strength of feeling on the matter and will consider whether further protections, over and above the significant protections that already exist under PACE in relation to journalists themselves, are appropriate where the collateral effect of warranted intrusion discloses their sources.[81]

The Government's amendments were accepted without division. Harriet Harman's amendments were not pushed to a division.

4.3 Public Authorities Entitled to Access Communications Data

The Bill would allow for communications data to be sought by law enforcement, the security and intelligence agencies, local authorities and a number of other public bodies.[82] Local authorities would only seek communications data with the approval of a justice of the peace[83] and are not permitted to acquire ICRs.

At report stage Conservative backbencher Stephen McPartland (MP for Stevenage) proposed probing amendments to restrict access to communications data to only law enforcement and the security and intelligence agencies. He said:

> Schedule 4 currently includes the Food Standards Agency and the Gambling Commission, and I am not clear what evidence there is for including those organisations and granting them access to such intrusive powers when other organisations will not have that access. The Bill gives incredibly wide-ranging powers and there is clear nervousness about that on both sides of the House. I completely respect the integrity of the security services and the police, but a lot of the fear seems to stem from the behaviour of some local authorities in the past and how they have used anti-terrorism powers to spy on people to see whether or not they have been recycling correctly and so on.[84]

SNP Spokesperson Gavin Newlands noted that:

> No fewer than 47 bodies are listed, a reflection of the tightly drawn nature of the Bill—or otherwise. That suggests that access to communications data may be granted for a range purposes, which will almost certainly be disproportionate and inconsistent with the guidance offered by the European Court of Human Rights.[85]

Conservative backbencher Victoria Atkins (MP for Louth and Horncastle) countered this position, arguing that the bodies listed—such as the Department for Work and Pensions, Her Majesty's Revenue and Customs and the Financial Conduct Authority—undertook thousands of prosecutions each year, for which communications data was essential evidence.[86]

---

[81] ibid, col 1138.
[82] Schedule 4 of the Bill lists the public authorities and designated senior officers within them that can seek access to communications data.
[83] In Scotland a sheriff, and in Northern Ireland a district judge.
[84] HC *Hansard*, 7 June 2016, cols 1113–14.
[85] ibid, col 1126.
[86] ibid, cols 1132–3.

In response the Solicitor General said that he would "commit to publishing a detailed case for the minor public authorities ahead of these provisions being further considered in the other place".[87] The amendments were withdrawn by Stephen McPartland.

Fellow Conservative backbencher Will Quince (MP for Colchester) tabled a probing amendment to require applications for communications data by local authorities to be approved by a Judicial Commissioner (rather than a justice of the peace). He said that:

> It will discourage over-zealous officers from applying for authorisations if they know that their chief executives will see those authorisations before they take effect, and, in the event that a council officer is found to have misused the powers, the chief executive will be accountable. Chief executives will never be able to say that they did not know what was happening in their authorities.[88]

In response, the Solicitor General said that the Government "wish to consider the matter further, and return to it in the other place".[89] The amendment was not pressed to a vote.

4.4 Internet Connection Records

Alistair Carmichael, speaking for the Liberal Democrats, argued against the accessing of internet connection records (ICRs). He tabled amendments, supported by the SNP, to remove them from the Bill. In a short speech he said that:

> David Anderson QC described the expanded data collection by internet service providers as "overstated and misunderstood"—to the point and understated. There is no other "Five Eyes" country in which operators have been forced, or are being forced, to retain similar internet connection data. That surely tells us all that we need to know. The case has not been made. It is always open to the Government to come back on some future occasion to make a case and to put these provisions in another Bill. They have not made the case, and the provisions should not be in this Bill.[90]

The amendment was defeated at division by 69 votes to 282.[91]

Andy Burnham acknowledged the need for ICRs as a tool to deal with the changing nature of crime. However he said that:

> There is still a lack of clarity about what exactly can and cannot be included in an ICR, and a risk that if that is not clearly spelled out, there could be drift over the years—they could change and mutate, and become much intrusive. As they are a new construct, it would help to build public trust if the Bill contained a clear definition of ICRs and what they can include.[92]

---

[87] ibid, col 1114.
[88] ibid, col 1131.
[89] ibid, col 1131.
[90] HC *Hansard*, 7 June 2016, col 1135.
[91] ibid, col 1143.
[92] ibid, col 1119.

