PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

INVESTIGATORY POWERS BILL

Eighth Sitting

Tuesday 19 April 2016

(Afternoon)

CONTENTS

No proofs can be supplied. Corrections that Members suggest for the final version of the report should be clearly marked in a copy of the report—not telephoned—and must be received in the Editor's Room, House of Commons,

not later than

Saturday 23 April 2016

The Committee consisted of the following Members:

Chairs: Albert Owen, † Nadine Dorries

† Atkins, Victoria *(Louth and Horncastle)* (Con)
† Buckland, Robert *(Solicitor General)*
† Cherry, Joanna *(Edinburgh South West)* (SNP)
† Davies, Byron *(Gower)* (Con)
† Fernandes, Suella *(Fareham)* (Con)
† Frazer, Lucy *(South East Cambridgeshire)* (Con)
† Hayes, Mr John *(Minister for Security)*
† Hayman, Sue *(Workington)* (Lab)
† Hoare, Simon *(North Dorset)* (Con)
† Kinnock, Stephen *(Aberavon)* (Lab)
† Kirby, Simon *(Brighton, Kemptown)* (Con)
† Kyle, Peter *(Hove)* (Lab)
† Matheson, Christian *(City of Chester)* (Lab)
† Newlands, Gavin *(Paisley and Renfrewshire North)* (SNP)
† Starmer, Keir *(Holborn and St Pancras)* (Lab)
† Stephenson, Andrew *(Pendle)* (Con)
† Stevens, Jo *(Cardiff Central)* (Lab)
† Warman, Matt *(Boston and Skegness)* (Con)

Glenn McKee, Fergus Reid, *Committee Clerks*

† attended the Committee

Public Bill Committee

Tuesday 19 April 2016

(Afternoon)

[Nadine Dorries *in the Chair*]

Investigatory Powers Bill

2 pm

The Chair: This will be a long session: five hours. If anyone is worried about comfort breaks, I do not have the constitution of Mr Speaker, so I will call one at around 4 o'clock or 4.15 pm. We are then expecting a vote on a programme motion at around 6 o'clock. That will, I hope, break it up nicely.

The Minister for Security (Mr John Hayes): On a point of order, Madam Chairman. I mentioned at the outset this morning that I had written to you and intended to make copies of that correspondence available to Committee members. In the course of the proceedings, I heard the Solicitor General report that I had also written to journalists. Hard copies of all that correspondence are available at the front of the room for collection by members, and I understand that it has also been sent to members by email.

The Chair: Thank you very much.

Clauses 70 and 71 ordered to stand part of the Bill.

Clause 72

Lawfulness of conduct authorised by this Part

Joanna Cherry (Edinburgh South West) (SNP): I beg to move amendment 246, in clause 72, page 57, line 35, leave out from "subsection (1)" to end of line 40.

This amendment ensures that if conduct cannot be justified it must remain unlawful.

The Chair: With this it will be convenient to discuss amendment 148, in clause 72, page 57, line 36, leave out paragraph (b).

Joanna Cherry: I think I can take this in fairly short compass. The clause deals with the lawfulness of conduct authorised by this part of the Bill. The amendment would delete clause 72(2)(b), the effect of which would be that conduct would have to remain unlawful if it could not be justified. As it is currently worded, the clause allows an exception to that principle, and that is not an appropriate exception. Conduct is either lawful or unlawful. If it is unlawful, it should be characterised as such and should not be justified. Strictly, if the amendment were to be passed, subsection (3) would have to be left out as well, for tidying-up purposes.

The Solicitor General (Robert Buckland): May I reassure the hon. and learned Lady that the provisions relating to lawfulness of conduct authorised by part 3 of the Bill replicate those that currently apply in the Regulation of Investigatory Powers Act 2000, and the Bill goes no further in providing indemnity from civil liability for conduct incidental to or reasonably undertaken in connection with a communications data authorisation? The clause is drafted to ensure that a person who engages in conduct only in connection with an authorisation cannot be subject to civil liability unless that activity could itself have been authorised separately under a relevant power. It must follow that the removal of that provision would mean that a person who was acting lawfully under an authorisation that had properly been granted under the Bill would be at risk of civil liability if some incidental or reasonably connected conduct were not expressly covered by the authorisation.

I can see the thrust of the hon. and learned Lady's argument, but I hope that I have reassured her that the Bill does not go any further than the status quo. For that reason, I urge her to withdraw the amendment.

Joanna Cherry: I beg to ask leave to withdraw the amendment for the time being.

Amendment, by leave, withdrawn.

Clause 72 ordered to stand part of the Bill.

Clause 73 ordered to stand part of the Bill.

Clause 74

Certain transfer and agency arrangements with public authorities

Question proposed, That the clause stand part of the Bill.

Keir Starmer (Holborn and St Pancras) (Lab): There are matters relating to this clause on which I would like to press the Minister. This is the clause that provides for what is effectively the transfer of certain functions between the Secretary of State and other public authorities. The functions to be transferred are the functions in clauses 58 to 60, at which we looked in some detail last week: the filtering arrangements for obtaining data. As set out in clause 58, it is for the Secretary of State to maintain and operate arrangements. It is then for the relevant public authority, acting through a designated senior officer, to effectively carry out the exercise, using authorisations as and where necessary and appropriate. We discussed that arrangement.

Clause 74 provides for a transfer of functions of the Secretary of State—which I take to include establishing, maintaining and operating arrangements—from the Secretary of State to another public authority. That seems to me to cut through the thrust and the purpose of clause 58, which has a clear hierarchy to it: the Secretary of State, then the designated senior officer. Subsection (1)(b) is freestanding and transfers any function exercisable by a public authority back the other way to the Secretary of State, so there is a complete provision for a swap of roles. Subsection (3) indicates that:

"Regulations under subsection (2) do not affect the Secretary of State's responsibility for the exercise of the functions concerned".

Then schedule 5, in the back of the Bill, is referred to, but that does not add a great deal.

The question for the Minister is: how it is anticipated that these powers are to be exercised? On the face of it, this is an odd structure for a Bill to set out. This

structure goes from the Secretary of State down to the relevant public authority, with the Secretary of State having a much wider role of setting up the arrangements, only for us to find, several clauses later, that it is possible to flip the functions and have the public authority making the arrangements. That seems to remove some of the formality and the safeguards intended by clause 58.

Mr Hayes: The hon. and learned Gentleman, with his typical diligence—which is at least matched, by the way, by those on the Treasury Bench—has identified, quite properly, both the reasons for this clause and the character of the transfer of arrangements that it details. He accurately identified subsection (3), which emphasises that:

"Regulations under subsection (2) do not affect the Secretary of State's responsibility for the exercise of the functions concerned".

The transfer of arrangements will change neither the Secretary of State's responsibility nor the process for authorising requests for data. It is about the technical running of the filtering capability. It is there to require flexibility; it might be appropriate at some future point for another authority to exercise the filtering function, but without responsibility moving from the Secretary of State. The Secretary of State will retain responsibility, but the operational running of the filter might change over time. This is essentially about future proofing.

Keir Starmer: I am grateful to the Minister. I am not being pernickety; I just want to be clear. Subsection (3) appears to apply only to regulations under subsection (2), which I think is about changing the powers of public authorities lest they should not have the power to carry out functions on behalf of the Secretary of State. In other words, when the Secretary of State is modifying the powers available to a public authority, that comes within subsection (3). On reflection, I wonder whether sub-clause 3 should say "regulations under subsections (1) and (2) do not affect the Secretary of State's responsibility", because I think that is the thrust of what the Minister said.

Mr Hayes: That is not an unreasonable point, actually. Someone who read the Bill could certainly come to the same conclusion as the hon. and learned Gentleman. I will look at that from a drafting perspective, because it is important that we are clear. First, in all these matters, filtering arrangements take effect only as the result of a lawful process; the process for permission will not change. Secondly, that permission rests with the Secretary of State; I do not want there to be any ambiguity—as the hon. and learned Gentleman suggests there might be—about which parts of this clause that affects. On re-reading the clause, I can see what he means, so I am happy to take it away and check whether the drafting needs to be amended in the way that he describes. In that spirit, and with that immensely generous offer, I hope we can move on.

Keir Starmer: I am grateful.

Question put and agreed to.

Clause 74 accordingly ordered to stand part of the Bill.

Schedule 5 agreed to.

Clause 75 ordered to stand part of the Bill.

Clause 76

EXTRA-TERRITORIAL APPLICATION OF PART 3

Keir Starmer: I beg to move amendment 150, in clause 76, page 59, line 26, after "Kingdom", insert

"the notice shall be served at that person's principal office outside the United Kingdom where it is established for the provision of services. Where it is considered unfeasible or inappropriate in the circumstances,".

The Chair: With this it will be convenient to discuss amendment 151, in clause 76, page 59, line 39, leave out subsection (4) and insert—

"(4) Subsections (1) or (2) of section 57 shall not be applicable where the taking of any steps by a relevant operator outside the United Kingdom—

(a) would cause the operator to act contrary to any laws or restrictions under the law of the country or territory where it is established, for the provision of services, or

(b) could be achieved via a notice served pursuant to an international mutual assistance agreement or subject to an EU mutual assistance instrument.".

Keir Starmer: We return to familiar territory here, in relation to the extraterritorial application of authorisations under part 3. When I made my observations last week, I outlined the concerns that a number of service providers and tech companies have; I do not intend to repeat them.

Amendment 150 would tighten the service provisions in relation to the extraterritorial application of part 3. Amendment 151 would introduce a restriction that had the effect of not requiring a relevant operator outside the UK

"to act contrary to any laws or restrictions under the law of the country or territory where it is established, for the provision of services,"

or to take steps that

"could be achieved via a notice served pursuant to an international mutual assistance agreement or subject to an EU mutual assistance instrument."

We reached this point last week in relation to provisions that were not dissimilar. The Minister made various points, both about service and about other provisions—particularly those relating to the way international mutual assistance agreements currently work. I will not press these amendments to a vote, for the same reasons as last week, but would indicate that the thrust and purpose of the amendments was to anticipate the agreements on extraterritorial application that it is hoped will be reached—particularly with the US—and that are being negotiated at the moment.

2.15 pm

Let me make one or two of the wider points that came up in discussion last week and that, in fairness, I ought to deal with. When we debated equivalent provisions last week, the hon. Member for Louth and Horncastle pointed out that some of the concerned companies and service providers had not given oral evidence to the Joint Committee on the Draft Investigatory Powers Bill. She will be pleased to know that they are all listening to our proceedings or reading the transcripts and paying keen attention. They were keen to point out

that it was not a refusal of principle; they were given very short notice and were asked to come as a team on the same day and at the same time, which was not available to them. I am simply putting their points. They did submit strong written evidence. They later discovered that the Committee took some evidence by Skype, but that was not offered to them.

Victoria Atkins (Louth and Horncastle) (Con): The hon. and learned Gentleman will appreciate I was not chairing the Committee, so this is very much my own impression of what went on. Lord Murphy was, as one would expect, very keen to accommodate the service providers and the Committee Clerks proposed several dates. We were grateful for the written evidence and formed the view we did, but it would have been nice if they could have fitted us into their busy schedules.

Keir Starmer: We probably will not gain much by arguing the detail, particularly as I was not there. The point that the service providers wanted to get across was that in principle they did want to give evidence. They gave written evidence. It was simply that the dates would not work for them as a group, rather than any unwillingness to share their concerns.

The Minister for Security raised a point about the Sheinwald arrangements and the progress being made. As I said a moment ago, these amendments are intended to foreshadow the—I hope—new world of working arrangements, which will cover not only evidence for use in prosecutions but the facilitation of the exercise of powers of this Bill in much faster time than some of the current mutual assistance agreements. The Minister made a further point about the differing views of the companies concerned. There are different views about some aspects of the Bill, but on the issues of extraterritorial application they speak with one voice.

There is an important broader issue to put on the table. As we move forward to international agreements, particularly with the US, it is very important that not only our Government but the US Government are comfortable with the arrangements, because whatever arrangements are put in place will be reciprocal.

Finally, may I hand a schedule to you, Ms Dorries, to the Minister and his team and to the hon. and learned Member for Edinburgh South West? I do not intend to speak at great length to this document, which was prepared for me. What it points out is the inconsistency in approach on extraterritorial jurisdiction. It is quite telling in a number of respects. It tracks whether there is extraterritorial jurisdiction, which clauses give rise to it, whether there is a reasonableness test or a reference to conflict of laws built in, whether it is enforced by overseas service providers, whether there is an international mutual assistance framework and whether there is an obligation on the Secretary of State to consult. What struck me when I went through the document was the inconsistencies. If they are intentional inconsistencies that can be defended, all well and good. I am simply bringing it to the Minister's attention that we have found these apparent inconsistencies. If they are not intentional, it might be a good idea if somebody looked at them to tidy up the provisions and ensure that where they should be consistent, they are.

Lucy Frazer (South East Cambridgeshire) (Con): I am looking at the hon. and learned Gentleman's amendment 150, and of course it is necessary to serve someone so that they get notice. The provisions of service are always about the substance of whether the person gets the notice. It is clear to me from the current drafting that if there were service in accordance with any of clause 76(3), the company would get notice. I have a few concerns about the amendment. I am very wary, because people often take points of service to disrupt a substantive issue. It would be unfortunate if people could take the point that they were not properly served and therefore not comply. Does "principal office" have a meaning in other jurisdictions? If there are different services, will "provision of services" cause confusion? What is the meaning of "unfeasible or inappropriate" and how will it be applied? I believe that the clause will maintain what is desired, which is that it will come to the company's attention, so I am slightly concerned about the amendment.

Keir Starmer: I am grateful to the hon. and learned Lady for her intervention. I am not pressing amendments 150 and 151. They have been put forward to draw attention to concerns. The hon. and learned Lady made submissions last week about service in relation to civil proceedings under the White Book, which I noted and could see the sense of. I do not want to push amendment 150 and accept that "unfeasible" and "inappropriate" may not be the best way to articulate the point.

What underlies both amendments is a genuine concern on the part of those who, when the Bill receives Royal Assent, will be called on to assist in relation to warrants and who want clarity on how the procedure is to operate, what they are to do and what the safeguards are, in particular when they find themselves, as we mentioned last week, required under penalty of criminal proceedings in this country to do something that constitutes an offence in the country in which they are operating. That is a very real concern for them.

Mr Hayes: I shall deal as pithily as is possible with the points the hon. and learned Gentleman made. The first was his helpful contribution in the form of this schematic, to which I will not respond now. He would not expect me to as I have only just seen it. It might form part of my next letter to the Committee to explain why in different parts of the Bill these matters are handled in different ways. In doing so, I will implicitly consider his point about whether that is healthy eclecticism or unhappy inconsistency.

Secondly, it is important to point out that clause 76 essentially maintains provisions on extraterritoriality as they are now, replicating the arrangements under RIPA, clarified by the Data Retention and Investigatory Powers Act 2014. The hon. and learned Gentleman is right, but there is nothing new here.

Thirdly, there is a need to retain flexibility about where the notices are served. I take the hon. and learned Gentleman's point that companies may take a view on these things, and sometimes those might be overlapping or conflicting views about different aspects of the Bill, but in those terms it is important to maintain a degree of flexibility about the communications data notice and where it can be delivered.

Fourthly, on the hon. and learned Gentleman's point about coming more speedily to an agreement that is more satisfactory than either current arrangements or those that might be delivered through a mutual legal assistance treaty, I can offer the Committee the assurance, as I have previously, that that work is under way. We are hopeful—indeed, confident—that we can achieve the sort of outcome that he has described. He referred, as I did, to the comments of David Anderson, which were critical of the mutual legal assistance treaty process on the grounds that it is slow. It is not always the best way of achieving the objective set out in the Bill, because it is not designed for that purpose but an entirely different one.

Finally, I would say that this is really important. Although the hon. and learned Gentleman is right that this is a particular part of a particular part of the Bill and so could be overlooked, it is important to understand that, in terms of the objectives we seek to achieve—that is, those of us who want the Bill to work well, which I think applies to the whole Committee—these powers are significant. Much of what happens is now happening overseas and much of the process by which we deal with overseas organisations is vital to the work of our security services and others. Dealing with extraterritorial matters is significant, but not straightforward. It is dynamic, for the reasons that we have both offered to the Committee. In that respect, I believe we have got the Bill about where it wants to be. I do not say that these things will not evolve over time, but for the purposes we have set out, the clause works.

As with all these things, I start from the perspective of wanting to be both convivial and conciliatory; both helpful and positive. I never ignore arguments put in these Committees or on the Floor of the House, as people know who know how I operate. The House has an important function in making government as good as it can be, and that is partly about the interaction and tension between Government and Opposition. Of course I am always prepared to listen, but I think we have got this right. With the appropriate humility, I suggest that we move on.

Keir Starmer: I indicated would not press the amendments at this stage. I beg leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Question proposed, That the clause stand part of the Bill.