He tabled an amendment to explicitly state that an ICR could not include content (only communications data) in order to "remove any lingering ambiguity".[93]

Mr Burnham also pressed the Government on the potential use of communications data and ICRs. He said that:

> Communications data should not be capable of being accessed to investigate any crime, regardless of how serious the offence is and the impact on victims […] There should be a clear and simple threshold for the use of communications data—namely, serious crime punishable by at least six months in prison, or crime where significant mental or physical harm could be caused. As I said, given the more intrusive nature of internet connection records, the threshold for their use should be even higher than that.[94]

In response, John Hayes said:

> I commit to doing what the right hon. Gentleman asked. I do so because it is really important that we have a threshold that works, particularly on ICRs. ICRs are, as the right hon. Gentleman says, qualitatively different. He is right about cases of harassment, and so on and so forth, which is why the matter is challenging and complex.[95]

The amendment was not pressed to a vote.

4.5 Request Filter

The Bill proposes that the Secretary of State would operate a filtering arrangement, known as the Request Filter, which the Government says would act as a safeguard for the handling of communications data. The Filter would sit between bodies seeking access to communications data and the CSPs holding the data and would prevent data from being provided to a public authority that is not directly relevant to the request.[96] The operation of the Request Filter will be overseen by the Investigatory Powers Commissioner.

Stephen McPartland tabled amendments in relation to the Request Filter. He described it is as a "highly intrusive search facility" and said that his amendments "try to restrict the use of the filter to exceptional circumstances".[97]

The Solicitor General replied that:

> That is a filter that will be maintained by the Secretary of State. It does not hold data of itself; it is a safeguard. It is there to prevent collateral information being provided to the public authority. It is an innovation and it specifically limits the communications data retained to only that which is relevant. I would argue that the measure is essential because it serves the interests of privacy that have formed such a part of the debates in this House, and it will help to reduce error. The filter will accept only communications data disclosed by communications service providers in response to specific requests from public authorities, each of which must be necessary and proportionate. Any

---

[93] ibid, col 1119.
[94] ibid, col 1119.
[95] ibid, col 1120.
[96] Home Office, *Investigatory Powers Bill Factsheet—Request Filter*, March 2016.
[97] HC *Hansard*, 7 June 2016, cols 1114–15.

> irrelevant data that do not meet those criteria will be deleted and not made available to the public authority.[98]

The amendments were not pressed to a division.

5. Part 5: Equipment Interference

Part 5 of the Bill would allow for targeted equipment interference (EI) to be undertaken by law enforcement and the security and intelligence agencies. Equipment interference is the accessing of equipment (eg computers, mobile phones etc) in order to obtain stored communications and other data.[99]

The authorisation system for targeted EI warrants is largely the same as that for targeted interception warrants (see part 2). Unlike interception warrants, targeted EI warrants for law enforcement could be issued with the consent of a law enforcement chief[100] and a Judicial Commissioner, rather than the Secretary of State and a Judicial Commissioner.

At report stage, the debates on the judicial review test, warrant purposes and modifications that were discussed in relation to part 2 applied to this part as well. Various consequential government amendments were accepted without division to implement the equivalent changes made to part 2.

The Government proposed an amendment to extend the safeguards for Members of Parliament in relation to targeted EI warrants. If a targeted EI warrant is being sought in order to obtain the stored communications or private information of a member of a relevant legislature, the law enforcement chief must get the approval of the Secretary of State and the Prime Minister (as well as a Judicial Commissioner) in order to issue the warrant. The amendment was accepted without division.

Backbencher Stephen McPartland (Conservative MP for Stevenage) questioned the breadth of the EI powers and proposed probing amendments to tighten the definitions of the circumstances in which the powers could be sought. He said:

> The next set comprises amendments 178 to 186, which try to refine the matters to which targeted equipment interference warrants may relate by removing vague and overly broad categories, including equipment interference for training purposes. People outside this place may not be aware of it, but when we talk about "equipment interference", we are basically talking about hacking devices that can hack into mobile phones, computers, e-mail systems, or the apps that people use for their banking. "Equipment interference" is a nice way of saying state-authorised hacking, which is what we are talking about here. To me, this is an incredibly intrusive power, permitting real-time surveillance, as well as access to everything we store on our digital devices, from text messages to address books, calendars and emails, along with the websites people visit, which apps they use and how they use them.[101]

His amendments were not considered further.

---

[98] ibid, col 1137.
[99] Home Office, *Investigatory Powers Bill Factsheet—Targeted Equipment Interference*, March 2016.
[100] Schedule 6 of the Bill sets out the posts which qualify for the authorisation of targeted EI warrants.
[101] HC *Hansard*, 6 June 2016, col 966.

6. Part 6: Bulk Warrants

Part 6 of the Bill would provide for the security and intelligence agencies to be able to apply for warrants to conduct bulk interception, bulk equipment interference and the bulk acquisition of communications data.[102] Bulk interception and bulk EI relate to communications and equipment outside the British islands, while bulk communications data may be collected in relation to people within the UK.

These powers exist in previous legislation but have only recently been avowed by the Government. Bulk interception is provided for under section 20 of the Regulation of Investigatory Powers Act 2000, bulk communications data acquisition in section 94 of the Telecommunications Act 1984 and bulk equipment interference by sections 5 and 7 of the Intelligence Services Act 1994.[103]

6.1 The Operational Case for Bulk Powers

The bulk powers have been one of the most controversial areas of the Bill, with questions raised about the clarity and scope of the powers, their legality, effectiveness, and the safeguards that exist.[104] The Joint Committee on the Draft Investigatory Powers Bill called on the Government to publish a fuller justification for each of the bulk powers alongside the Bill and that the powers should be assessed by an independent body.[105] The ISC in its scrutiny of the draft Bill concluded that the case had not been made for bulk EI warrants.[106]

The Government published an additional operational case document for bulk powers alongside introduction of the Bill,[107] however debates about the powers continued at second reading and committee stage.

Between committee stage and report stage, letters were exchanged between Home Secretary Theresa May and Shadow Home Secretary Andy Burnham. At a debate on the Loyal Address on 24 May 2016, Andy Burnham announced that the Home Secretary had given a commitment for an independent review of the operational case for bulk powers.[108] He said:

> It is not only the right thing to do, but could build trust in the whole process. I am pleased that she has agreed in the letter to look at having a review and has approached David Anderson QC to lead it. The Opposition strongly welcome that development, which we believe will build trust and support behind the Bill.[109]

---

[102] For more information about the bulk powers, see Home Office, *Investigatory Powers Bill Factsheet—Bulk Interception*; *Investigatory Powers Bill Factsheet—Bulk Equipment Interference*; and *Investigatory Powers Bill Factsheet—Bulk Acquisition* (March 2016).
[103] Joint Committee on the Draft Investigatory Powers Bill, *Draft Investigatory Powers Bill*, 11 February 2016, HL Paper 93 of session 2015–16, para 307.
[104] See, for example, Joint Committee on the Draft Investigatory Powers Bill, *Draft Investigatory Powers Bill*, 11 February 2016, HL Paper 93 of session 2015–16, paras 306–74.
[105] Joint Committee on the Draft Investigatory Powers Bill, *Draft Investigatory Powers Bill*, 11 February 2016, HL Paper 93 of session 2015–16, para 319.
[106] Intelligence and Security Committee of Parliament, *Report on the Draft Investigatory Powers Bill*, 9 February 2016, HC 795 of session 2015–16, para D.
[107] Home Office, *Operational Case for Bulk Powers*, March 2016.
[108] HC *Hansard*, 24 May 2016, col 502.
[109] ibid, col 502.

Further letters were then exchanged between Security Minister John Hayes, and Shadow Immigration Minister Kier Starmer about the details of the review.[110] At report stage, Kier Starmer said:

> We know that David Anderson QC will conduct the review. We have great faith in him, as I think do most Members of this House. It is important that the task he is performing is clear. We have argued that he should look not at the utility of the bulk powers but at their necessity, that he should be able to choose a suitably qualified security cleared panel himself to help him, that he must have access to all the material necessary to carry out the review effectively, including, of course, the material made available to the Intelligence and Security Committee, and that he must have time to carry out his review; we envisage that he will report in time for the consideration in Committee in the House of Lords of parts 6 and 7 of the Bill, which should be in about three months.[111]

A terms of reference document for the review was subsequently published[112] and David Anderson QC set out further details of the review on his website.[113] The review will include the issue of bulk personal datasets (part 7 of the Bill).