Joanna Cherry: I oppose the clause. I hear what the Minister has to say, but I am not reassured by the Government's approach. Harking back to something I said last week, I do not think that the Government have got the balance right, because in seeking to gather to themselves an extraterritorial application through United Kingdom law, there are hidden dangers.

If international companies are required to arbitrate between conflicting legal systems, it is leaving the protection of human rights to the good will and judgment of those companies. Companies such as the ones the hon. and learned Member for Holborn and St Pancras mentioned have already expressed concerns to David Anderson, for his report "A Question of Trust", that

"unqualified cooperation with the British government would lead to expectations of similar cooperation with authoritarian governments, which would not be in their customers', their own corporate or democratic governments' interests."

In my view, the most appropriate way forward is to pursue the route, which I am pleased the Minister has assured us that the Government are well down, of mutual legal assistance agreements with other states. If we do not pursue that route in the way that both David Anderson and Sir Nigel Sheinwald recommended with appropriate alacrity, and instead rely simply on clauses such as this one, which are spread throughout the Bill, we will create real difficulty for corporate entities. We will also create difficulties for the international enforcement of human rights, which I consider a bit more important than difficulties for corporate entities, although we should not set the latter to one side, because they are significant. For that reason, notwithstanding the Minister's assurances, the SNP opposes clause stand part.

2.30 pm

Mr Hayes: I will not make a case again for the clause, but I shall say this, in the spirit of helpfulness and kindness. It is really important that the Committee sends out a combined message to overseas communications service providers—on which the obligations will have an important effect because their commercial endeavours have a significant relationship with the powers we are trying to cement in the Bill—so that they have a very clear impression that we as a Committee of this Parliament are clear that we expect them to do their bit to do what is right. We should not, out of a sense of good will, allow ourselves to be misled and encouraged not to have high expectations or make serious demands of those organisations.

I simply say to the hon. and learned Lady that clause 76 is about giving a clear signal, as does clause 57, with which it should be read in tandem, that telecommunications operators should comply with the notice given, whether or not they are in this country. I accept that that is difficult and challenging—I made that point at the outset—but my goodness, it is vital that we take these steps. I know that she is open-minded and a woman of great good will, but we should not allow that to dilute in any way that common message to those big companies. I do not want those companies to get away with anything that that should not get away with.

Joanna Cherry: I am not so much concerned about the message we send out to the companies; I am more concerned about the message we send out internationally and potentially to authoritarian regimes. The difficulty is that if the British Government demand from these companies unqualified co-operation with British laws, that might encourage authoritarian Governments to do likewise. We clearly would not want that, so we need to be very careful about the messages we send out and think carefully about their full implications. That is why such matters should be approached by way of mutual legal agreement internationally, rather than the unilateral imposition of one Parliament's will outwith the area where its sovereignty operates.

Question put, That the clause stand part of the Bill.

The Committee divided: Ayes 9, Noes 2.

Division No. 23]

AYES

Atkins, Victoria	Hoare, Simon
Buckland, Robert	Kirby, Simon
Davies, Byron	Stephenson, Andrew
Frazer, Lucy	Warman, Matt
Hayes, rh Mr John	

NOES

Cherry, Joanna	Newlands, Gavin

Question accordingly agreed to.

Clause 76 ordered to stand part of the Bill.

Clause 77 ordered to stand part of the Bill.

Clause 78

POWERS TO REQUIRE RETENTION OF CERTAIN DATA

Keir Starmer: I beg to move amendment 164, in clause 78, page 61, line 5, leave out subsection (1) and insert—

"(1) A Judicial Commissioner may issue a data retention warrant under this Part to authorise the retention of relevant communications data if the Judicial Commissioner considers that the authorisation is necessary and proportionate for one or more of the following purposes—

(a) in the interests of national security, or

(b) for the purpose of preventing or detecting serious crime, or

(c) for the purpose of preventing death or serious injury."

The Chair: With this it will be convenient to discuss the following:

Amendment 165, in clause 78, page 61, line 10, leave out "A retention notice may" and insert "A data retention warrant must".

Amendment 154, in clause 78, page 61, line 19, leave out "notice" and insert "warrant".

Amendment 155, in clause 78, page 61, line 30, leave out "retention notice" and insert "retention warrant".

Amendment 235, in clause 78, page 61, line 30, leave out second "notice" and insert "warrant".

Amendment 156, in clause 78, page 61, line 32, leave out "notice" and insert "warrant".

Amendment 157, in clause 78, page 61, line 33, leave out "notice" and insert "warrant".

Amendment 158, in clause 78, page 61, line 34, leave out "notice" and insert "warrant".

Amendment 159, in clause 78, page 61, line 36, leave out "notice" and insert "warrant".

Amendment 160, in clause 78, page 61, line 37, leave out "notice" and insert "warrant".

Amendment 161, in clause 78, page 61, line 38, leave out "Secretary of State" and insert "Judicial Commissioner".

Amendment 162, in clause 78, page 61, line 41, leave out "notice" and insert "warrant".

Amendment 166, in clause 79, page 62, line 26, leave out "notice" and insert "warrant".

Amendment 220, in clause 79, page 62, line 26, leave out "Secretary of State" and insert "Judicial Commissioner".

Amendment 168, in clause 79, page 62, line 28, leave out "notice" and insert "warrant".

Amendment 169, in clause 79, page 62, line 30, leave out "notice" and insert "warrant".

Amendment 170, in clause 79, page 62, line 31, leave out "notice" and insert "warrant".

Amendment 171, in clause 79, page 62, line 32, leave out "notice" and insert "warrant".

Amendment 172, in clause 79, page 62, line 33, leave out "notice" and insert "warrant".

Amendment 173, in clause 79, page 62, line 35, leave out "notice" and insert "warrant".

Amendment 174, in clause 79, page 62, line 35, leave out "Secretary of State" and insert "Judicial Commissioner".

Amendment 176, in clause 80, page 62, line 38, leave out "notice" and insert "warrant".

Amendment 198, in clause 80, page 62, line 40, leave out "back to the Secretary of State" and insert "to the Investigatory Powers Commissioner for review".

Amendment 335, in clause 80, page 62, line 40, leave out "notice" and insert "warrant".

Amendment 177, in clause 80, page 62, line 41, leave out "notice" and insert "warrant".

Amendment 178, in clause 80, page 62, line 42, leave out "notice" and insert "warrant".

Amendment 180, in clause 80, page 63, line 5, leave out "notice" and insert "warrant".

Amendment 181, in clause 80, page 63, line 6, leave out "notice" and insert "warrant".

Amendment 199, in clause 80, page 63, line 7, leave out "Secretary of State" and insert "the Investigatory Powers Commissioner".

Amendment 182, in clause 80, page 63, line 7, leave out "notice" and insert "warrant".

Amendment 183, in clause 80, page 63, line 8, leave out "notice" and insert "warrant".

Amendment 200, in clause 80, page 63, line 10, leave out "Secretary of State" and insert "the Investigatory Powers Commissioner".

Amendment 201, in clause 80, page 63, line 12, leave out subsection (b).

Amendment 184, in clause 80, page 63, line 14, leave out "notice" and insert "warrant".

Amendment 185, in clause 80, page 63, line 16, leave out "notice" and insert "warrant".

Amendment 193, in clause 80, page 63, line 19, leave out "Secretary of State" and insert "Judicial Commissioner".

Amendment 194, in clause 80, page 63, line 24, leave out "Secretary of State" and insert "Judicial Commissioner".

Amendment 202, in clause 80, page 63, line 25, leave out "Secretary of State" and insert "Investigatory Powers Commissioner".

Amendment 249, in clause 80, page 63, line 25, leave out "and the Commissioner".

Amendment 186, in clause 80, page 63, line 27, leave out "notice" and insert "warrant".

Amendment 187, in clause 80, page 63, line 28, leave out "notice" and insert "warrant".

Amendment 188, in clause 80, page 63, line 30, leave out "notice" and insert "warrant".

Amendment 203, in clause 80, page 63, line 31, leave out "Secretary of State" and insert "Investigatory Powers Commissioner".

Amendment 197, in clause 80, page 63, line 33, leave out "Secretary of State" and insert "Judicial Commissioner".

Amendment 189, in clause 80, page 63, line 33, leave out "notice" and insert "warrant".

Amendment 204, in clause 83, page 64, line 13, leave out "Secretary of State" and insert "Judicial Commissioner".

Amendment 210, in clause 83, page 64, line 13, leave out "notice" and insert "warrant".

Amendment 205, in clause 83, page 64, line 14, leave out "Secretary of State" and insert "Judicial Commissioner".

Amendment 206, in clause 83, page 64, line 15, leave out "Secretary of State" and insert "Judicial Commissioner".

Amendment 211, in clause 83, page 64, line 22, leave out "notice" and insert "warrant".

Amendment 207, in clause 83, page 64, line 23, leave out "Secretary of State" and insert "Judicial Commissioner".

Amendment 212, in clause 83, page 64, line 27, leave out "notice" and insert "warrant".

Amendment 213, in clause 83, page 64, line 28, leave out "notice" and insert "warrant".

Amendment 214, in clause 83, page 64, line 31, leave out "notice" and insert "warrant".

Amendment 215, in clause 83, page 64, line 32, leave out "notice" and insert "warrant".

Amendment 216, in clause 83, page 64, line 34, leave out "notice" and insert "warrant".

Amendment 217, in clause 83, page 64, line 36, leave out "notice" and insert "warrant".

Amendment 218, in clause 83, page 64, line 37, leave out "notice" and insert "warrant".

Amendment 208, in clause 83, page 64, line 38, leave out "Secretary of State" and insert "Judicial Commissioner".

Amendment 370, in clause 83, page 64, line 39, leave out "notice" and insert "warrant".

Amendment 372, in clause 83, page 64, line 40, leave out "Secretary of State" and insert "Judicial Commissioner".

Amendment 209, in clause 83, page 64, line 41, leave out "Secretary of State" and insert "Judicial Commissioner".

Amendment 219, in clause 83, page 65, line 7, leave out "notice" and insert "warrant".

Amendment 221, in clause 83, page 65, line 9, leave out "notice" and insert "warrant".

New clause 7—*Persons who may apply for issue of warrant*—

"(1) Each of the following organisations may apply for a communications data retention warrant—

(a) a police force maintained under section 2 of the Police Act 1996,

(b) the Metropolitan Police Force,

(c) the City of London Police Force,

(d) the Police Service of Scotland,

(e) the Police Service of Northern Ireland,

(f) the British Transport Police Force,

(g) the Ministry of Defence Police,

(h) the Royal Navy Police,

(i) the Royal Military Police,

(j) the Royal Air Force Police,

(k) the Security Service,

(l) the Secret Intelligence Service,

(m) GCHQ, and

(n) the National Crime Agency."

New clause 10—*Requirements that must be met by warrants*—

"(1) A warrant issued under this Part must name or otherwise identify the person or persons, organisation, premises, or location to which the warrant relates.

(2) A warrant issued under this Part must describe the investigation or operation to which the warrant relates.

(3) A warrant issued under this Part must relate to one or more of the following purposes—

(a) in the interests of national security, or

(b) for the purpose of preventing or detecting serious crime, where there is reasonable suspicion that a serious criminal offence has been or is likely to be committed, or

(c) for the purpose of preventing death or injury.

(4) A warrant may only be issued under this Part if there are reasonable grounds for believing that the material is likely to be of substantial value to the investigation or operation to which the warrant relates."

Keir Starmer: I will not say, at this stage, that I am withdrawing all of those amendments.

The Chair: That is a joke, right?

Keir Starmer: It is a joke, Ms Dorries. We now come to a very important clause. In some respects, over the last part of Thursday and today we have been working backwards through the way in which the functions will be exercised, because clause 78 is the starting point in relation to communications data. It relates to the power to require retention of data in the first place, and everything we have discussed has been about how those data can be filtered and accessed after they have been retained. It is a very important clause.

I draw attention to the breadth of the clause, which states:

"The Secretary of State may by notice…require a telecommunications operator to retain relevant communications data if the Secretary of State considers that the requirement is necessary and proportionate for one or more of the purposes falling within paragraphs (a) to (j) of section 53(7)".

The first thing that crops up in relation to the clause is what the test for retention is. The test is, of course, necessity and proportionality but the real question is: what does that necessity and proportionality bite on?

[Keir Starmer]

That pushes us straight back to clause 53(7), which is problematic because it sets such a low threshold for these extensive retention powers.

There should be no doubt that this provision gives the Secretary of State the power to require the retention of a huge amount of data. There may be circumstances in which that is necessary and proportionate, but the test for whether that power is exercised is pushed all the way back to clause 53(7). To take an example that we touched on last week, extensive data can be retained

"for the purpose of preventing or detecting crime"—

any crime. Any crime of any level can trigger a power to retain data. The importance of the issue of retention over that of access is that at this stage it is about retaining the data of those who are not necessarily suspects or targets but anybody whose data come within the types that are intended to be retained. It is a very wide provision.

Sign-off is by the Secretary of State, so there is no double lock and no reference to a judicial commissioner here. The Secretary of State operates the powers, which are very wide. Clause 78(2) states that

"a retention notice may…relate to a particular operator";

it may

"require the retention of all data or any";

it may

"identify…periods for which data is to be retained";

it may "contain…restrictions" and

"make different provision for different purposes,";

and it may "relate to data" that are not even in existence at the time. These are very wide-ranging powers triggered by the test set out in clause 53(7), and that is a cause of significant concern. The retention period is 12 months, so this is an extensive hoovering-up exercise.

It is clear that the clause applies to internet connection records, because that is stated in subsection (9). We touched on internet connection records last week in relation to when internet connection records are to be accessed. Now, I touch on it for a different purpose: to highlight how all our internet connection records can be swept up in a data retention notice issued under this provision.

For that purpose, one obviously starts with the definition of internet connection record in clause 54(6)(a) and (b), which we looked at last week. I will not read it out again but just give some examples of what is intended to be included. I will do so in chronological order. The operational case for the retention of internet connection records was published in August last year. Page 3 made it clear that internet connection records are:

"a record of the internet services that a specific device connects to—such as a website or instant messaging application—captured by the company providing access to the internet".

So that is within the scope of an internet connection record, as set out in the operational case of August 2015. An annexe setting out terminology and definitions was put in evidence before the Joint Committee in January this year, which made it clear that not only web and IP addresses are included, but names and addresses, email addresses, phone numbers, billing data, customers, users, and so on. In the explanatory notes to the Bill, paragraph 2.30, on clause 78(9) makes it clear that,

"communications data that can be retained includes internet connection records. Internet connection records, which are defined in clause 54(6), are a record of the internet services that a specific device connects to—such as a website"

That is therefore consistent with the operational case.

What is swept up under clause 78 are internet connection records, which means connections to the internet and websites to which any device has connected. When anyone uses a device to connect to a website, that is recorded by the provider and comes within the definition. It therefore comes within the retention order. That is what the clause gives the Secretary of State power to retain.

It is fair to point out that clause 54(4), which deals with accessing the data that are retained, says that the access through an authorisation can be allowed only if the purpose is to identify: which person is using the internet, which internet service is being used, where the person or apparatus whose identity is already known is, and so on. It is true to say that on the point of access there is restriction of the way in which internet connection records are accessed, but we need to be absolutely clear that for the purpose of retention, it is a record of all websites visited or accessed by a device.

Mr Hayes: I do not doubt that my hon. and learned Friend the Solicitor General will deal with these points at some length, but is it not fair to say—the hon. and learned Gentleman is in the mood to be fair—that the two subsequent clauses both build a set of safeguards into the system and provide for a review of the system? There is further work in the Bill that caveats what might be taken to be the extremes of his argument.

2.45 pm

Keir Starmer: I am grateful for that intervention, and I accept that there are safeguards in subsequent provisions. I will be corrected if I am wrong, but on the face of it at least—I am not saying they are incapable of a review—the safeguards do not restrict the definition of an internet connection record in a way that would prevent websites visited being swept up in the retention order.

Mr Hayes: Yes.

Keir Starmer: The message to my and all of our constituents is that, even if they are not a target, a record of the websites they have visited can be retained under a data retention order, and if retained will be retained for 12 months—every website they have visited. But if somebody later wants to access it, there is then a tighter test for that. The chilling effect of clause 78 is that the websites visited will be retained if a retention order is issued. We need to be absolutely clear about that. The tighter definition does not kick in until a later stage of the exercise, and that is a cause of real concern to our constituents, certainly to the people who have engaged with me on the topic, and to our fellows across both sides of the House.

Joanna Cherry: I note what the hon. and learned Gentleman says about web addresses being revealed. Is it not also the case that we see from the data released by the Home Office, after being pressed about its factsheet accompanying ICRs, that what will be revealed are not

only web addresses and IP addresses, but the names, addresses, email addresses, phone numbers and billing data of customers—our constituents?

Keir Starmer: I cannot double check on my feet, but that sounds like the further evidence that was put before the Joint Committee when it was in the middle of its deliberations. In fairness, the Home Office did go beyond websites to include some, maybe all, of the matters to which the hon. and learned Lady just referred.