The announcement of the review was sufficient for Labour not to oppose the inclusion of bulk powers at report stage. However, Anne McLaughlin, speaking for the SNP, said that it did not satisfy her Party:

> The review the Government have agreed to is most welcome but they must get it right. It must be conducted properly if it is to be of any value to the process of parliamentary scrutiny or is to secure the public's confidence in its conclusions […] The review needs to be given the time to do a thorough job, however, and we simply do not believe that three months is long enough […] I would argue that the review should have happened before now. Even if it is completed within three months, that will not be while scrutiny of the Bill is taking place here by elected Members; the scrutiny will be in the other place by Members of the House of Lords, who are not elected.[114]

The SNP called for parts 6 and 7 of the Bill to be shelved "until such time as an argument for their inclusion has been demonstrated by an independent review of their proportionality and operative necessity"[115] and tabled amendments to that effect. Anne McLaughlin argued that, given a review of the powers of the National Security Agency (NSA) in America had concluded that similar powers were not essential to preventing attacks, that Members should be "circumspect about trusting this Government with their votes".[116] She concluded that:

> When we are dealing with proposals that are so broad—the proposal is effectively for bulk data harvesting from mainly innocent citizens—it is incumbent on the Government to prove that there is an operational case and that the powers are necessary, and to ensure that the safeguards in place are rigorous. The Government have neither proven

---

[110] Letter from Kier Starmer to John Hayes, 6 June 2016 and Letter from John Hayes to Kier Starmer, 6 June 2016, DEP2016-0549.
[111] HC *Hansard*, 6 June 2016, col 883.
[112] Home Office, *Independent Review of the Operational Case for Bulk Powers: Terms of Reference*, 7 June 2016.
[113] Independent Reviewer of Terrorism Legislation, 'Bulk Powers Review Announced', 7 June 2016.
[114] HC *Hansard*, 7 June 2016, cols 1053–4.
[115] ibid, col 1053.
[116] ibid, col 1055.

> the operational case for the powers nor have they delivered safeguards and oversight of sufficient calibre to make the powers justifiable.[117]

In response, ISC chair Dominic Grieve said:

> In an ideal world, it would always be better if we used targeted interception. If we know what it is we are trying to intercept and have reasonable grounds that are necessary and proportionate for doing so, then clearly that is what we should be aiming to do. The reality, however, is that the use of the internet today, in respect of the transfer of information, is of such an order that if there were not bulk powers to enable the agencies to look to intercept bulk and then search it to find what they are looking for, it would in practice be very difficult for the agencies to defend our security against espionage and, in particular, terrorism. That is the reality […] the idea that there is bulk harvesting of data in order to carry out a detailed examination of them is, in fact, fanciful. That is not what is happening. What is happening is that there may be the retention of a bulk group of data in which in reality the vast majority—in fact, probably over 99 percent—will never be looked at, except in so far as it exists as a few digits on a screen. Ultimately, the agencies are interested in the nugget—or, as he described it, the needle in the haystack—that they are actually looking for. The idea that the privacy of an individual will be compromised if it just so happens that their internet traffic is caught in that particular net is simply not real.[118]

The Security Minister, John Hayes, in his summing up said that:

> The point is not whether the powers are necessary, it is whether we can put in place sufficient safeguards to ensure that they are used only when, how and where they should be. That was the point made by the chair of the ISC and by the ISC when it had the chance to consider these matters. As the chair of the ISC said, it then also had a chance to reconsider them, having been given further information of a secure kind—that is its function after all—and its members were persuaded that the powers were indeed necessary. It is right to have an informed, thoughtful debate about safeguards, checks and balances, and constraints, but we cannot have a grown-up debate about whether the powers count, because they are not new; they are existing powers. The Bill simply introduces additional safeguards, which I would have thought any reasonable Member would welcome.[119]

The SNP amendment to remove parts 6 and 7 of the Bill was defeated by 66 votes to 285.[120]

6.2 Operational Purposes for Bulk Powers

Dominic Grieve proposed a series of amendments to require the security and intelligence agencies to maintain a designated list of operational purposes for the bulk powers, agreed with the Secretary of State and shared with the IPC. Any application for a bulk warrant would then have to specify one of those purposes.

---

[117] HC *Hansard*, 7 June 2016, col 1056.
[118] ibid, col 1059.
[119] ibid, col 1095.
[120] ibid, col 1101.

The amendments also required that the list of operational purposes be reviewed annually by the Prime Minister and a summary of those purposes published each year. The ISC and the Judicial Commissioners would be notified of any changes to the list.

In the debate, Dominic Grieve said that:

> In the ISC's report on the draft Bill, we were critical of what appeared to us to be the lack of transparency around operational purposes, which are of the utmost importance […] as they provide the justification for examining material collected using bulk powers. If it falls outside legitimate operational purposes, one cannot examine it […] Our amendments are therefore intended to give effect to our original recommendations for greater scrutiny and transparency, while also trying to create a formal mechanism for the establishment, management, modification and review of the list of operational purposes.[121]

In response, the Security Minister, John Hayes, said: "I am absolutely committed to considering the matter in the way he describes, and I am prepared to say now that we will go away and consider his amendments, with a view to introducing further amendments to the Bill to satisfy him and his Committee on this issue".[122]

Mr Grieve said that he was grateful to the Minister, that he would consider his proposals to be probing amendments and that he hoped "the matter can be properly resolved as the Bill goes through another place".[123]

6.3 Modifications to Bulk Warrants

Conservative backbencher Stephen McPartland (MP for Stevenage) proposed amendments to remove the clauses in the Bill that would allow for the modification of bulk warrants. He said that these were probing amendments and that, following the remarks from the Security Minister the day before about modifications (see the debate on modifications and renewals on part 2) he was reassured that the Government's position and amendments helped to address his concerns on this issue.[124]

Government amendments on the serving and modification of, and safeguards for, bulk warrants were approved without division. Many of these were equivalent to or consequential from the debate on modifications on part 2 of the Bill.

7. Part 7: Bulk Personal Dataset Warrants

Part 7 of the Bill would allow the security and intelligence agencies to apply for warrants to acquire and retain bulk personal datasets (BPDs). BPDs are large datasets containing information about a wide range of people, most of whom are not of interest to the agencies. Examples include lists of people who have a passport or a licensed firearm.[125]

---

[121] HC *Hansard*, 7 June 2016, col 1061.
[122] ibid, col 1061.
[123] ibid, col 1063.
[124] ibid, col 1091.
[125] Home Office, *Investigatory Powers Bill Factsheet—Bulk Personal Datasets*, March 2016, p 1.

The Bill provides for two types of BPD warrant; specific BPD warrants for particular datasets and class BPD warrants for any dataset of a certain type.

Along with the bulk powers, the SNP proposed the removal of part 7 of the Bill as they argued that there was not a satisfactory operational case for the power (see discussion on part 6).

Dominic Grieve said that the ISC "have seen the entire list of bulk personal datasets and we have never been of the opinion that anything is being collected that is not legitimate, and some of it, I can tell the House, is pretty mundane as well".[126]

7.1 Class BPD Warrants

Dominic Grieve explained that the ISC had recommended the removal of class BPD warrants from the Bill, as the potential intrusion into privacy was too great and that specific approvals for specific datasets was more appropriate.[127] He said that, however:

> We then had further evidence—as has happened in the dialogue with the Government and the agencies—in particular from the Secret Intelligence Service, about the rationale for retaining class warrants in the Bill. In particular, the evidence highlighted the fact that many of these datasets covered the same information or type of information. In those circumstances, we considered that a class warrant would be appropriate, as the privacy considerations were identical.[128]

Mr Grieve said that, in order to accept class BPD warrants, further restrictions were required. He proposed a new clause which would prevent datasets including sensitive personal data (using the definitions in the Data Protection Act 1998, ie data on a person's race, political opinions, religious beliefs, trade union membership, physical or mental health, or sexual life) from being acquired or retained under a class BPD warrant. The new clause also sought to exclude "novel or out of the ordinary" datasets from class warrants and to put a limit on the number of individual datasets:

> We should not end up with bulk personal dataset inflation and have suggested that bulk personal dataset warrants should be limited to 20 individual datasets. I emphasise to the House that that is a completely arbitrary figure in many ways. If the Government have an alternative approach, I am more than happy to listen. I accept that if we impose a limit of 20, it is possible that the Home Secretary might be asked to sign two identical bulk personal dataset warrants in one go, if they are expecting to pick up 40. However, it seems to me that there needs to be some numerical cap, above all to ensure that the Home Secretary or Foreign Secretary, depending on who it is, is aware of what is being collected.[129]

In response, the Security Minister, John Hayes, said that:

> The Government certainly accept in principle the argument that we should provide further restrictions on the use of class bulk personal dataset warrants. We also accept

[126] HC *Hansard*, 7 June 2016, col 1063.
[127] ibid, col 1063.
[128] ibid, col 1063.
[129] HC *Hansard*, 7 June 2016, col 1063.

> much of the detail contained in the ISC's draft clause, including reference to the need for restrictions relating to sensitive personal data.[130]

He also said that "it would be undesirable to set an arbitrary figure" on the number of datasets within a class BPD warrant but that the argument "is not without merit. I am not sure that this is a matter to be dealt with on the face of the Bill, but it certainly should be dealt with".[131]

The amendments were not considered further.