The way this will operate in practice is a cause of real concern. The Secretary of State, without the double check of a judicial commissioner, and operating against a low-level threshold—clause 53(7)—can issue a retention order that will permit the retention of a record of all the websites that somebody has visited. That record will then be kept for 12 months, albeit with a different test if it is to be accessed later.

The amendments—I think you have called them the first set of amendments, Ms Dorries—are intended to construct in the first instance a different framework around this power, because it is so extensive, and put it in the hands of a judicial commissioner rather than the Secretary of State. That would provide a greater safeguard in relation to clause 78, with independent oversight through the function of the judicial commissioner. Alternatively, amendments 152, 153 and 222 would give the Investigatory Powers Commissioner some oversight. In other words, the intention behind these amendments is to put some rigour and independence into the exercise of what is a very wide power that, in fact, is the starting point for the exercise of all the other powers under the parts of the Bill that we are now concerned with.

An anxiety that has been expressed on a number of occasions about cost. Huge amounts of data could be required for retention under clause 78. The Government have estimated the cost at £170 million. That is considered to be a gross underestimate by those who will no doubt be called upon to actually retain the data. For those reasons, these amendments are intended to tighten up a clause that is very wide and very loose. It permits a huge amount of data to be retained, including websites visited by you, by me, or by our constituents.

Gavin Newlands (Paisley and Renfrewshire North) (SNP): It is a great pleasure to rise as part of this ongoing scrutiny, and to offer my hon. and learned Friend the Member for Edinburgh South West a brief respite in this Committee. It is also a great pleasure to serve under your chairmanship, Ms Dorries. It is great to follow the hon. and learned Member for Holborn and St Pancras, who in his customary fastidious and engaging manner has covered in a short space of time all the aspects of many amendments. Some of that bears repeating, and I will speak to new clause 10, which is tabled in my name and that of my hon. and learned Friend the Member for Edinburgh South West.

My hon. and learned Friend spoke at length about the important role that the judiciary, in the form of judicial commissioners, should bring to this process. We do not think it is good enough that the Bill only proposes to use judicial commissioners to review the process used by the Secretary of State in making a decision. The Government may claim that it is important that the Home Secretary retains the power to issue retention notices to internet service providers, as it will ensure that democratic accountability is a salient feature of the process, but I do not accept that to be the case. In fact, I would argue that because of the political arena that any Home Secretary operates in, it is right that this power is handed to and delegated to an independent official such as a judicial commissioner.

It is also worth noting that we know very little of the various notices that the Home Secretary issues, and as such there is no possible opportunity to hold her to account for them. Building the role of judicial commissioners into this part of the process will help to ensure that we have appropriate checks and balances when it comes to the retention of communications data. This is vitally important, because it is the proper constitutional function of the independent judiciary to act as a check on the use of intrusive and coercive powers by state bodies, and to oversee the application of law to individuals and organisations. Liberty rightly points out that judges are professionally best equipped to apply the legal tests of necessity and proportionality to ensure that any surveillance is conducted lawfully.

I turn now to new clause 7. Schedule 4 provides a lengthy list of bodies that are able to access or retain data, including several Government Departments, such as the Department for Transport, and a range of regulatory bodies, such as the Food Standards Agency and the Gambling Commission. This suggests that access to communications data may be allowed for a range of purposes which may be disproportionate and inconsistent with the guidance offered by the European Court of Human Rights.

Mr Hayes: I draw the hon. Gentleman's attention to clause 79, which we are not debating at the moment but which is directly relevant to the point he made about proportionality. Clause 79(1)(a) states:

"(1) Before giving a retention notice, the Secretary of State must, among other matters, take into account—

(a) the likely benefits of the notice".

To me, that would be a pretty strong way of enforcing proportionality. Yet the hon. Gentleman is in his peroration claiming that that would not be taken into account, or not sufficiently so.

Gavin Newlands: I am grateful for the Minister's intervention. I appreciate that that is a safeguard, but we must ask whether those Departments should be getting access in the first place.

Mr Hayes: I do not want to be unnecessarily brutal with the hon. Gentleman, but either he is making an argument about proportionality or he is not. If he is saying that nothing is proportional, then it should not happen at all, that is hardly an argument about proportionality. Those of us who take a more measured view of these things are considering whether such collection and access to data are proportionate. Proportions by their nature require an assessment of balance, do they not? Yet the hon. Gentleman is suggesting that the scales are weighted all on one side.

Gavin Newlands: The Minister did not actually address why these Departments need access to this data in the first place. I appreciate the point that he is making, but these Departments should not, in my view, require access to this information.

Joanna Cherry: The Minister talked about the duty to take into account the likely benefits of the notice, but does my hon. Friend agree that something may be beneficial without being necessary?

Gavin Newlands: I agree with my hon. and learned Friend. We are not opposed to every measure in the Bill. There are benefits, but unfortunately they are not covered by enough safeguards and are not drawn tightly enough. I would like to make progress but I will give way once more.

Simon Hoare (North Dorset) (Con): I apologise if I missed the hon. Gentleman outlining the Departments, but could he tell me which ones should be excluded and not have access to this?

Gavin Newlands: That has been dealt with at length. I have already mentioned the Food Standards Agency as one of the regulatory bodies. Schedule 4 does currently provide a lengthy list of bodies that should be able to access the data. New clause 7 would ensure that only the police forces and security agencies may request a communications data warrant, except where the warrant is issued for the purpose of preventing death, in which circumstances emergency and rescue services also fall within the definition.

New clause 10 outlines the requirements that must be met by warrants.

Simon Hoare: As, for example, the Food Standards Agency cannot itself bring a prosecution, may I conjure in the hon. Gentleman's mind a situation whereby a criminal gang, as part of its activities, seeks to bring into the United Kingdom for sale to the British public a contaminated food source? Is that not something to which the Food Standards Agency should have access to information in order to ensure that citizens and consumers are safe?

Gavin Newlands: I understand the hon. Gentleman's point, but surely the police would be interested in that scenario and would have access.

Simon Hoare: In the abstract—by golly, isn't this debate being held in the abstract?—the hon. Gentleman is absolutely right, but we invest the powers with the agency. The police are not an infinite resource. If we have the many who are charged with multiple areas of our lives—

The Chair: Order. Mr Hoare, can we keep it to an intervention, please, not a speech?

Simon Hoare: Forgive me. The hon. Gentleman knows my point.

Gavin Newlands: These powers are very large and we should limit who has access to them. The police can pass on the relevant information to the agencies that can deal with that particular incident, but in my view, only the police and security forces should have access. I want to finish my point on new clause 10 but I will allow one last intervention.

Victoria Atkins: I want to understand the hon. Gentleman's understanding of how cases are prosecuted in England and Wales, if not in Scotland. Is the hon. Gentleman saying that Her Majesty's Revenue and Customs, for example, should not have access to any of these powers? Is the hon. Gentleman saying that the investigation of economic crime that can potentially alter the GDP of another member state is not worthy of these powers? I wonder what the differentiation is between those organisations he thinks should have these powers and those that cannot. At the moment, it is not clear.

The Chair: Order. May I just ask that interventions be kept short, please, or we will be here all night? Mr Newlands.

Gavin Newlands: I appreciate what the hon. Lady says but, as I am not a lawyer, I am struggling to distinguish the difference between Scottish and English law. Perhaps my colleague could address that.

Joanna Cherry: My hon. Friend will no doubt agree that, in Scotland at least, it is the police who investigate serious crime, under the direction of the Lord Advocate.

Victoria Atkins: Will the hon. Gentleman give way?

Gavin Newlands: The point has been dealt with, and I think we need to move on. The effect of new clause 10 —*[Interruption.]* I will finish, amid the chuntering. These new clauses require data retention notices to be issued only for specific investigative or operational purposes, to obtain specified data where those data are believed to be of substantial value. We do not believe, however, that the role of communications data in the investigation of crime justifies the Secretary of State's mandate for blanket retention of historical communications data for the entire population for 12 months.

3 pm

Instead of the Secretary of State imposing an arbitrary and speculative data retention notice to cover the entire population, we propose that police forces should be able to apply to a judicial commissioner for targeted data retention warrants, where data is required for specific purposes. Building the role of judicial commissioners into that part of the process will help to ensure that we have appropriate checks and balances when it comes to retention of communications data. That is vital, as it is a proper constitutional function of the independent judiciary to act as a check on the use of intrusive and coercive powers by the state.

Christian Matheson (City of Chester) (Lab): I am delighted to see you back in the Chair, Ms Dorries, as I break my couple of sessions' silence; it is always very reassuring. I certainly do not wish to keep the Committee here all night, but I will reiterate a point that I made earlier in our considerations, and that relates to the retention of certain data. As my hon. and learned Friend the Member for Holborn and St Pancras pointed out, we understand the need for data retention. However, on looking at the Bill, I am still not entirely satisfied that the Government have taken into account the need for additional security for data retention.

I look to the Minister for reassurance that, when telecommunications and internet providers and suchlike are obliged to retain data, there is a consequent obligation on them to maintain it securely. We know that several such providers have problems with internet security: we saw that with the TalkTalk hack, and we believe another large provider has been hacked recently. Those attacks were on personal data; the Solicitor General and I have had exchanges in this room about the potential for charging them as theft—about whether the sanctions against somebody who committed that offence would be contained in existing legislation.

This part of the Bill needs to look at obliging or maintaining a minimum acceptable level of security, to provide security and privacy for people whose data may have been accepted. I realise that it might not necessarily be covered in detail in the new clause, but now might be a good time for the Ministers to consider whether they believe internet security and the security of personal data held under the terms of clause 79 should be considered in the Bill. Do they believe guidance should be given to telecommunications providers to maintain that security, or do they feel that it is not relevant and that they are quite satisfied with the status quo? I must say that I am not. Notwithstanding the need for the retention of individual data, as described so eloquently by my hon. and learned Friend, it remains a major concern of mine that individual privacy and data are at risk: it puts a question mark over the whole clause and over the areas we are discussing.

The Solicitor General: I am grateful to hon. Members for a wide-ranging debate. I would first like to reiterate on behalf of the Government the position adopted by the Joint Committee on the draft Investigatory Powers Bill, which quite clearly indicated its conclusion that the case was made for a retention period of up to 12 months for relevant communications data. In the report from David Anderson, QC, "A Question of Trust", recommendation 14 is:

> "The Home Secretary should be able by Notice (as under DRIPA 2014 s1 and CTSA 2015 s21) to require service providers to retain relevant communications data for periods of up to a year".

There we have it: the Government are acting upon the specific endorsement of an independent reviewer and a Joint Committee of this House. There is an element of the waving of the proverbial shroud when it comes to the retention of data, because the word "relevant", which is contained in the second line of clause 78(1), is the governing word here. It is very important to remember that this is not carte blanche for the Secretary of State to authorise communication service providers to retain everything for 12 months. That is not the case. Where there is no case of necessity and proportionality for a 12-month period, a shorter period must be adhered to. Indeed, if the material is not relevant, it falls outwith the ambit of any such authorisation.

I reassure the hon. Member for City of Chester, who makes quite proper points about the integrity of data, that he is right to make them. That issue affects all those in this room and beyond. He is also right to allude to the criminal law. I reassure him that communication service providers have to comply with the Data Protection Act 1998 and the Privacy and Electronic Communications (EC Directive) Regulations 2003, which together contain those requirements that the data is appropriately secured. When he has the time—which I am sure is as precious to him as it is to the rest of us—chapter 16 of the draft communications code of practice contains an entire set of provisions relating to the security, integrity and, indeed, destruction of retained data, which very much underpin the principles of why CSPs have to operate and will give him the reassurance that he properly seeks about the position with regard to individual data and people's privacy.

Data retention legislation has existed in this country since the Anti-terrorism, Crime and Security Act 2001, which allowed the Secretary of State to enter into voluntary agreements with telecommunications operators so that they could retain data that otherwise would be deleted. The Data Retention (EC Directive) Regulations 2007 were the first piece of data retention legislation that provided for the Secretary of State to require the retention of such data. We currently have DRIPA 2014 and the data retention regulations of that year. We hope to replace those with the provisions in the Bill. A very important point is that there is nothing new about these proposals. Our data retention legislation has always had the Secretary of State involved in the process and there are very good reasons for that. It has worked successfully until now. As I have indicated, it has been recommended to us by David Anderson.

The amendments that have been tabled seek to drive a coach and horses through all of that. There is a simple and blindingly obvious reason why we wish to maintain the system of data retention. For example, when a crime happens or a child goes missing, it is impossible to know in advance which data would be relevant in any subsequent investigation. It is therefore important that we require the retention of all relevant communications data that matches a certain description wherever it is necessary and important. Because it is impossible to know which data will be the most relevant in advance of any crime, it is impossible to know whether a specific piece of data will be of value to MI5 in locating a terrorist, for example, or to the National Crime Agency in identifying a paedophile, or for any other legitimate purpose. For that reason it does not make sense for those authorities to apply for retention warrants individually. What makes sense is for the requirement of all relevant public authorities to be considered together. The person best placed to do that is the Secretary of State. Public authorities set out their requirements for data retention to the Home Office and they are then carefully considered. As they usually overlap, the Secretary of State is able to identify the specific telecommunications operators and specific data types that it is necessary and proportionate to make subject to data retention notices. As the full costs of data retention are covered by the Secretary of State, only he or she can decide whether or not the benefits of data retention are proportionate to the costs.

There has been some discussion about cost again today. The £170 million figure is based on the cost of our anticipated implementation, which takes into account data that is already obtained under existing legislation. We noted the evidence of BT when it talked about the costs being dictated by its implementation approach, and we continue to discuss implementation with those communication service providers likely to be inspected. Whatever the final cost, however, the important underwriting by the Government is a vital factor in

[The Solicitor General]

giving reassurance to the industry, not only on the practicability of these measures, but on the importance therefore of involving the Secretary of State.

My worry is that if we went down the road proposed by the amendments, we would end up with a rather confused system that would not allow for the overall benefits of retaining a particular type of data, because the judicial commissioner would only ever be able to consider the benefits to the particular public authority applying for a warrant. It would therefore be impossible to judge the overall necessity and proportionality of requiring a particular company to retain a particular dataset.

We have heard about new clause 10 and its provisions. Given that it is impossible to predict in advance what data would need to be retained, this approach relies on data being retained only after a crime has been committed and/or an investigation has begun. Preservation only works if the data is there to preserve and it is of limited benefit without an existing retention scheme. Without data retention, data protection rules require that the data that is no longer needed for business purposes must be deleted. Without data retention, the data that is needed would not exist. Therefore, the regime of warrantry—the double lock, indeed the proposals put forward by Opposition Members—none of it would matter, because the material would not be there. That is particularly relevant when it comes to the increasing move of criminals and their ilk away from conventional telecommunications to the internet and internet connections.

A number of reports published by the EU Commission show the value of communications data and why the concept of data preservation, as envisaged in new clause 10, is not a viable alternative. In a Europe-wide investigation into online child sexual exploitation, of the 371 suspects identified here in the UK, 240 cases were investigated and 121 arrests or convictions were then possible. Of the 377 suspects in Germany, which does not have a data retention regime, only seven could be investigated and no arrests were made.

I have explained why the existing data retention regime that the Bill replicates is the appropriate model. May I deal with the change proposed by a set of amendments that involve changing the word "may" to "must" in clause 78(2)? That would require a data retention notice to cover certain issues. I am sympathetic to the aim of the amendment, because I am in favour of specific requirements, but the amendment is misconceived because subsection (7) already requires that a retention notice must specify the operator to whom it relates, the data which is to be retained, the period of retention, the requirements and restrictions imposed by the notice, and information on costs. Subsection (2) sets out the scope of what a notice may require and subsection (7) requires that the notice must make clear what is required. The two subsections are therefore aimed at different things.

The effect of this amendment would be to require a notice to cover issues that it might not have any reason to cover. For example, a retention notice may

"make different provision for different purposes".

With respect, it therefore does not make sense to say it must make different provision for different purposes, because a notice may not relate to those different purposes. I would argue that there is therefore nothing to be gained by moving these amendments. That is all I wish to say, but for those reasons I urge hon. Members to withdraw the amendments.

3.15 pm

Keir Starmer: Clause 78 is important for all the reasons that I have set out, but at this stage, I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Gavin Newlands: I beg to move amendment 303, in clause 78, page 61, line 12, leave out—

"of all data or any description of data"

and insert

"of specified relevant communications data".

The Chair: With this it will be convenient to discuss the following:

Amendment 304, in clause 78, page 61, line 14, leave out paragraph (2)(d).

Amendment 305, in clause 78, page 61, line 16, leave out paragraph (2)(e).

Gavin Newlands: I will not detain the Committee for too long; these issues have already largely been addressed. Amendments 304 and 305 seek to remove paragraphs (d) and (e) from clause 78(2). In a Bill replete with vagueness, those two subsections stand out as being particularly vague. The new clause that I will come to in a moment would require a data retention notice—or warrant, as we would wish—to be issued only for a specific investigative or operational purpose. The SNP has tabled amendments that will bring greater clarity to when and why a warrant would be issued.