7.2 Medical Records

At report stage, Kier Starmer raised the issue of BPDs including medical records. He said:

> There has been an ongoing concern, raised first by the Scottish National Party and then by Labour in Committee, about access to medical records. The concern for Labour, which I am sure is the shared position, has been about "patient information", as defined by section 251 of the National Health Service Act 2006. That means information relating to mental health, adult social care, child social care and health services. I do not need to spell out for the House why many members of the public—my constituents and, I am sure, those of many Members—are deeply concerned about the very notion of the security and intelligence services having bulk access to those sorts of sensitive records.[132]

The Government had tabled a new clause to address health records in BPDs, requiring additional steps to be taken when making an application for a specific BPD warrant relating to health records and also stating that the Secretary of State may only issue the warrant if he or she "considers that there are exceptional and compelling circumstances that make it necessary".

Kier Starmer concluded that the Government's clause responded to his demands and said he would not press his amendments to a vote.[133] The Government's clause was accepted without division.

8. Part 8: Oversight Arrangements

Part 8 of the Bill would provide the structure for the authorisation and oversight of investigatory powers. The Bill creates a new Investigatory Powers Commissioner (IPC), supported by a team of Judicial Commissioners, all of whom must hold or have held high judicial office.

The IPC will have a broad remit to scrutinise and review the operation of investigatory powers. The oversight role of the IPC replaces the roles and functions currently exercised by the Intelligence Services Commissioner, the Interception of Communications Commissioner and the Chief Surveillance Commissioner.

---

[130] ibid, col 1098.
[131] ibid, col 1063.
[132] ibid, cols 1071–2.
[133] ibid, col 1071.

The IPC and Judicial Commissioners would be appointed by the Prime Minister following consultation with the Lord Chief Justice of England and Wales, the Lord President of Scotland, the Lord Chief Justice of Northern Ireland, the Scottish Ministers, and the First Minister and Deputy First Minister in Northern Ireland. The IPC would report annually to the Prime Minister, and would be able to report on other matters as he or she deemed necessary, or as requested by the Prime Minister.

8.1 Appointment of Judicial Commissioners

At report stage the process of appointing the Judicial Commissioners by the Prime Minister was raised by Keir Starmer. He said that "it is not appropriate for the Prime Minister to decide that sort of deployment—he does not have the skills and experience to do it—nor, in a sense, should it be a political deployment. This is something routinely done by the Lord Chief Justice of England and Wales".[134] He proposed an amendment that would require the Prime Minister to act upon the recommendation of the Lord Chief Justice in appointing the Commissioners.

In response, the Solicitor General, Robert Buckland, said:

> I listened carefully to the arguments, and I agree that there is real merit and value in providing expertise from the heads of the judiciary in the appointment process. I also believe that there is a role for the Lord Chancellor in these appointments. He has responsibility for ensuring that the Courts and Tribunals Service has enough judges to operate effectively. Given the limited number of High Court judges, these appointments could affect that. Involving the Lord Chancellor in making a recommendation on appointment would help to avoid any accusations of judicial patronage. On the basis that we will table an amendment in the other place to fulfil that aim, I invite the hon and learned Gentleman to withdraw his amendments.[135]

The amendment was not considered further.

8.2 Separation of Authorisation and Oversight Functions

JCHR chair Harriet Harman tabled an amendment on behalf of the Committee proposing that the Judicial Commissioner undertaking the authorisation of warrants be separate from those conducting oversight of the use of the investigatory powers. She said that it "is a problem to have the same person both carrying out approval of a warrant and overseeing their approval of the warrant"[136] and proposed that "there should at the very least be Chinese walls" between them.[137] She was supported in this view by SNP Spokesperson for Justice and Home Affairs Joanna Cherry.[138]

In response, the Solicitor General, Robert Buckland, argued that David Anderson QC had said that there should be a relationship between the judicial authorisation function and the inspectorate, and though there needs to be distance between them "creating the sort of division envisaged in the amendment would break the important link that exists to allow those

---

[134] HC *Hansard*, 6 June 2016, col 890.
[135] ibid, col 922.
[136] HC *Hansard*, 6 June 2016, col 904.
[137] ibid, col 905.
[138] ibid, col 900.

who review fully to understand how the process works in practice".[139] He said that the Government would resist the amendment, however time in the session ran out before it could be reached.