As we know, communications data is defined as data that would be used to identify, or assist in identifying, the who, where and how. However, instead of allowing a blanket surveillance approach that treats everyone as a suspect, the amendments would allow the police to apply to a judicial commissioner for targeted retention warrants, in which data is required for the purposes of a specific investigation into serious crime, or for the purpose of preventing death or injury. I trust that these amendments are acceptable to the Government.

The Solicitor General: I rise to address the concerns of the hon. Gentleman. It is good to hear from him; I should have said that during the last group. He has made the point about his concerns of vagueness. However, I would argue that it is very important that a notice can have a degree of flexibility within it, because a single telecommunications operator may provide a number of different communications services, such as mobile telephony and internet access. However, there may be different complexities and sensitivities about the different types of communications data that are generated by those services. Considerable preliminary work is carried out between the Government and telecoms operators in advance of the service of a retention notice. That covers a number of issues, including the type of data that will be retained, the complexities of the operator's systems, and the relevant security requirements. Flexibility is needed to ensure that the notice can appropriately

reflect those issues, and that it imposes the minimum requirements necessary to meet the operational requirements.

What we are counter-intuitively getting at is to make sure that there is necessary give and take within the system to prevent what the hon. Gentleman and I would regard as an overweening approach from the Secretary of State, which would impede the ability of communications service providers to carry out their operations. For that reason, I respectfully urge him to withdraw the amendment.

Gavin Newlands: I hear what the Solicitor General has said, but I do not wholly agree with him. I reserve the right to bring this back at a later stage. I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Joanna Cherry: I beg to move amendment 306, in clause 78, page 61, line 18, at end insert—

'(2A) A retention notice may not require a telecommunications operator to retain any data belonging to a third party data, unless that third party data is retained by the telecommunications operator for their own business purposes."

The Chair: With this it will be convenient to discuss amendment (a) to amendment 306, leave out "notice" and insert "warrant".

Joanna Cherry: Amendment 306 would insert at the end of clause 78(2) a provision in relation to third party data. Third party data are defined in the code of practice as data that a communications service provider is able to see

"in relation to applications or services running over their network…but does not process that communications data in any way to route the communication across the network".

To its credit, the Home Office has been unequivocal that such third party data would not be covered in the Bill; the Home Secretary informed the House on 4 November 2015 that the Bill

"will not include powers to force UK companies to capture and retain third party internet traffic from companies based overseas".—[*Official Report*, 4 November 2015; Vol. 601, c. 969.]

The draft code of practice for communications data states at paragraph 2.61:

"A data retention notice can never require a CSP to retain the content of communications or third party data".

The overly broad definition of relevant communications data, which now extends to 16 different definitions and sub-definitions, could however be interpreted as giving the Secretary of State the power to require a communications service provider to retain third party data, since the definition does not expressly exclude third party data unless this amendment is agreed. There are currently no clauses in the Bill that explicitly state that communications service providers will not be required to retain third party data. That is the purpose of the amendment. Given that they have been so clear on the Floor of the House and in the code of practice that that is their intention, if the Government will not accept the amendment, the Minister must tell us why. Where we are dealing with such potentially intrusive powers, we must be as clear as possible.

The Solicitor General: Amendment 306 is tabled, quite properly, to tease out from the Government the more detailed reasoning behind the important statement made by the Home Secretary on Second Reading. The hon. and learned Lady is quite right to refer to that statement. I once again reiterate the Government's position that we will not be requiring the retention of third party data through these provisions.

The question is how best to achieve that; therein lies the tension. Attractive though the approach advanced by the hon. and learned Lady might be, there are some drafting issues and problems about legal certainty, which mean that putting those provisions in the Bill with suitable detail is problematic.

One of the main functions of the Bill—and one of my desiderata—is to ensure that it is resilient and stands the test of time. My concern is that if we end up with a definition that is too technologically neutral, it will either fail the test of time in this place, or be subject to challenge. As a Law Officer, legal uncertainty is something I have to take very seriously when considering how legislation is presented. That is why I commend the detailed provisions within the draft code of practice on third party data—paragraphs 2.68 to 2.72—that the hon. and learned Lady referred to. That is not only an explicit reiteration of our commitment but the sort of detail needed for those operating the provisions, which could not be properly put in the Bill.

It is generally well understood what third party data are, but perhaps I should briefly explain the important areas of detail that could not be covered on Second Reading. Where one communications service provider is able to see the communications data in relation to applications or services that run over their network, but does not process that communications data in any way to route the communication across the network, then that is regarded as third party data. For example, an email provider, such as Yahoo or Gmail, knows that a certain internet access service, such as BT Internet, was used to send email, but that fact is not needed or used to send it. So it is in everybody's interest, not least that of the service providers themselves, that there is sufficient clarity about the data that can be retained under the provisions. As I have said, I think the code of practice is the right vehicle for this. It is also the appropriate vehicle for ensuring that there can be a sufficiently detailed definition of third party data for the reasons I have outlined. In those circumstances, I respectfully ask the hon. Lady to consider withdrawing her amendment.

Joanna Cherry: I am not happy about withdrawing the amendment in the absence of elaboration of what the Solicitor General means by drafting issues and problems of legal certainty. I am not clear at the moment why we cannot have both the amendment and the further elaboration that will be provided in the codes of practice.

Amendment proposed to amendment 306: (a), leave out "notice" and insert "warrant".—(*Gavin Newlands.*)

Question put, That the amendment be made.

The Committee divided: Ayes 7, Noes 9.

Division No. 24]

AYES

Cherry, Joanna	Newlands, Gavin
Hayman, Sue	Starmer, Keir
Kyle, Peter	Stevens, Jo
Matheson, Christian	

NOES

Atkins, Victoria	Hoare, Simon
Buckland, Robert	Kirby, Simon
Davies, Byron	Stephenson, Andrew
Frazer, Lucy	Warman, Matt
Hayes, rh Mr John	

Question accordingly negatived.

Question put, That amendment 306 be made.

The Committee divided: Ayes 2, Noes 9.

Division No. 25]

AYES

Cherry, Joanna	Newlands, Gavin

NOES

Atkins, Victoria	Hoare, Simon
Buckland, Robert	Kirby, Simon
Davies, Byron	Stephenson, Andrew
Frazer, Lucy	Warman, Matt
Hayes, rh Mr John	

Question accordingly negatived.

3.30 pm

Gavin Newlands: I beg to move amendment 317, in clause 78, page 61, line 34, leave out "(or description of operators)" and insert "or operators".

The Chair: With this it will be convenient to discuss the following:

Amendment 315, in clause 78, page 61, line 37, leave out "(or description of operators)" and insert "or operators".

Amendment 319, in clause 78, page 61, line 42, leave out "(or description of operators)" and insert "or operators".

Amendment 328, in clause 79, page 62, line 33, leave out "(or description of operators)" and insert "or operators".

Amendment 338, in clause 80, page 62, line 42, leave out subsection (3).

Amendment 361, in clause 83, page 64, line 16, leave out "(or description of operators)" and insert "or operators".

Amendment 374, in clause 83, page 65, line 1, leave out "(or description of operators)" and insert "or operators".

Amendment 375, in clause 83, page 65, line 8, leave out "(or description of operators)" and insert "or operators".

Gavin Newlands: The SNP has tabled the amendments to provide for clear, appropriate and limited grounds on which data retention warrants may be issued. The amendments require that the data to be retained are specified and that organisations served with warrants to retain communication data should be identified rather than merely described.

Amendments 315 and 317 affirm that organisations that have been served a notice or warrant to retain the communications of their customers are properly and explicitly identified. The term "description of operators" is far too vague and we urge that it is changed to "or operators". Amendment 328 ensures that those organisations are defined and named before a retention notice can be issued. Amendment 338 removes the possibility of the Home Secretary being able merely to describe the telecommunications operators that she wants to target. Amendments 361, 374 and 375 provide the basis for a concrete description to be included when there is any variation of a notice.

The amendments attempt to bring to the Bill some clarity, which is sadly lacking. It is not good enough that the Home Secretary can sign a notice that merely describes who is impinged on or directly affected by these intrusive powers, because that approach opens up the space for the powers to be abused. We need to act to ensure that, as much as possible, we operate a targeted approach.

The Solicitor General: I understand the purpose behind the amendment in that, in the opinion of the hon. Member for Paisley and Renfrewshire North, it would ensure greater specificity in the giving of notices. However, I shall give a brief example of what a "description of operators" might be. With this provision we would have been able to give the same retention notice to all wi-fi providers supplying wi-fi to the Olympic park in London during the 2012 Olympics. In these circumstances the operators are providing precisely the same kind of communications service and the data required to be retained is the same. Whether a notice relates to a description of operators or to a single operator, it can only contain what the Bill's provisions allow and the Secretary of State must consult with the operators to which it relates. Operators also have the opportunity to refer the notice back to him or her in relation to any aspect of it. Therefore, on that basis, I invite the hon. Gentleman to withdraw his amendment.

Gavin Newlands: I am content to withdraw the amendments at this stage. I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Keir Starmer: I beg to move amendment 152, in clause 78, page 61, line 36, at end insert ", and

(c) only when approved by the Investigatory Powers Commissioner.

(5A) In deciding whether to approve a notice, the Investigatory Powers Commissioner must determine whether a notice is—

(a) that the conduct required by the notice is necessary for one or more of the purposes in section 53(7); and

(b) that the conduct required by the notice is proportionate to what is sought to be achieved by that conduct."

The Chair: With this it will be convenient to discuss the following:

Amendment 153, in clause 78, page 61, line 38, leave out "Secretary of State" and insert "Investigatory Powers Commissioner".

Amendment 222, in clause 83, page 64, line 21, at end insert "and

( ) the variation has been approved by the Investigatory Powers Commissioner."

Keir Starmer: For better or for worse, I spoke to these amendments during my submission on earlier amendments. I do not have any additional points and I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Gavin Newlands: I beg to move amendment 320, in clause 78, page 62, line 13, leave out subsection (9) and insert—

"(9) In this Part 'relevant communications data' means—

(a) communications data of the kind mentioned in the Schedule to the Data Retention (EC Directive) Regulations 2009 (SI 2009/859), or

(b) relevant internet data not falling within paragraph (a).

(9A) In this part 'relevant internet data' means communications data which may be used to identify, or assist in identifying, the sender or recipient of a communication (whether or not a person)."

Thus far while debating the clause we have covered providing for the judiciary, in the shape of judicial commissioners, to issue data retention warrants rather than notices, and removing the Secretary of State from the role, making it clear on the face of the Bill who is eligible to apply for a warrant; limiting the grounds for the issuing of warrants; ensuring that all targets are identified and not described; and that the data to be retained should be specified. The fact that we in opposition have had to table so many amendments highlights the main problem in the drafting of the Bill: vagueness. The Bill is wholly lacking in specificity and clarity and nothing highlights that more than the issue of internet connection records.

As trailed by my hon. and learned Friend the Member for Edinburgh South West during the debate on clause 54, the SNP has significant reservations about the provisions on internet connection records as drafted in the Bill. Not only are the definition and legality of the provisions unclear, but the Government's case for ICRs has simply not been made. Amendment 320, which stands in my name and that of my hon. and learned Friend, would effectively remove ICRs from the Bill and replicate the Data Retention and Investigatory Powers Act 2014 in its original form, to ensure that the definition of "relevant communications data" is consistent with current legislation. That will help provide the legal certainty and clarity that the industry needs to understand its legal obligations appropriately. At the moment the industry is having difficulty in understanding what exactly the Government want and require it to do. Although the industry is willing to work with the Government to try to implement their vision for ICRs, it does not know what ICRs are, and it looks as though the Government do not altogether know either.

Despite the significance of ICRs, very little detail about them has been provided, with the Government consistently saying that the detail can be worked out later. That lack of clarity is simply not good enough when the Government are asking us to sign off on legislation that will have a significant impact on the industry and impinge significantly on the right to basic privacy that our constituents, quite rightly, expect. Indeed, the Internet Service Providers Association says:

> "The Investigatory Powers Bill deals with highly complex technical matters, however, our members do not believe that complexity should lead to a Bill lacking in clarity."

I could not agree more. As has been mentioned already, the clearest definition of an ICR is not in the Bill itself but in the document "Operational Case for the Retention of Internet Connection Records" from the Home Office. That describes ICRs as

"a record of the internet services that a specific device connects to – such as a website or instant messaging application – generated and processed by the company providing access to the internet."

A concrete definition of what specific data form an ICR, exactly who has access, precisely what for and exactly who must retain the data must be on the face of the Bill.

The Home Office may want to have a "flexible" definition, as typified in clause 54(6), but given that we are dealing with a Bill that may have the biggest impact on civil liberties than any other Bill for generations, that simply will not cut the mustard. The Intelligence and Security Committee helpfully referred to ICRs as providing information on the "who, when and where" of someone's internet use. The Government claim that they have no plans to acquire the content of the said communications, but DRIPA and RIPA suggest that that does not matter, given that acquiring the sort of information that is going to be held under an ICR can provide important details on the date, time, location and type of communication used. Liberty suggests that ICRs will provide a detailed and revealing picture of somebody's life in the digital age. That point was highlighted by the Information Commissioner when he said that ICRs can reveal a great deal about the behaviours and activities of an individual. In fact, Stewart Baker, former senior counsel to the United States National Security Agency, stated that it

"absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content."

Based on those statements alone, it is important to assess the proportionality and necessity of ICRs, but also question whether they are in accordance with the law. We live in a digital world and, quite rightly, our constituents place a lot of importance on their right to privacy as they use the internet. We accept that the security authorities need adequate powers to keep us safe and it is only proper that the Government consider what new powers they need for the digital age. However, like most people, I am deeply concerned about the complete lack of specifics about ICRs. In publishing such widely-drafted legislation and telling the sector that the detail will come shortly, the Government are asking us all to trust them. They are asking us, as Members of this House, to pass and approve legislation without knowing what its full impact, costs or consequences—unintended or otherwise—will be. In effect, they are asking us to sign a blank cheque on much of the communications data powers. Is that really a proper and effective way to devise and develop legislation that has such civil liberty repercussions?

The SNP is not opposed to certain authorities having the power to obtain communications data or internet connection information critical to their investigations. We fully accept that some power is not only necessary,

[Gavin Newlands]

but crucial, for law enforcement in the 21st century. However, rather than a blanket collection of the websites that everyone in the UK has visited in the last 12 months, we prefer a specific, targeted solution. We agree that intercepting someone's communication data can be an important part of any criminal investigation and it is important that we do that for those suspected of being engaged in criminal activity. There is an obvious difference, though, in intercepting the communications of those suspected of criminal activity and those of the vast majority of our constituents, who are, by and large, law-abiding citizens.

The Government are asking companies to hold and retain information on all the internet sites that an individual visits. It is unclear how much information the Government want those companies to hold, but it is clear that it is going to be a huge amount of data and we still do not know about the feasibility or costs involved. The sort of information that the Government want companies to retain could be sites that the person has mistakenly accessed; it could be a website that the person has spent only a few seconds on; it could also be an internet site that a person has accessed for deeply personal reasons, such as receiving advice on domestic violence or on health matters. Putting the sensitivity and privacy argument to one side, we need to consider whether the Government are going to have too much information at their disposal and thus, inadvertently, make it harder for our security services to complete their investigations.

During the evidence session I made a point about mobile devices always being connected to the internet via various apps, following a similar point made by the hon. and learned Member for Holborn and St Pancras. Those applications are constantly creating ICRs and that will increase as phones become even more advanced and able to process more information more quickly, with bigger memories.

It is unclear how many automatic ICRs are being created by my phone alone, but the Government are demanding that the various communications companies retain these ICRs for a period of 12 months. Conversations with people in the industry have shown that companies have yet to figure out how they will separate the automatic data that are generated through a third-party app from the data that are generated manually by a user. According to the definitions in the Bill, both will generate the same data, showing that the user has accessed an app and recording the date, location, time and so on of that use.

Another industry expert told me that a single app could generate up to 100 ICRs per minute—that is just one single app. I am unsure of the figures for over here, but in America there is an average of 27 apps on every smartphone. If it is the same in the UK, and taking into account the average number of apps and possible connections, this could lead to 2,700 ICRs per phone per minute, or 100,000 ICRs per phone per day. Well over 3 million ICRs could be generated just by the phones in this room. The third party app issue has been raised by the industry time and time again, but it has not been properly addressed by the Government. In evidence given to this Committee, the CEO of BT security, which has been working with the Government, said in response to the third party app issue:

"We are considering whether to propose an amendment to the Home Office on the third party data question, which is the case in point here, and how that should be approached. We think that the principle is that other providers who have that data are the ones who should be subject to it, and that it should be explicit in the Bill".

I then pressed him on whether at the moment the Bill was not clear enough on that aspect. He replied:

"It could be clearer, and we are thinking about proposing an amendment specifically to over-the-top providers, making it clear that they are responsible for that".

I have to say, if BT are unsure who is involved, how are the rest of the industry supposed to know? We have to ask whether or not it is necessary or proportionate for the Government to have information and data on the apps that I or anyone else has on their phone. Given these points, among others, I can understand why so many people are calling ICRs a Home Office solution to a police problem, instead of being a police solution to a police problem. This point was articulated during the evidence session by Sara Ogilvie of Liberty, who said:

"It seems clear that, given the bulk nature of these powers, they will not deliver that kind of information in a helpful manner. If anything, it seems more likely to drive criminals to use bits of the internet that will not be captured by the service".—[*Official Report, Investigatory Powers Public Bill Committee,* 24 March 2016; c. 49, 15.]

We also need to be mindful of the amount of information that we want to expose and the potential for this to be targeted by criminal hackers. When a similar plan to collect web logs was proposed in 2012, the Joint Committee on the draft Communications Data Bill concluded that it would create a

"honeypot for casual hackers, blackmailers, criminals large and small from around the world, and foreign states".

This wealth of data in the wrong hands could be used for identity theft, scamming, fraud, blackmail and even burglaries, as connection records can show when internet access occurs in or out of the house, representing a daily routine. This is an unacceptable level of risk to inflict on innocent internet users. The Chair of the Science and Technology Committee said:

"There remain questions about the feasibility of collecting and storing Internet Connection Records (ICRs), including concerns about ensuring security for the records from hackers. The Bill was intended to provide clarity to the industry, but the current draft contains very broad and ambiguous definitions of ICRs, which are confusing communications providers. This must be put right for the Bill to achieve its stated security goals".

Furthermore, not to be outdone, the Joint Committee tasked with scrutinising the draft Communications Data Bill said in its final report that,

"storing web log data, however securely, carries the possible risk that it may be hacked into or may fall accidentally into the wrong hands, and that, if this were to happen, potentially damaging inferences about people's interests or activities could be drawn".

Surely with these warnings, which were issued by such influential and important Committees, the Government should have listened and addressed some of their concerns, but it would seem not. With regards to some of the case studies laid out in "Operational Case for the Retention of Internet Connection Records", the likelihood of ICRs proving vital in identifying criminals has been questioned by ISPs and technologists. The justification for ICRs being helpful relies on the assumption that online criminals offend using a regular browser or

public file sharing service on their own device, using personal internet connections, without employing the most basic of the widely available anonymity tools to avoid detection. The use of VPNs or Tor helps anonymise users of the internet. As such, ICRs will be unusable and, in fact, misleading where such privacy tools have been used. It is obvious for all to see that the more information that is retained, the greater the costs entailed to either the industry or the taxpayer.

When I spoke to people at TechUK last week, they explained that the introduction of ICRs will be a significant change to the industry and that all organisations will have to re-adapt to meet the new expectations and responsibilities that are being put on them. In addition, they are concerned about the new types of technology that they will need to install to allow them to cope with the new demands from Government. For example, they are concerned that many in the industry will have to install new filtering systems to help companies deal with the vast amount of data they now have to retain. It is difficult even to question the feasibility of such demands due to the limited information and detail provided by the Home Office.

3.45 pm

The Home Office has said that companies will be reimbursed for the additional cost placed on them, but that commitment does not appear in the Bill. These companies, large and small, are being asked to make a significant investment into their operations and all they have from the Government is an IOU. They may have to invest significant capital in the event of this Bill passing; they will need something more concrete than an IOU from the Home Secretary. The Government have earmarked £175 million for a reimbursement fund to help these companies to meet the cost of their new responsibilities. However, most in the sector believe that that sum will barely scratch the surface. The Government need to understand what they are asking these companies to do and come up with a true reflection of what it will cost. The companies themselves estimate that the cost of implementing ICRs could reach over £1 billion. I accept that the Government do not want the industry to pick up the tab for these new costs, but it is unfair to demand a blank cheque from the taxpayer without being open and honest about the possible costs involved.

It is also important that we look at other places that have attempted to introduce similar powers, to find out whether we can learn any lessons from them. It is unfortunate that a similar scheme of logging data has recently been abandoned in Denmark. Before Government Members jump up and say that ICRs are different, as they have already said many times, I have to point out that their argument to substantiate that point and explain the difference has so far seemed to be "They just are". Without clearly defining what ICRs will be and what will be held, it is impossible for the Government to argue that there is a vast difference in the two schemes. I accept that ultimately there may well be small differences, but we have to examine similar operations in the scrutiny of this one.

The Danish scheme operated for seven years, from 2007 to 2014, and on its abandonment the Danish security services expressed their difficulty making proper and effective use of the large amount of data that had been gathered. It seems that, instead of spending their valuable time locating criminals, the security services will spend most of their time working on spreadsheets and filtering out useless information from data that could be of use. It should also be noted that there have been claims that the Danish model was also proving to be too expensive and that the costs were spiralling out of control. The Danish telecommunications industry association has estimated that the initial investment costs alone for the Danish scheme would amount to 1 billion Danish kroner—a figure that has subsequently been confirmed by Ernst and Young, which was commissioned by the Danish Ministry of Justice.

We also need to consider why the United States—home of the Patriot Act, no less—is dismantling much of its intrusive powers and is going in the opposite direction to the UK. Australia also looked at a similar proposal but quickly learned that it would be a costly and ultimately ineffective way of tackling crime in a digital age. Instead of going out our way to implement these powers on our own, we should be working with the international community to see how we can implement more effective powers—for example, by incentivising the rollout of the IP address protocol IPV6, which would effectively allow any and all devices connected to the internet to have their own fixed IP address, thus taking IP address resolution problems out of the equation.

Lastly, the question whether the Bill is in accordance with the law is up for debate.

3.48 pm

Sitting suspended for a Division in the House.

4.4 pm

On resuming—

Gavin Newlands: This is the first speech I have made in this place that has required an intermission. It has been suggested that I start from the beginning as I cannot remember where I had got to. I am nothing but a crowd pleaser, Ms Dorries, but I have found the place where I left off, so I shall continue.

I was saying that the question whether the Bill is in accordance with the law is up for debate. If this part is left unchanged, Liberty and others suggest that it will be in conflict with human rights law, including breaching the EU charter of fundamental rights and freedoms. In July 2015, the High Court upheld its challenge and struck down sections 1 and 2 of the Data Retention and Investigatory Powers Act 2014, finding them incompatible with the British public's right to respect for private life and communications, and protection of personal data under articles 7 and 8 of the EU charter of fundamental rights.

In addition, we should be mindful that the challenge against DRIPA is ongoing and that the outcome will have an impact on whether this part of the Bill is lawful, although I suspect not. On that basis, I question whether ICRs will do the job the Government intend them to do. The Home Office has become entrenched with regard to ICRs and its fixation with them is clouding its ability not only to look at alternatives, but to assess whether ICRs are proportionate, necessary or in accordance with the law. The SNP believes that ICRs fail those three basic assessments.

I want to quote an unlikely ally, who, in 2009, said in Committee:

"Our consideration of the regulations comes against the backdrop of an increasingly interventionist approach by the Government

[Gavin Newlands]

into all of our lives, seemingly taking the maxim 'need to know' to mean that they need to know everything. Certainly, we need to know what the Government's intentions are in relation to the creation of a new central database, which would create a central store of our electronic communications."—[*Official Report, Fourth Delegated Legislation Committee,* 16 March 2009; c. 6.]

That ally was none other than the right hon. Member for Old Bexley and Sidcup (James Brokenshire), now Minister for Immigration at the Home Office, speaking in a delegated legislation Committee on an EC directive with very similar provisions to parts of this Bill. That statutory instrument was passed by the House, but notable opponents included Members who are now Scottish Secretary, Home Secretary and Minister for Security—the Minister in charge of this Bill.

We in the SNP are mindful of the evidence that has been presented and submitted to the Committee, but it is our opinion, backed up by case law, that the power to retain ICRs is incompatible with the right to privacy and the protection of personal data, and I urge hon. Members to amend the Bill and ask the Government to think again.

The Solicitor General: I am grateful to hon. Members for this important debate, which, although it relates to an amendment, inevitably strayed into what is, in effect, the stand part debate on communications data.

The hon. Member for Paisley and Renfrewshire North set out his case comprehensively, but his arguments relate to measures and proposals that are not before the Committee. We have moved a long way from 2009, and certainly from 2012, when the original draft Bill was considered by a predecessor Joint Committee. We are not in the situation where the Government will hold a centralised database. That sort of measure was rightly opposed by my right hon. Friend the Minister for Immigration and other of my hon. Friends at that time, because we are naturally suspicious of an organ of Government directly blanket-holding such data.

That is why this provision is not remotely like that. It does not contain anything like the provisions that the hon. Gentleman rightly cautions against, most importantly because the retention of that data is not in the hands of Government. That arm's length approach is a key difference, which I am afraid undermines all the seeming quality of his argument.

Gavin Newlands: I thank the Solicitor General for giving way. Will the series of private databases under the Bill be any safer from hacking than a central Government database?

The Solicitor General: The hon. Gentleman makes a proper point about security. This, in respect of the code of practice and in collaboration with the industry, will be at the forefront of everybody's mind. What is important is that the Government do not have a pick-and-mix or help yourself avenue within which they can mine data for their own capricious purposes.

The framework of the Bill quite properly severely circumscribes the circumstances within which the Government can seek access to that material. Most importantly, when it comes to content, the warrantry system—the world-leading double lock system we are proposing—will apply. An internet connection record is not content; it is a record of an event that will be held by that telecommunications operator. It relates to the fact of whether or not a customer has connected to the internet in a particular way. If it goes further into content, the warrantry provisions will apply. It is important to remember that framework when determining, and describing and putting into context, what we are talking about. The Committee deserves better than indiscriminate shroud-waving about prospects and concerns that simply do not arise from the measures in the Bill.

The hon. Gentleman quite properly raised the Danish experience. The Danish Government and authorities are in regular conversation with the United Kingdom Government. That dialogue goes on because they are naturally very interested to see how our model develops, although there are important differences that should be set out briefly. The Danish legislation was not technology neutral, unlike these proposals, because it specified two options that proved unworkable. We work with operators case by case so that the best option for their network at the appropriate time will be determined. The Bill builds on existing data retention requirements, such as the retention of data necessary to resolve IP addresses, which regime already exists under the Counter-Terrorism and Security Act 2015. The full cost recovery underpinning by the Government means that there is no incentive for communication service providers to cut corners, as I am afraid happened in Denmark. There are important differences between the two.

The hon. Gentleman rightly talks about IPR6. Although it is a great aim and something that all of us who have an interest in this area will have considered carefully, it still is, with the best will in the world, a way away, I am afraid. It will take a long time for all service providers to implement in full, and until then, there will be both types of system. Even with IPR6, CSPs may choose to implement address sharing or network address translation, meaning that it is not the guaranteed solution that perhaps has been suggested. Servers who host illegal material are much less likely to move to that system, meaning that, in practice, IPR4 may well remain with us. We therefore have to act in the interim, because, as has been said, the drift away from what I have called conventional telecommunications to the internet carries on whether we like it or not. We have to face up to the world as it is, rather than the world as we would love it to be, and therefore take into account the fact that we are in danger of being unable to detect criminality and terrorism.

Joanna Cherry: The Solicitor General says we have to face up to the world as it is. Why is it, then, that no other democratic nation in the world is implementing legislation of this sort?

The Solicitor General: The hon. and learned Lady has asked that question before, and I have said to her before that somebody has to step up, try it and make that change. I am proud that the United Kingdom is prepared to do that, as we have done it in so many ways.

Joanna Cherry: Is the Solicitor General aware that it is not that other countries have not looked at the problem? They have looked at the problem and decided that this is not the way to solve it.

The Solicitor General: I am afraid I do not agree with the hon. and learned Lady. What they have looked at is the sort of centralised, Governmental-based database that all of us have quite properly rejected. They are looking with interest to see how this particular proposal develops, bearing in mind that it has now been refined through many Committees of the House. Accordingly, I think what we are doing is innovative, world leading and, with its technology-neutral approach to the definitions, striking the right balance.

The problem with the amendment as I see it is not only that it is technically deficient, but that, on close reading, it does not exclude the retention of internet connection records, because it talks about the sender and recipient of communications, which is either end of the communication we are talking about when it comes to ICRs. Let us assume that that is an error. Even if we consider its intention at face value, the problem with going back to the 2009 regulations is that we are returning to the language of dial-up—the sort of non-broadband, non-mobile internet access we were all used to 15 years ago, but which now belongs in a museum. If we imprison ourselves in that sort of language, the danger that I have outlined becomes very real.

What next? Are we going back to the telex or the marconigram? We have to make sure that the language of the Bill keeps pace with the breathtaking scale of technological change. In the words of the hon. Member for Paisley and Renfrewshire North, the amendment just does not cut the mustard and I urge that it be withdrawn.

4.15 pm

Gavin Newlands: I hear what the Minister has to say but I am not assuaged by his comments, so this shroud-waver would like to press the amendment to a vote.

Question put, That the amendment be made.

The Committee divided: Ayes 2, Noes 9.

Division No. 26]

AYES

Cherry, Joanna	Newlands, Gavin

NOES

Atkins, Victoria	Hoare, Simon
Buckland, Robert	Kirby, Simon
Davies, Byron	Stephenson, Andrew
Frazer, Lucy	Warman, Matt
Hayes, rh Mr John	

Question accordingly negatived.

Clause 78 ordered to stand part of the Bill.

Clause 79

Matters to be taken into account before giving retention notices

Keir Starmer: I beg to move amendment 175, in clause 79, page 62, line 34, at end insert—

"() the public interest in the protection of privacy and the integrity of personal data; and

() the public interest in the integrity of communications systems and computer networks.".

Clause 79 sets out those matters to be taken into account before giving a retention notice, as well as likely benefits and the likely number of users. Amendment 175 would add two public interest matters to that list. My argument is similar to the one I made on other provisions. Where matters are to be taken into account, it is important that the protection of privacy and the integrity of personal data and of communications systems are specifically listed. I have moved to a position of thinking that an overarching privacy clause is probably the way to achieve this end; this is therefore a probing amendment and I will not press it to a vote.

The Solicitor General: I am grateful for the way in which the hon. and learned Gentleman states his case. To put it extremely simply, we would argue that the public interest in the protection of privacy and in the integrity of personal data are already factored in by the provisions of the Bill.

First, proportionality must include consideration of the protection of privacy. Secondly, the integrity of personal data being such an important public interest is why clause 81 requires any retained communications data to be of at least the same integrity as the business data from which they are derived. A retention notice will therefore not be permitted to do anything that would undermine the integrity of the data that the operator already holds for business purposes. That is all I want to say about the matter, but I assure hon. and learned Gentleman that those important considerations are at the heart of the processes we have followed.

Keir Starmer: I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Clause 79 ordered to stand part of the Bill.

Clause 80

Review by the Secretary of State

Keir Starmer: I beg to move amendment 179, in clause 80, page 62, line 40, leave out "Secretary of State" and insert "Judicial Commissioner".

The Chair: With this it will be convenient to discuss the following:

Amendment 190, in clause 80, page 63, line 7, leave out "Secretary of State" and insert "Judicial Commissioner".

Amendment 191, in clause 80, page 63, line 8, leave out "Secretary of State" and insert "Judicial Commissioner".

Amendment 192, in clause 80, page 63, line 10, leave out "Secretary of State" and insert "Judicial Commissioner".

Amendment 195, in clause 80, page 63, line 25, leave out "Secretary of State" and insert "Judicial Commissioner".

Amendment 196, in clause 80, page 63, line 31, leave out "Secretary of State" and insert "Judicial Commissioner".

Keir Starmer: As members of the Committee will have observed, these tidying-up amendments are consistent with previous amendments that would have entrusted decision making to a judicial commissioner rather than the Secretary of State. We had the discussion in principle in relation to those earlier amendments, which I withdrew, and I will not repeat my arguments now, although I would like to return to them at a later stage.

Joanna Cherry: As the hon. and learned Gentleman says, the amendments would require that review under clause 80 be by a judicial commissioner rather than the Secretary of State. Will the Government tell us why the provision of such a route of review would not, in their opinion, give the telecommunications providers greater reassurance that notices are not only lawful, necessary and proportionate but stable and legally certain? It seems to me that a review by a judicial commissioner, or at the very least by the Investigatory Powers Commissioner, would provide that reassurance.

The Solicitor General: The hon. and learned Lady asks a perfectly proper question. I reiterate the position that we have taken in principle: the Secretary of State is the appropriate and accountable person to be responsible for reviewing retention notices. However, although the Secretary of State must be responsible for giving notices and must therefore be the person ultimately responsible for deciding on the outcome of the review, that does not mean that she or he can make the decision on the outcome of the review without consultation—far from it.