8.3 Creation of an Investigatory Powers Commission

The SNP also moved an amendment to create a body called the Investigatory Powers Commission, within which the Investigatory Powers Commissioner and Judicial Commissioners would operate. This echoed the conclusion of the Joint Committee on the Draft Investigatory Powers Bill which said:

> It is unclear to us why the Home Office chose to create a group of Judicial Commissioners rather than creating an Independent Intelligence and Surveillance Commission as recommended by David Anderson QC, a recommendation endorsed by the knowledgeable and experienced Interception of Communications Commissioner's Office. The benefits of having a senior independent judicial figure in the Investigatory Powers Commissioner would not be lost by putting the IPC at the head of a Commission. The evidence we have heard is that the work of the oversight body will be significantly enhanced by the creation of a Commission with a clear legal mandate. We recommend that such a Commission should become the oversight body in the Bill.[140]

In response, the Solicitor General said he was "not persuaded that the creation of an independent non-departmental public body—namely the investigatory powers commission—would add anything to the thrust of reforms that we are already undertaking, other than cost to the taxpayer".[141] The amendment was defeated at division by 64 votes to 281.[142]

8.4 IPC Remit and Role of the ISC

Dominic Grieve moved two amendments on behalf of the ISC. The first added a requirement that the IPC scrutinise the underlying safeguards, procedures and processes relating to bulk powers, including the arrangements for the protection of, and control of access to, material obtained through their use. The second allowed the Prime Minister to issue directions to the IPC at the request of the ISC. Both amendments were accepted by the Government without division.

A government amendment to extend the oversight of the IPC to include the work of prison governors in relation to preventing the illegal use of mobile phones in custodial institutions was also passed without division. John Hayes acknowledged that this amendment responded to the issue raised by SNP Spokesperson for Justice and Home Affairs Joanna Cherry at committee stage.[143]

---

[139] ibid, col 922.
[140] Joint Committee on the Draft Investigatory Powers Bill, *Draft Investigatory Powers Bill*, 11 February 2016, HL Paper 93 of session 2015–16, para 574.
[141] HC *Hansard*, 6 June 2016, col 922.
[142] ibid, col 928.
[143] HC *Hansard*, 6 June 2016, col 879.

8.5 Protection for Whistleblowers and Notifications for Subjects of Investigatory Powers

The SNP also proposed an amendment to give protection from criminal prosecution to whistleblowers. Joanna Cherry said that the amendment "reflects our concern that provisions in the Bill may inadvertently risk discouraging or preventing individuals within public authorities or agencies, or in communication services providers, from approaching the Investigatory Powers Commissioner with concerns or communicating with the commission frankly".[144]

In response, the Solicitor General, Robert Buckland, said that he was "happy to consider how to make it absolutely clear that whistleblowers can make disclosures to the IPC without fear of prosecution" and that he would "consider how to amend the Bill to bring even greater clarity to that issue".[145] The amendment was defeated at division by 67 votes to 281.[146]

The SNP also proposed a new clause to require the IPC to notify individuals if they had been the subject of one of the investigatory powers in the Bill (and some powers in other legislation) after the authorised action had taken place. It was defeated at division by 64 votes to 278.[147]

9. Part 9: Miscellaneous and General Provisions

Part 9 of the Bill covers various miscellaneous powers and details. It includes provisions to allow the Secretary of State to serve national security notices and technical capability notices on communications service providers (CSPs). National security notices require a CSP to take such actions that the Secretary of State considers necessary in the interests of national security, while technical capability notices require the CSP to ensure that it has the capability in place to provide assistance that may be requested under other warrants.

Part 9 also includes a provision requiring the Secretary of State to review the operation of the Act five years after it is passed.

9.1 Judicial Authorisation for Notices

At report stage, the Government introduced a new clause and consequential amendments to subject the issuing of notices to the 'double lock' authorisation process, with the approval of a Judicial Commissioner required alongside that of the Secretary of State. Another amendment made explicit that, in the event of a national security notice presenting conflicting legal duties on a CSP in relation to the Communications Act 2003, the requirements of the notice must be complied with. These amendments were accepted without division.