Clause 80(6) ensures that the Secretary of State must consult both the Investigatory Powers Commissioner and the technical advisory board. The commissioner must consider the proportionality of the notice; the board must consider the technical feasibility and financial consequences of it; and both must consult the operator concerned and report their conclusions to the operator and the Secretary of State. Only then can the Secretary of State can decide whether to vary, revoke or give effect to the notice. That system provides rigorous scrutiny of the notice and maintains the accountability of the final decision resting with the Secretary of State. We therefore believe it is the best mechanism for review. Accordingly, I commend the unamended clause to the Committee.

Keir Starmer: I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Clause 80 ordered to stand part of the Bill.

Clause 81

DATA INTEGRITY AND SECURITY

Question proposed, That the clause stand part of the Bill.

Christian Matheson: I seek the Minister's guidance. Throughout our considerations, I have spoken of my fears whether data held under this Act are held securely. I hope that clause 81 will address many of my fears; I seek the Minister's advice on whether it lays responsibility on communications providers to maintain those data securely. I simply reiterate my concern that when theft does take place, there has to be a consideration of an offence of unlawful possession of stolen data, on the basis that the communications provider that has suffered the theft would also be legally responsible for that theft when the provider is in fact a victim of the theft itself. Bodies that seek to obtain illicitly a person's private communications data may try to make financial gain as a result. Is the Minister confident that clause 81 gives me the kind of assurances that I have been looking for on internet security? Is there sufficient deterrent, in terms of possession of unlawfully obtained data, that might be included later in the Bill?

The Solicitor General: The hon. Gentleman has been consistent in stating his concerns. I assure him that clause 81 contains the sort of requirements that he would reasonably expect. It sets out the matter clearly. It should be read in conjunction not only with other legislation that I have mentioned, such as the Data Protection Act 1998 and the Privacy in Electronic Communications Regulations 2003, but with clause 210, which provides for the Information Commissioner to audit the security, integrity and destruction of retained data, and the codes of practice to which I referred earlier. The provisions in the communications data draft code of practice go into more detail about the security arrangements.

We had a discussion some days ago about the existence of adequate criminal legislation. The Bill has a number of provisions that relate to those who hold data, and we discussed whether existing legislation could cover those who come into possession of the data unlawfully. I say to the hon. Gentleman that I will take the matter away and consider it, and come up with a proper considered response to his query.

Question put and agreed to.

Clause 81 accordingly ordered to stand part of the Bill.

Clauses 82 and 83 ordered to stand part of the Bill.

Clause 84

ENFORCEMENT OF NOTICES AND CERTAIN OTHER REQUIREMENTS AND RESTRICTIONS

Keir Starmer: I beg to move amendment 225, in clause 84, page 65, line 20, after "not", insert ", without reasonable excuse,".

There are two points to make here. One is to state the principle that reasonable excuse defences are needed to protect those who are exposed in wrongdoing. We had that debate last week and I listened carefully to the response given. The practical reason is the inconsistencies may be intentional, or they may be unintentional. Clause 73(1), under which unlawful disclosure is made an offence under part 3, has a "without reasonable excuse" provision. Clause 84, which is in part 4, does not. There may be a very good reason for that, but it escapes me at the moment. That is either a point that the Solicitor General can deal with now, or I am happy for him to deal with it later on. It may be just one of those things when you draft a long, complicated Bill, but there is an inconsistency of approach here, because reasonable excuse is sometimes written in and other times not, for no apparent reason.

The Solicitor General: The hon. and learned Gentleman askes what the policy objective is of not having such a defence. The clear policy underlining this is the Government's policy of not revealing the existence of data retention notices. They are kept secret because revealing their existence could damage national security and hamper the prevention and detection of crimes, because criminals may change how they communicate in order to use a provider that is not subject to data retention requirements. Clause 84 places a duty on providers not to reveal the existence of notices.

4.30 pm

Keir Starmer: Just to be clear, I do not need to be persuaded about the policy objective of a clause that keeps a retention notice safe. It is the policy objective of not having a "reasonable excuse" defence to the provision, which operates as an exclusion to the prohibition, of which I need to be persuaded. I do not need persuading about the prohibition for safety.

The Solicitor General: I was coming to that. We are talking about a duty here; the earlier clause the hon. and learned Gentleman referred to is an offence. That will, I think, explain the importantly different context.

To deal with the question of "reasonable excuse", the problem is that once the information is out in the public domain, it cannot be withdrawn—whether that information has been introduced with good or bad intentions does not matter. It cannot be right for the Bill to allow a person to release sensitive information in that way and then subsequently rely on a "reasonable excuse".

May I deal with clause 84(4), which is relevant to this provision? It provides an exemption where the Secretary of State has given permission for the existence of the notice to be revealed. The Government intend that such permission would be given, for example, where a provider wishes to discuss the existence of their retention notice with another provider subject to similar requirements. Should the operator wish to reveal the existence of the notice, they should discuss the matter with the Secretary of State, and in such circumstances permission is likely to be given. There will be those sort of scenarios, as I am sure the hon. and learned Gentleman will understand, and they will help improve the operational model.

My concern about using the "reasonable excuse" provision in the context of a duty would be that it would undermine the important policy objective that I have set out. For that reason I would urge the hon. and learned Gentleman to withdraw the amendment.

Keir Starmer: I will withdraw the amendment. As to the difference between a duty and an offence, I understand that in principle, but I am pretty convinced that elsewhere in the Bill a breach of the duty becomes an offence, as otherwise it is an unenforceable provision, so I am not sure it is a distinction that withstands scrutiny. That being said, I am not going to press this to a vote. It would be helpful and reassuring if the Solicitor General would agree to set out the route by which a whistleblower brings this to attention. I think we have already agreed in general terms and it may come within the umbrella of the undertaking that has been given; if it does, all well and good. That would reassure those that have concerns about exposing wrongdoing. I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Keir Starmer: I beg to move amendment 223, in clause 84, page 65, line 21, after "person", insert

"except the Investigatory Powers Commissioner or a Judicial Commissioner".

The Chair: With this it will be convenient to discuss amendment 224, in clause 84, page 65, line 26, leave out "Secretary of State" and insert "Investigatory Powers Commissioner".

Keir Starmer: These amendments were consistent with earlier amendments that have now been withdrawn, the purpose of which was to put the decision-making power in the hands of the Investigatory Powers Commissioner or the judicial commissioner. The other amendments having been withdrawn, I will not press these to a vote; they do not make sense within the unamended Bill as it now stands.

The Solicitor General: We have already discussed the importance of protecting the identities of those companies subject to data retention notices, but there are circumstances where a telecommunications operator should be able to disclose the existence of a retention notice. Clause 84 allows the Secretary of State to give them permission to do so. The amendment would ensure that a telecommunications operator could disclose the existence or content of a retention notice to the IPC without the need for permission to be given. I would say the proposal is unnecessary, because it is absolutely the Government's intention to give telecommunications operators permission to disclose the existence and content of the retention notice to both the relevant oversight bodies—the IPC and the Information Commissioner—at the point at which a notice is given. In any event, clause 203 as drafted would permit the telecommunications operator to disclose a retention notice to the IPC in relation to any of his functions.

Amendment 224 would mean that the IPC, not the Secretary of State, would be granting permission for a telecoms operator to disclose the existence of the notice. In practice the Secretary of State would consider, at the point that a retention notice was issued, to whom the telecommunications operator could disclose the existence of a notice. It would not make any sense for this issue to be considered separately by the commissioner following the issue of a notice by the Secretary of State.

Further requests by a telecommunications operator to disclose a retention notice are likely to cover administrative matters, such as disclosure to a new systems supplier. Such matters should appropriately be considered by the Secretary of State. I think that explanation not only justifies opposition to the amendments, which I know are being withdrawn, but supports clause 84.

Keir Starmer: I have nothing further to add, so I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Keir Starmer: I beg to move amendment 226, in clause 84, page 66, line 15, at end insert—

"(2B) No notice shall be served under subsection (1) where the relevant telecommunications operator outside the United Kingdom.

(a) is already subject to a comparable retention requirement in the country or territory where it is established, for the provision of services, or

(b) where there is no comparable retention requirement under its domestic law, any extraterritorial requirement is limited to the making of preservation requests to the telecommunications operator."

Committee members will understand why this amendment has been tabled. It reflects the concerns of those who will be caught by these provisions in cases where a comparable retention requirement exists in the country in which they are working. The provisions in this part of the Bill are unnecessary in relation to them. That is the amendment's intention and purpose.

Mr Hayes: I think we can deal with this briefly. I entirely agree with the hon. and learned Gentleman: where it was neither necessary nor proportionate to attempt to retain data in another place, we would not do so, so that is very straightforward. All data retention notices that are given to telecommunications companies, whether here or abroad, must pass the test of necessity and proportionality. Where they did not do so, it simply would not happen, because it would not be necessary, so for that purpose the amendment is unnecessary.

The second part of the amendment would remove the ability to serve data retention notices on telecommunications operators in countries that do not have a comparable data retention regime. Of course, the fact that they do not have a comparable data retention regime does not necessarily mean that there are no data to obtain, and I think that this part of the hon. and learned Gentleman's proposal would add rigidity where flexibility is needed. I accept that there are not always comparable systems, but that does not mean that no system of any kind prevails. Again, with the caveat of proportionality and the proven need established, I think it would be unhelpful to limit our capacity to take action as necessary in the way that he suggests. The same could be said of the third element of his proposal, which is about the preservation of data. When there are no data to preserve, this does not really apply, but when there are, we need at least the capacity, born of the flexibilities provided by the Bill, to take action as is necessary and reasonable.

Keir Starmer: I am grateful to the Minister. I am sure that those who have the primary concern here will take some comfort from what is said about necessity and proportionality but, in practice, where there are comparable retention requirements in the country, it will rarely, if ever, be necessary or proportionate. Obviously, that will have to be determined case by case, or authorisation by authorisation, but I note what he has said on the record. I therefore beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Clause 84 ordered to stand part of the Bill.

Clause 85 ordered to stand part of the Bill.

Clause 86

EXTRA-TERRITORIAL APPLICATION OF PART 4

Question proposed, That the clause stand part of the Bill.

Joanna Cherry: The clause relates to extraterritorial effect and the SNP's opposition is for the same reasons as outlined in relation to clause 76.

Question put, That the clause stand part of the Bill.

The Committee divided: Ayes 9, Noes 2.

Division No. 27]

AYES

Atkins, Victoria	Hoare, Simon
Buckland, Robert	Kirby, Simon
Davies, Byron	Stephenson, Andrew
Frazer, Lucy	Warman, Matt
Hayes, rh Mr John	

NOES

Cherry, Joanna	Newlands, Gavin

Question accordingly agreed to.

Clause 86 ordered to stand part of the Bill.

Clause 87 ordered to stand part of the Bill.

Clause 88

WARRANTS UNDER THIS PART: GENERAL

Keir Starmer: I beg to move amendment 381, in clause 88, page 66, line 38, leave out "information" and insert "specified data".

This amendment seeks to more clearly outline what material may be obtained by hacking.

The Chair: With this it will be convenient to discuss amendment 382, in clause 88, page 67, line 40, leave out from "6" to end of line 43.

This amendment requires that an examination warrant is required for the examination of all data, removing the exception of equipment data and the broad category of 'not private information' which is collected under bulk warrants.

Keir Starmer: We need to spend some time on this clause, because it is the one that deals with equipment interference under part 5. There are real concerns about the breadth of the clause, which provides for two kinds of warrant: a targeted equipment interference warrant and a targeted examination warrant. Those warrants allow interference with equipment, such as remote—not always remote—interference with equipment with your, my and many other people's equipment, Ms Dorries, to secure any of the purposes under subsection (2).

The warrants allow others to interfere with our communications data equipment to obtain "communications", "equipment data" or, to draw attention to subsection (2)(c), "any other information"—to hack into or interfere with equipment to obtain unlimited "any other information". That is why the amendment seeks to limit subsection (2)(c) to "any other specified data". In other words, the clause as drafted will in effect allow interference for pretty well any purpose, as long as it is to obtain information from your computer, my computer, my laptop, your laptop and so on. The provisions are very wide.

The equipment interference in subsection (4) includes interfering by

"monitoring, observing or listening to a person's communications or other activities"

or

"recording anything which is monitored, observed or listened to."

Let us pause there and reflect on how wide the provision is. In terms of invasion of privacy, that will put an incredibly powerful provision in the hands of those who will operate these measures.

4.45 pm

Mr Hayes: I intervene merely because I know that the hon. and learned Gentleman is as much a stickler for accuracy as I am and is perhaps even less prone to hyperbole than me. He will therefore want the Committee to consider the draft code of practice, particularly where it deals with exactly the matters to which he is referring. I will discuss this at greater length than an intervention will allow in a moment, but he will see in the draft code of practice a comprehensive list of qualifications to the breadth that he is outlining.

Keir Starmer: I am grateful for that intervention. I have been referring throughout to the code of practice and its role. Consistent with the in-principle argument I have been making, the Bill and the code serve different functions. I understand the argument that a code is one way not only to give more detail to the provisions in the Bill, but to future-proof it. In other words, a code allows an approach that can be changed without amending the legislation.

As a matter of principle, though, I argue that where limits are to be put on the exercise of the power, and thus important safeguards are in place, they should be in the Bill. What should be resisted is a wide and generalised power in the Bill that finds constraint and limitation only in the code of practice. The extent of these powers should be set out in the Bill. The code of practice is the place for more detailed provision—provision that may change over time—and other obvious future-proofing techniques; it is not the right place for the limitations themselves.

Moving on, consistent with the earlier clauses on warrants, subsection (5) allows conduct in addition to the interference itself in order to do what is expressly authorised or required and any conduct that facilitates or gives effect to the warrant. I now want to take a bit of time on subsection (6).

Mr Hayes: Given the hon. and learned Gentleman's desire to move on, and so that he can do so with greater velocity, let me be absolutely clear that the clause would not allow warrants to be issued without the information being sought being specified.

Keir Starmer: I am grateful for that intervention. It is helpful to have such matters on the record so that others can follow how the clauses are intended to operate.

Returning to subsection (6), one of the welcome measures in the Bill is that clause 3(4) makes it clear that, when a communication is intercepted, interception includes the communication at

"any time when the communication is stored in or by the system".

I know that sounds very technical, but it became a real issue in a number of cases in which the question was whether a voicemail that was accessed once it was on a voicemail machine was in the course of its transmission. If the answer to that was no, there was nothing unlawful about retrieving it, listening to it and publishing it. A lot of time and energy went into the interpretation of the relevant clause. One of the advantages of the Bill is that clause 3 spells out in no uncertain terms that communications are protected if they are intercepted in the course of transmission, including if stored either before or after transmission. That protects any communication, sent to us or anybody else, which is either listened to at the time or not, but is later stored either in a voicemail, on a computer or in any way. We all store communications all the time; it is very rare that they exist only in real time. That is a step in the right direction.

We then get to clause 88(6):

"A targeted equipment interference warrant may not, by virtue of subsection (3), authorise or require a person to engage in conduct, in relation to a communication other than a stored communication".

It protects the communication and excludes its content from this part—I think that is the idea—but only half does the job and leaves quite a gap, in my view. We get back to the same problem. If there is equipment interference to obtain a communication, that communication would be protected from one of these warrants as long as it is in the course of its transmission. If it has arrived, it is not. If I am wrong about this I will stand corrected, but all of the good that was done by amending clause 3 will be undone by clause 88; the same ends could be achieved by using an equipment interference warrant, namely obtaining by interference a communication that is in the course of its transmission, either before or after it is sent.

Mr Hayes: I am grateful to the hon. and learned Gentleman for his humility in suggesting that he would stand corrected; I now stand to correct him. An equipment interference warrant would not allow interception of real-time information of the kind that he describes. He is right that to intercept that kind of information would require a different process, as we discussed earlier in our considerations. If further explanatory notes need to be made available to provide greater clarity about that I am more than happy to do so. I will talk more when I respond, before you rightly chide me for going on for too long, Ms Dorries.

Keir Starmer: I am grateful to the Minister. If he could point to the provision that makes good the submission he has just made, then that will deal with this particular point. Just to be clear, subsection (6) is intended to ring-fence and exclude from one of these warrants communications the interception of which would

"constitute an offence under section 2(1)",

but only in relation to communications in the course of their transmission in the real sense of the term, not including those that are "stored". I put on the record—if this is capable of being answered, so be it—that "stored" in subsection (6) has the same meaning as in clause 3, which is intended to include stored communications within the prohibition. I will not take it any further; the Minister has my point, which is that one would expect subsection (6) to protect the same content that is expressly protected by clause 3(4), but it does not—unless he or

[Keir Starmer]

somebody else can point to another provision that adds to subsection (6), though that would be an odd way of doing it.

I will move on. Subsection (9) defines targeted examination warrants. This is important because subsections (1) to (8) deal with targeted equipment interference warrants—warrants issued in a targeted way; the targeted examination warrant deals with examining material obtained by way of a bulk warrant. It therefore serves a different purpose. Subsection (9) is an extremely wide provision:

"A targeted examination warrant is a warrant which authorises the person to whom it is addressed to carry out the selection of protected material…in breach of the prohibition in section 170(4)".

To understand that, we need to turn to section 170(4), which raises questions that relate to an argument I made earlier on another, not dissimilar, provision. It states:

"The prohibition…is that the protected material may not…be selected for examination if (a) any criteria used for the selection of the material for examination are referable to an individual known to be in the British Islands at that time, and (b) the purpose of using those criteria is to identify protected material consisting of communications sent by, or intended for, that individual or private information relating to that individual."

That is intended to give protection to individuals known to be in the British islands, by placing limits on the examination of their material: in relation to their material or their communications one needs a targeted examination warrant to get around the prohibition in clause 170(4). The point I make here is similar to the point that I made before: this is temporal. Whether a person is in the British islands or not depends on where they are physically. I am protected so long as I am in the British islands, but I fall out of protection—as would everybody else—the moment I leave them, whether I am leaving for a day, a week, a month or a year. That is a real cause for concern, as is the wide definition of protected material that immediately follows in clause 88(9); amendment 382 would limit the extent of that definition by stopping the clause after the words "Part 6", which are on page 67, line 40, of the draft Bill.

In conclusion, this is a very wide-ranging clause, and it contains insufficient safeguards—if there are safeguards, they should be in the Bill. There are questions on subsections (6) in (9), taken in conjunction with clause 170(4), that the Minister will have to deal with.

Joanna Cherry: I rise to support the hon. and learned Gentleman in his submissions on these two amendments. As we have just reached part 5, I want to take the opportunity to make some general comments on it. Powers to conduct equipment interference—or "hack", which is the more generally used term—are new; they do not exist in any previous legislation. They therefore require significant scrutiny, by the Committee and by parliamentarians generally, before they are added to the statute book. By its very nature, hacking is an extremely intrusive power, because it grants the authority to see all past and future information and activity on a computer or other device. Beyond the implications for privacy, the potential ramifications for the whole country's cyber-security and for fair trials mean that hacking should be used only as a tool of last resort. The SNP's position is that stronger protections must be added to the Bill.

5 pm

As the hon. and leaned Gentleman has already explained in his characteristically succinct way, the powers afforded by clause 88 are extremely wide. Even with these amendments, this part of the Bill contains very wide powers. Warrants can last for up to six months and can be renewed potentially indefinitely. The warrant applications will be subject to what we argue is a weak system of judicial review. The warrants for interference can be modified by Ministers without the approval of a judicial commissioner, and a modification can include changing the name, descriptions and scope of the warrant. Chief constables are required to have their decisions to modify warrants reviewed by a judicial commissioner unless they consider the modification to be urgent.

Hacking is potentially very intrusive. It is more damaging than other forms of traditional surveillance, such as bugging and the interception and acquisition of communications data. Uniquely, hacking grants the hacker total control over a device. Phones and computers can be turned on or off, their microphones and cameras can be activated, and files can be added or deleted, all of which can be done without the fact of the hack being known or knowable to the target.

The potential for the intrusiveness of hacking is intensified in the digital age, when our computers and mobile devices have replaced and consolidated our filing cabinets, photo albums, video archives, personal diaries, journals, address books, etc. Devices may contain not only details about the user's personal circumstances, age, gender and sexual orientation but financial information, passwords and possibly privileged legal information. Hacking is perhaps more comparable to searching a house than to intercepting.

With hacking come considerable security concerns. When malware is deployed, there is often a risk of contagion, both overseas and at home. We have seen many examples of that internationally in recent years. We as parliamentarians should consider the cost of widespread hacking by the authorities. Hacks create and maintain permanent vulnerabilities that can be exploited by criminal elements. For example, to use colloquial language, if the good guys hack into a device, it makes it easier for the bad guys to hack in after them. We are all well aware of the risks and costs of cybercrime to the British economy.

Hacking also has repercussions for fair trials. Because hacking, by its nature, can require the alteration of the content on a target device or network, new questions are raised about the potential for electronic surveillance to undermine the integrity of a device or material located on a device that could later be sought to be used in evidence in a criminal or a civil trial. At present, there is no specific regulation of the use of hacking product in criminal trials, and none has been presented in the Bill or the code of practice.

Liberty and Justice, among others, suggested that in recognition of the unique potential of hacking capabilities and to avoid future miscarriages of justice and collapsed trials, the Bill should contain proposals to ensure audit trails and police disclosure where prosecutions result from investigations that have utilised hacking capabilities. That is in all of our interests so that we can fairly and effectively try those who subsequently turn out to be guilty.

Any amendments that the SNP table to part 5 of the Bill are against the background of those concerns. It is because of them that I support the hon. and leaned Gentleman's arguments in support of amendments 381 and 382.

Mr Hayes: As the shadow Minister said, part 5 of the Bill is very important. It deals with equipment interference. He is right to say that equipment interference is, by its nature, quite a radical technique—I will explain that in a few moments—but of course it is for a purpose. It fulfils a proper function and allows those missioned to keep us safe to do so by means of the exercise of that power.

Let me deal with the hon. and learned Lady first. I thought that her contribution—I say this kindly because, despite all of my instincts, I cannot help liking her—*[Interruption.]* Someone said "saintly instincts". I would not go as far as to say "saintly"; I would say "wholesome instincts". I thought that her speech exemplified the curious cocktail at the heart of Scottish nationalism: a mix of paranoia and assertiveness.

I have two things to say in response to her. First, these powers are not new; they already exist in the Intelligence Services Act 1994 and the Police Act 1997. Secondly, the exercise of those existing powers has been scrutinised. They are particularly used by GCHQ.

The Chair: Order. There is a Division in the House. We will suspend for 15 minutes, or 25 if there are two. Be back as quickly as you can if there are three.

5.5 pm

Sitting suspended for Divisions in the House.

5.30 pm

On resuming—

Mr Hayes: Having characterised the Scottish National party in a vivid and, in some people's view, slightly too generous way, I will move on to the specifics of what the hon. and learned Lady said. She is right that there need to be important safeguards in respect of equipment interference. I do not think that there is any difference between us on that. She is right that GCHQ's use of equipment interference powers—although they are more widely available, it is GCHQ that uses them particularly—are central to its purpose and of course must be lawful. She will be pleased to know that the Investigatory Powers Tribunal found them to be just that when it looked at the matter as recently as February of this year. Of course it is right, given the radical character of those powers, that we put in place all the right checks and balances. One might say that transparency and stronger safeguards are part of what the Bill is defined by.

It is important to emphasise in that context the draft codes of practice, which I drew attention to in a brief intervention on the hon. and learned Member for Holborn and St Pancras. They are clear in two respects. I draw attention first, in general terms, to part 8 of the draft code of practice on equipment interference, which deals with handling information, general safeguards and so on, and secondly to the specific areas covered in part 4.10, which lists an extensive series of requirements for the information that a targeted equipment interference warrant should contain. I will not go through them exhaustively, Ms Dorries, because that would please neither you nor other Committee members. Suffice it to say that such a warrant should contain details of the purpose and background of the application, be descriptive and clearly identify individuals where that can be done. Those requirements also necessitate an explanation of why equipment interference is regarded as essential and refer to conduct in respect of the exercise of such powers, collateral intrusion, and so on. They are pertinent to the consideration of the clause.

There is always, as I predicted there would be in this case, a debate in Committee about what is put in the Bill and what is put in the supporting material. As you will be familiar with, Ms Dorries, having been involved in all kinds of Committees over time, Oppositions usually want more in Bills and Governments usually want more flexibility. Perhaps that is the nature of the tension between government and opposition. I have no doubt that were the Labour party ever to return to Government, the roles would be reversed; we would be the ones saying, "More in the Bill," and that Labour Government would probably be arguing for more flexibility. The truth lies somewhere between the two: of course it is important to ensure that there is sufficient in the Bill both to ensure straightforward legal interpretation and to cement the safeguards and protections for which the hon. and learned Gentleman rightly calls, but in achieving those ends one must always be careful that specificity does not metamorphose into rigidity. Where we are dealing with highly dynamic circumstances, changing technology and, therefore, changing needs on the part of the agencies and others, rigidity is a particular worry.

In the Bill as a whole, and in this part of the Bill, we have tried to provide sufficient detail to provide transparency, navigability and a degree of resilience to legal challenge while simultaneously providing the flexibility that is necessary in the changing landscape. That is why the codes of practice matter so much, particularly in respect of this clause and these amendments, and it is why the codes of practice have changed in the light of the consideration of the Joint Committee of both Houses, and others. It is also why I predict—I put it no less strongly than that—that the codes of practice will change again as a result of the commentary that we have already enjoyed in Committee and will continue to provide over the coming days.

The need for equipment interference could not be more significant, and I will explain what it comprises. Equipment interference is a set of techniques used to obtain a variety of data from equipment that includes traditional computers, computer-like devices—such as tablets, smartphones, cables, wires—and static storage devices. Interference can be carried out remotely or by physically interacting with the equipment. Although equipment interference is increasingly important for the security, intelligence and law enforcement agencies, it is not new. Law enforcement agencies have been conducting equipment interference for many years, and I described the legislative basis for that in response to the hon. and learned Member for Edinburgh South West. It is probably fair to say that equipment interference is likely to become still more important as a result of the effect that changes in technology are having on other capabilities. I do not

[Mr John Hayes]

want to overstate this, but encryption, for example, is likely to make equipment interference more significant over time.

I will amplify the clarity with which I delivered my advice to the hon. and learned Member for Holborn and St Pancras. Warrants cannot be issued without specifying what information is being sought, and on that basis it is hard to see why clause 88 should be amended. Chapter 4 of the code of practice states:

"An application for a targeted equipment interference warrant should contain… A general description of any communications, equipment data or other information that is to be (or may be) obtained".

Together, the provisions provide the issuing authority with the information it needs to assess an application and with the power to constrain the authorised interference as it sees fit on a case-by-case basis. Amendment 382 would extend the requirement to obtain a targeted examination warrant to circumstances where the agencies need to select for examination the equipment data and non-private information of an individual who is known to be in the British islands. I tend to agree with the argument made by the hon. Member for City of Chester in an earlier sitting of the Committee that it is right that there are particular provisions for UK citizens in what we do in this Bill, rather than with the argument made by the hon. and learned Member for Edinburgh South West.

Keir Starmer: I just want to clarify my concern, because I think the Minister just said, "UK citizens". I understand that the distinction is made between UK citizens and others. My concern about this provision is that, whether someone is a citizen or not, if they are physically outside of the British Isles they fall outside the protection. That has been my driving concern, or one of my driving concerns, here. There may be a good reason for this and there may be a longer explanation for it, but I was surprised to see in the Bill that the protection was not to British citizens or to some other description of people with the right of residence in this country, but in fact depends on whether someone is physically in the country or not. On my understanding, I lose the protection that is provided by this Bill in this and other provisions if I go to France for a short period of time.

Mr Hayes: To be fair to the hon. and learned Gentleman, the Bill refers to people within "the British Islands", so he is right, and there are very good reasons why enhanced safeguards should apply for the content of people in the UK. As he implied, we explored these issues in an earlier part of the debate.

I will conclude, but I want to do so on the basis of clarifying this matter, too. The subsection that the hon. and learned Gentleman described earlier makes it clear that when a warrant for equipment interference is used to examine a phone, the police can look at all data on the phone, including text messages, but not in real time. I wonder whether there has been a misunderstanding or misapprehension about this issue—either a misunderstanding about the meaning or misapprehension about the purpose.

I repeat this solely for the sake of convincing the hon. and learned Gentleman and others that we are doing the right thing. These are important powers with stronger safeguards with absolute determination to be clear about legal purpose; they can only be used when necessary and can only be used lawfully. They are fundamentally not new but a confirmation of what is already vital to our national interest and to the common good.

Keir Starmer: I am grateful to the Minister for taking us through in some detail how the clause is intended to work with the code of practice. I reiterate my point that the essential safeguards should be in the Bill. Amendments 381 and 382 would not delete the provisions in clause 88; they would tighten the provisions in clause 88, and I intend to push both of them to a vote.

Question put, That the amendment be made.

The Committee divided: Ayes 7, Noes 8.

Division No. 28]

AYES

Cherry, Joanna	Newlands, Gavin
Hayman, Sue	Starmer, Keir
Kinnock, Stephen	
Matheson, Christian	Stevens, Jo

NOES

Atkins, Victoria	Hoare, Simon
Buckland, Robert	Kirby, Simon
Davies, Byron	Stephenson, Andrew
Hayes, rh Mr John	Warman, Matt

Question accordingly negatived.

5.45 pm

Amendment proposed: 382, in clause 88, page 67, line 40, leave out from "6" to end of line 43.—*(Keir Starmer.)*

This amendment requires that an examination warrant is required for the examination of all data, removing the exception of equipment data and the broad category of 'not private information' which is collected under bulk warrants.

Question put, That the amendment be made.

The Committee divided: Ayes 7, Noes 8.

Division No. 29]

AYES

Cherry, Joanna	Newlands, Gavin
Hayman, Sue	Starmer, Keir
Kinnock, Stephen	
Matheson, Christian	Stevens, Jo

NOES

Atkins, Victoria	Hoare, Simon
Buckland, Robert	Kirby, Simon
Davies, Byron	Stephenson, Andrew
Hayes, rh Mr John	Warman, Matt

Question accordingly negatived.

Clause 88 ordered to stand part of the Bill.

Clause 89

MEANING OF "EQUIPMENT DATA"

Keir Starmer: I beg to move amendment 384, in clause 89, page 68, line 13, leave out from "information" to end of line 15.

This amendment acknowledges that "data" relating to the fact of a communication or the existence of information has meaning and must not be exempt from privacy protections afforded to other categories of data.

This amendment deletes the words

"or from any data relating to that fact".

It is important because an equipment interference warrant can permit interference with equipment data, as in clause 88(2)(b). As we have seen, clause 88(9) makes provision for protected material, the definition of which includes equipment data. Over the page, clause 89 deals with the meaning of "equipment data":

"(a) systems data;

(b) data which falls within subsection (2)."

Subsection (2), broadly speaking, refers to systems data as identifying data that is included in, attached to or associated with a communication but that can be separated from it and that, if separated,

"would not reveal anything of what might reasonably be considered to be the meaning (if any) of the communication".

That is a logical way of approaching it. It is data linked to a communication that can be separated from it, but if separated, it would not reveal the meaning of the communication. Thus, it does not undermine the special protection given to the communication.

Then the final part of clause 89(2), paragraph (c), says

"disregarding any meaning arising from the fact of the communication".

As has been said today, the fact of the communication, in many respects, can be as revealing as the content. However, the provision goes on to say

"or from any data relating to that fact",

which broadens even further the exclusion from protection intended for communications.

In that way, the clause undermines the very protection being given to communications, so this short amendment would omit the words that I have indicated, in order to limit the exclusion from protection for the communication.

Joanna Cherry: May I add my supportive comments? This is a joint amendment from the Labour party and the Scottish National party.

5.48 pm

Sitting suspended for a Division in the House.

6 pm

On resuming—

Joanna Cherry: I rise to add my support to amendment 384 on behalf of the Scottish National party. Historically, communications data were considered much less revealing than the content of the communication, and consequently the protections offered to communications data under RIPA were weaker than those existing in the interception regime. However, as communications have become increasingly digital, the data generated are much more revealing and copious than before, allowing the state to put together a complete and rich picture of what a person does and thinks, who they do it with, when they do it and where they do it.

As the Bill stands, clause 88(9) would allow for the examination of potentially vast amounts of data on people in Britain obtained under bulk equipment interference warrants, as vague categories of "data" in 88(9)(a) and (b) are asserted to have no meaning. Data relating to the fact of a communication or the existence of information do have meaning and must not be exempt from the privacy protections afforded to other categories of data.

I urge the Committee to ensure that the Bill does not treat data relating to the fact of a communication or the existence of information relating to that fact as unimportant. In fact, there is extraordinarily high value to such material, precisely because it is highly revealing. It therefore demands equal protection.

Mr Hayes: All these disruptions and delays are adding interest and variety to our affairs. There is a straightforward argument for why the amendment is unnecessary, which I will make. If that is insufficient to persuade the Committee, I will add further thoughts.

The straightforward reason why the amendment is unnecessary is that it would undermine the principle that the most robust privacy protections should apply to the most intrusive kinds of data. I simply do not agree with the hon. and learned Lady that, for example, systems data—the highly technical data that will be separated out as a result of the endeavours in this part of the Bill—are better excluded from those extra protections. The unintended consequence of the amendment—at least, I hope it is unintended—is that it would lead to disproportionate access requirements for less intrusive data. That would be unhelpful and could, through confusion, hamper the work of the services.

Keir Starmer: I want to be clear as to how clause 89 operates, because subsection (2) suggests it is an attempt to identify data associated with a communication that can be separated from the communication, but which, if separated, would not touch on the meaning of the communication, thereby protecting it. That is all good. That is a safeguard, which is supported and welcome, but after the comma, as I read it, disregarded from that protection is everything that follows on. At the moment, I do not follow how the amendment removes protection, because the last bit of clause 89(2)(c) after the comma disregards from the protection and thus leaves unprotected from the scheme of clause 89

"the fact of the communication or the existence of the item of information or from any data relating to that fact."