9.2 Notices and Encryption

Technical capability notices had been an issue of concern during the scrutiny of the Bill, as they would allow for "obligations relating to the removal by a relevant operator of electronic protection applied by or on behalf of that operator to any communications or data". Concerns

---

144 ibid, col 901.
145 ibid, col 922.
146 ibid, col 931.
147 ibid, col 925.

had been raised that a requirement to remove electronic protection would mean that CSPs could be required to break or undermine the encryption used to secure and safeguard data on their networks.[148]

The Home Secretary told the Joint Committee on the Draft Investigatory Powers Bill that:

> We are not proposing in the Bill to make any changes in relation to the issue of encryption and the legal position around that. The current legal position in respect of encryption will be repeated in the legislation of the Bill. The only difference will be that the current legal position is set out in secondary legislation and it will now be in the Bill. We say that, where we are lawfully serving a warrant on a provider so that they are required to provide certain information to the authorities, and that warrant has gone through the proper authorisation process and is entirely lawful, the company should take reasonable steps to ensure that it is able to comply with the warrant that has been served on it. That is the position today, and it will be the position tomorrow under the legislation.[149]

The Joint Committee recommended that the Bill be amended to make this clear and that the Government should clarify that CSPs providing encrypted communication services should not be expected to decrypt them if it is not practicable to do so.[150]

At report stage, the Government tabled an amendment to clarify that national security notices could not require companies to remove encryption.[151] The amendment was accepted without division.

10. Third Reading in the House of Commons

Speaking at third reading, the Home Secretary, Theresa May, said:

> The first duty of Government is the protection of their citizens, and the first duty of Parliament is to hold the Government to account for the way they protect those citizens. This landmark Bill will ensure that our police and security and intelligence agencies have the powers they need to keep us safe in an uncertain world. It provides far greater transparency, overhauls safeguards and adds protections for privacy. It also introduces a new and world-leading oversight regime. It is a vital Bill—on that, we are agreed across the House.[152]

---

[148] For further information about the debate on encryption, see Joint Committee on the Draft Investigatory Powers Bill, *Draft Investigatory Powers Bill*, 11 February 2016, HL Paper 93 of session 2015–16, paras 248–64. For information about the breaking of encryption see, Parliamentary Office of Science and Technology, *Data Encryption*, 15 March 2016.
[149] Joint Committee on the Draft Investigatory Powers Bill, *Draft Investigatory Powers Bill*, 11 February 2016, HL Paper 93 of session 2015–16, para 262.
[150] Joint Committee on the Draft Investigatory Powers Bill, *Draft Investigatory Powers Bill*, 11 February 2016, HL Paper 93 of session 2015–16, paras 263–64.
[151] HC *Hansard*, 6 June 2016, col 951.
[152] HC *Hansard*, 7 June 2016, col 1145.

Theresa May said that the Bill had received "unprecedented scrutiny" and she commended the Opposition for its responsible and constructive approach to the issues.[153] She also acknowledged that further changes would be made:

> It is because we continue to listen that we have committed to make further changes when the Bill enters the Lords. Responding to another suggestion from the official Opposition, we will introduce a threshold for access to internet connection records, to put beyond doubt that those vital powers cannot be used to investigate minor crimes. We will introduce an amendment to respond to the Opposition proposal on the important appointment of the Investigatory Powers Commissioner. We have also committed to implement a number of further reforms proposed by the ISC.
>
> I look forward to the continued careful scrutiny the Bill will receive in the other place, but the key message their lordships should take from the last two days of debate is that this House supports the Bill. We have before us a world-leading piece of legislation, which has been subject to unparalleled scrutiny, and which now, I hope, commands cross-party support.[154]

Andy Burnham concluded that "the Bill leaves this House in a much better state than we found it" but that it would still need the changes promised by the Home Secretary.[155] He said that "if the Government continue with the same approach as the one they have adopted in recent weeks, I have every confidence that we will get there".[156]

Joanna Cherry said that:

> This is one of the most lengthy and complex Bills that the House has debated for many years. The powers it seeks to give to the state are immense and far-reaching. The Bill is of huge constitutional significance, yet we have had fewer than two full working days to debate it on Report. Accordingly, the number of amendments that could be put to a vote was just a very small proportion of the number tabled.[157]

She argued that the assurances provided by the Government were not sufficient and that the SNP would take a principled stand and vote against the Bill.[158] Alistair Carmichael for the Liberal Democrats agreed, and said "It would be an abdication of our responsibility as Opposition MPs to vote for it".[159]

The motion that the Bill be read a third time was passed by 444 votes to 69.[160]

---

153 ibid, cols 1146–7.
154 ibid, col 1146.
155 ibid, cols 1147–8.
156 ibid, col 1148.
157 ibid, col 1148.
158 HC *Hansard*, 7 June 2016, col 1149.
159 ibid, col 1153.
160 ibid, col 1156.