If I am wrong about that, there is a problem with the amendment, but I understand that part of clause 89(2)(c) to detract from the protection that the subsection is otherwise intending to put in place.

Mr Hayes: Let me see if I can deal with that question specifically. Equipment data include identifying data. Most communications and items of information will contain information that identifies individuals, apparatus, systems and services, or events and sometimes the location of those individuals or events. Those data are operationally critical to the agencies, as the hon. and learned Gentleman understands. In most cases that information will form part of the systems data, but there will be cases where it does not.

[Mr John Hayes]

The work that has been done to separate out and define data has been carefully designed to categorise logically the range of data generated by modern communications. Identifying data are operationally critical. It is important to be able to classify data correctly and coherently throughout the Bill. My assertion, therefore, drawing on the hon. and learned Gentleman's question, is that the amendment would inhibit though not prevent that by making the distinction less clear.

We can talk at length if necessary, although I suspect that at this juncture it is not necessary, about inferred meaning and its importance and relevance here. Misunderstanding frequently arises on inference, but I do not think that that is critical to this particular part of our discussion. My case is that the work we have done in better categorising the difference between the kinds of data assists the application of this part of the Bill, and assists the agencies accordingly. As I said, the amendment, perversely, would afford to those bits of technical data, for example, the same protection that is deliberately granted to more sensitive data under the Bill.

I do not like to do this on every amendment, or we would drown in a sea of paper, but as I write to the Committee regularly, if it would be helpful to cement that point in my next letter, I will happily do so. I am, however, confident that what I have said to the Committee is an accurate reflection of the work that I have described and of the content of the Bill.

Keir Starmer: I am grateful to the Minister, first for spelling out in detail the intended operation of the clause and, secondly, for indicating his willingness to write on the matter. This is something that ought to be in the Bill. My clear reading is that the amendment would not ring-fence anything from examination; it would simply require a warrant under clause 88 if equipment data, having satisfied all the other provisions under subsection (2)(a) to (c), included anything where there was a meaning arising from fact communication and so on. I will therefore press the amendment to a vote.

Joanna Cherry: I have nothing to add in support.

Question put, That the amendment be made.

The Committee divided: Ayes 7, Noes 8.

Division No. 30]

AYES

Cherry, Joanna	Newlands, Gavin
Hayman, Sue	Starmer, Keir
Kinnock, Stephen	Stevens, Jo
Matheson, Christian	

NOES

Atkins, Victoria	Hoare, Simon
Buckland, Robert	Kirby, Simon
Davies, Byron	Stephenson, Andrew
Hayes, rh Mr John	Warman, Matt

Question accordingly negatived.

Clause 89 ordered to stand part of the Bill.

Clause 90

SUBJECT-MATTER OF WARRANTS

Keir Starmer: I beg to move amendment 385, in clause 90, page 68, line 24, leave out paragraph (b)

This amendment, and others to Clause 90, refine the matters to which targeted equipment interference warrants may relate by removing vague and broad categories including "equipment interference for training purposes".

The Chair: With this it will be convenient to discuss the following:

Amendment 386, in clause 90, page 68, line 33, leave out paragraph (f).

Amendment 387, in clause 90, page 68, line 35, leave out paragraph (g).

Amendment 388, in clause 90, page 68, line 38, leave out paragraph (h).

Amendment 456, in clause 90, page 68, line 44, leave out subsection (2)(b).

Amendment 391, in clause 90, page 69, line 1, leave out paragraph (d).

Amendment 392, in clause 90, page 69, line 3, leave out paragraph (e).

Amendment 265, in clause 101, page 78, leave out lines 21 to 27.

Amendment 272, in clause 101, page 79, leave out lines 3 to 7.

Amendment 273, in clause 101, page 79, leave out lines 8 to 12.

Amendment 274, in clause 101, page 79, leave out lines 13 to 18.

Amendment 457, in clause 101, page 79, leave out lines 31 to 36.

Amendment 279, in clause 101, page 80, leave out lines 3 to 7.

Amendment 280, in clause 101, page 80, leave out lines 8 to 12.

Keir Starmer: We move to a different topic within the same general subject matter of thematic warrants.

Clause 90(1) sets out that a

"targeted equipment interference warrant may relate to"

and thereafter follows a long list from paragraph (a) to paragraph (h). Paragraph (a) specifies

"equipment belonging to, used by or in the possession of a particular person or organisation".

Paragraph (b) deals with groups or those

"who share a common purpose or who carry on…a particular activity".

Paragraph (c) deals with equipment

"in the possession of more than one person or organisation, where the interference is for the purpose of a single investigation or operation".

Paragraph (d) deals with

"equipment in a particular location".

And on it goes. In other words, the clause allows a very broad range of matters to be included in what is intended to be a targeted equipment interference warrant.

The evidence from the independent reviewer, David Anderson, was, in essence, that clause 90, or its forerunner, was so wide that he thought it was difficult to suggest anything that could not be included in a thematic targeted interference warrant. That gives rise to the suggestion that, in truth, this is a disguised bulk power. It is called a targeted equipment interference warrant, but it is so wide as to be tantamount to a bulk power. In so far as this sort of interference has been carried out in the past, it has been carried out under provisions of this sort rather than any bulk provision. It is an extremely wide and permissive thematic warrant that allows interference with equipment in a very wide range of circumstances, which of course includes monitoring, observing, listening to and so on. It is far too wide.

Amendments 385 and 386 are intended to cut out part of the wide thematic approach in subsection (1). Subsection (2) deals with a targeted examination warrant, and again there is a wide range of matters that the warrant may relate to, including

"a particular person or organisation…a group of persons"

and so on. As far as subsection (2) is concerned, the examination warrant is to operate in conjunction with or following on from a bulk warrant, so subsection (2) indicates the matters to which such a targeted warrant may relate, notwithstanding the wide breadth of the bulk warrant.

The powers are far too wide and they need to be better specified. The amendments are intended to draw in and narrow the scope of the thematic warrants, because otherwise it is hard to resist David Anderson's conclusion that it is hard to think what would not be included in one or other of the descriptions I have outlined.

6.15 pm

Joanna Cherry: I want to add my voice in support of the hon. and learned Gentleman's suspicions—sorry, submissions! We share suspicions about this clause. The clause, unamended, permits thematic, suspicion-less warrants and these shade into general warrants. General warrants are anathema to the common law of England and Scotland and fall foul of international human rights law.

I am pleased that the hon. and learned Gentleman prayed in aid what David Anderson, QC said about clause 90. If Members have read his supplementary written evidence to the Committee, they will have seen that at paragraph 5a he expressed grave concern about clause 90, describing it as "extremely broad" and continuing:

"The ISC noted this in relation to the EI power in February 2016…The Operational Case lodged with the Bill also acknowledged…that a targeted thematic EI"—

equipment interference—

"warrant may 'cover a large geographical area or involve the collection of a large volume of data'. This matters, because as the Operational Case also acknowledged…the protections inherent in a thematic warrant are in some respects less than those inherent in a bulk warrant. The very broad clause 90 definition effectively imports an alternative means of performing bulk EI, with fewer safeguards. The Government's explanation for this–that it will opt for a bulk warrant where extra safeguards are deemed necessary–may be argued to place excessive weight on the discretion of decision-makers."

That concern—that it gives excessive discretion to decision makers—is one that the Scottish National party has as a thread running through the Bill. David Anderson goes on to say:

"If bulk EI warrants are judged necessary, then it should be possible to reduce the scope of clause 90 so as to permit only such warrants as could safely be issued without the extra safeguards associated with bulk."

Even if the Minister does not consider the SNP's and the Labour party's concerns valid, what does he have to say about the lengthy passage that David Anderson has devoted to the matter in his supplementary written evidence?

Mr Hayes: I spoke earlier about velocity; now I will talk about breadth and speed. I emphasise that the powers in clause 90 are not new. They are existing powers used by law enforcement, for example, in a range of serious criminal investigations.

Joanna Cherry: Will the Minister tell us the legal basis of the existing powers?

Mr Hayes: I have done so already, but I will repeat it for the sake of the record. The powers are contained in the Intelligence Services Act 1994 and the Police Act 1997. I am more than happy to provide more information to the hon. and learned Lady on that detail, should she want me to do so.

Joanna Cherry: I am looking at the 1994 Act and it seems to me that it contains broad and vague enabling powers, which bear no resemblance to the powers in the Bill. Can the Minister contradict that?

Mr Hayes: One of the stated purposes of the Bill is to bring together those powers—to cement them and to put in place extra clarification and further safeguards. I have argued throughout that the essence of the Bill is delivering clarity and certainty. I would accept the hon. and learned Lady's point if she was arguing that, at the moment, the agencies draw on a range of legal bases for what they do, for that is a simple statement of fact. We are all engaged in the business of perfecting the Bill, because we know it is right that these powers are contained in one place, creating greater transparency and greater navigability, and making legislation more comprehensible and more resistant to challenge. That is at the heart of our mission.

I said I would talk about breadth. The breadth of the circumstances in which equipment interference could be used reflects the fact that, at the time of making an application for a warrant, the information initially known about a subject of interest may vary considerably. Last week, we spoke about the kind of case in which there may be an unfolding series of events, such as a kidnapping, where a limited amount might be known at the outset when a warrant is applied for. The warrant's purpose will be to gather sufficient information as to build up a picture of a network of people involved in a gang or an organised crime. That is very common and I intend to offer some worked examples in a number of areas.

Identifying members of such a gang can often come from interception arising from a thematic warrant. That might apply to interception, but frankly it might also

[Mr John Hayes]

apply to equipment interference where that is a more appropriate and more effective means of finding the information. Another example may be a group of people involved in child sexual exploitation. Frequently, partial information will allow for further exploration of a network of people who are communicating over a wide area, and who are careful about how they communicate, mindful of the activity that they are involved in. They will not be easy to discover or find, as they will very often disguise their identity. For that reason, it may be necessary to start by looking at sites commonly used to share indecent images of children and from there uncover information that leads, through the use of equipment interference, to those who are driving that unhappy practice. Those examples are not merely matters of theory; they are matters of fact. I know that in cases of kidnapping and in cases of child sexual exploitation, those techniques have been used and continue to be used.

Keir Starmer: I understand the point the Minister is making and the need for these powers to be practical and effective in real time. He says that they are not theoretical but real, and I absolutely accept that, but David Anderson is someone who will have appreciated that more than many others. He has been working in this field and dealing with those issues for many years. He is hardly likely to make the mistake of theorising about something that he knows about in great detail in the practical examination, so is he just plain wrong when he raises this concern? He has raised it not just once, but on a number of occasions, in detail, and he knows how these things work.

Mr Hayes: I will return to that point because it is important and fair, and I will return to the Anderson critique in a moment, but before I do so, I want to be clear about the second thing that I said I would speak about—speed.

The kind of cases that I have outlined can move rapidly. The information that becomes available from the kind of initial inquiries that I have described, when the character or names of individual actors may not be known but will become known through these techniques, may require law enforcement agencies to act very quickly to avert further serious crime. Owing to the need for speed, it is vital that those missioned to protect us are able to exercise all the powers when they need to, with confidence and lawfully. The Anderson critique is why the codes of practice limit specifically how thematic warrants can be used. I draw the Committee's attention to page 25 of the draft code of practice, which deals with such warrants and defines again, in some detail, exactly how they should be as specific as possible, given the breadth and speed requirements that I have set out.

I hear what is said about the David Anderson criticism. I think that we have gone further in being specific in the code of practice than we might have been expected to by our critics, but, rather as I said in relation to our consideration of an earlier group of amendments on warranting, I do not want to inhibit what is currently done; I do not want the Bill to leave the agencies and law enforcement with fewer powers; I do not want to leave them emasculated as a result of our consideration. It is right that we should have safeguards, definition, constraints and, where necessary, specificity, but these powers are vital to protect us from those who want to exploit our children and do us harm. Criminals are increasingly adaptable and sophisticated, rather like terrorists. We must outmatch them at every turn and I believe that those powers are vital for us to be able to do so. So I am unapologetic about making the case for them to the Committee and to Parliament.

Keir Starmer: I am grateful to the Minister for setting out his case in that way. To be clear, particularly in relation to his last point, I do not think that anyone is suggesting that those powers should not be available. The discussion is about whether they are rightly described as thematic warrants or whether they are, in truth, bulk warrants, which operate in different ways and have different safeguards, procedures and processes to go through. I do not want our challenging and probing to be portrayed as somehow to undermine the work that has to be done by law enforcement and others in real time, often in difficult circumstances.

That said, this is an important issue. I have listened to what has been said and I want to preserve the position. I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Keir Starmer: I beg to move amendment 389, in clause 90, page 68, line 40, at end insert—

"(1A) A targeted equipment interference warrant may only be issued in relation to any of the matters that fall under subsection (1) if the persons, organisations or location to which the warrant relates are named or otherwise identified."

The Chair: With this it will be convenient to discuss the following:

Amendment 458, in clause 90, page 69, line 4, at end insert—

"(2A) A targeted examination warrant may only be issued in relation to any of the matters that fall under subsection (2) if the persons, organisations or location to which the warrant relates are named or otherwise identified."

Amendment 266, in clause 101, page 78, line 18, leave out

"or a description of the person or organisation"

and insert

"or another identifier of the person or organisation".

Amendment 474, in clause 101, page 78, line 27, leave out

"or a description of, as many of the persons or organisations as it is reasonably practicable to name or describe"

and insert

"or another identifier of, each person or organisation".

Amendment 473, in clause 101, page 78, line 28, at beginning insert "The name and".

Amendment 268, in clause 101, page 78, line 31, leave out

"or a description of, as many of the persons or organisations as it is reasonably practicable to name or describe"

and insert

"or another identifier of, each person or organisation".

Amendment 269, in clause 101, page 78, line 36, leave out "description" and insert "specification".

Amendment 270, in clause 101, page 78, line 38, at beginning insert "The name and".

Amendment 271, in clause 101, page 78, line 40, leave out

"a description of as many of the locations as it is reasonably practicable to describe"

and insert "specification of each location".

Amendment 276, in clause 101, page 79, line 29, leave out

"or a description of the person or organisation"

and insert

"or another identifier of the person or organisation".

Amendment 278, in clause 101, page 79, line 40, leave out

"or a description of, as many of the persons or organisations as it is reasonably practicable to name or describe"

and insert

"or another identifier of, each person or organisation".

Keir Starmer: Ms Dorries, you have been indulgent in allowing me to trespass on the territory of some of these amendments in my general remarks on the clause. That probably applies to the Minister in reply as well. In those circumstances, it is not necessary for me to say any more about this group.

Mr Hayes: I have little to add, except to reassure the hon. and learned Lady and the hon. and learned Gentleman that the Investigatory Powers Tribunal has looked at this issue and supported the use of targeted thematic warrants. The Bill strengthens the safeguards.

Keir Starmer: I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Clause 90 ordered to stand part of the Bill.

Clause 91

POWER TO ISSUE WARRANTS TO INTELLIGENCE SERVICES: THE SECRETARY OF STATE

Keir Starmer: I rise to speak to amendment 395.

The Chair: With this it will be convenient to discuss amendments 396, 397, 398, 399, 400, 401, 402, 468, 469, 470, 403, 404, 407, 410, 411, 412, 413, 414, 283, 284, 285, 286, 287, 288, 289, 290, 291 and 292.

Keir Starmer: The clause deals with the power to issue warrants to the intelligence services. Subsections (1) and (2) deal with targeted equipment interference warrants, and subsections (3) and (4) deal with targeted examination warrants.

We have two concerns. First, although the test of necessity and proportionality is spelled out in the clause—in particular, in subsections (1)(a) and (b) and (3)(a) and (b)—the objective and aims to which the test of necessity and proportionality are attached, which are set out in subsection (5), are broad in the extreme. They are

"national security…preventing or detecting serious crime"

and our old friend,

"the economic well-being of the United Kingdom".

We have concerns about the breadth of those powers. Examination warrants obviously allow the examination of the material as well as its interception, and they go with the bulk power.

The first batch of amendments is intended to put some rigour and independence into the scheme by replacing the Secretary of State with the judicial commissioner. We have been over this territory in depth once and in summary form at least once again. I am not sure anybody is going to benefit, and they certainly will not welcome, my going over it at great length again—[HON. MEMBERS: "Hear, hear!"] The amendments would replace the Secretary of State with the judicial commissioner for the same reasons that I advanced a week ago today at a not dissimilar hour. I will not say more than that. In light of our discussion last week and the fact that I withdrew my amendments in relation to the scheme, I will not move these amendments; they are probing.

Ordered, That further consideration be now adjourned. *—(Simon Kirby.)*

6.33 pm

Adjourned till Thursday 21 April at half-past Eleven o'clock.

Written evidence reported to the House

IPB 66 Tom Hickman

IPB 67 The Internet Telephony Services Providers' Association

IPB 68 Letter from the Security Minister