PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

INVESTIGATORY POWERS BILL

Sixth Sitting

Thursday 14 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

Monday 18 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, *Committee Clerk*

† attended the Committee

Public Bill Committee

Thursday 14 April 2016

(Afternoon)

[Albert Owen *in the Chair*]

Investigatory Powers Bill

Clause 44

Interception in immigration detention facilities

2 pm

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

Joanna Cherry (Edinburgh South West) (SNP): The clause deals inter alia with interception in immigration detention facilities, and it is that which leads me to oppose its inclusion in the Bill. We can see that there is some replication of previous legislation in the provisions that deal with interception in prisons and psychiatric institutions, but the provision on immigration detention facilities is new and it is deficient in several respects. The theory underlying it is deficient, because immigration detention facilities are dealt with in a part of the Bill that includes psychiatric hospitals and the facilities are defined to include immigration removal centres, which are short-term holding facilities in which people, including families with children, are held in the so-called pre-departure accommodation.

Immigration detention has been the subject of much discussion on the Floors of both Houses because it is done by administrative fiat and without limit of time. The person detained will not have been brought before a court or tribunal to have the lawfulness of their detention or entitlement to bail considered, unless they instigate such a process; and the powers to detain are very broad and cover a large number of scenarios. The Bill states that conduct is to be authorised if it is done in the exercise of any power conferred by or under the detention centre rules or the rules for short-term holding facilities.

The Minister for Security (Mr John Hayes): It may help the hon. and learned Lady to abbreviate her remarks if I say that the provision is not intended and cannot be used to deal with someone's asylum or immigration status. That is not its purpose. With that assurance, perhaps the last point she made will not quite hold the water in her mind that it currently does.

Joanna Cherry: That does not really give me the assurance I seek. I was going to say that, under the clause, conduct is to be authorised if it is done in the exercise of any power conferred by or under the detention centre rules, or the rules for short-term holding facilities and pre-departure accommodation made under sections 157 and 157A of the Immigration and Asylum Act 1999 respectively. The latter sets of rules do not actually exist. Rules governing the regulation and management of short-term holding facilities were made in 2002, but it took until 2006 for draft rules to appear covering similar ground for short-term holding facilities as the detention centre rules do for immigration removal centres.

Back in 2006 the Home Office consulted on draft rules, to which various persons responded. In 2009 the Home Office consulted on another draft of the rules, to which there were further responses, many of them adverse; a number of freedom of information requests and parliamentary questions followed. In April 2012 the rules were described by the then Minister, the right hon. Member for Ashford (Damian Green), as being "still under development".

In March 2014, during the passage of the most recent immigration Bill, which became the Immigration Act 2014, Lord Taylor of Holbeach gave a commitment to Lord Avebury, who had been chasing the rules since 2006, that

"rules governing the management and operation of short-term holding facilities and the Cedars pre-departure accommodation will be introduced before the Summer Recess."—[*Official Report, House of Lords,* 3 March 2014; Vol. 752, c. 1140.]

Lord Avebury was informed before the recess that the commitment would not be met. He continued to pursue the matter, and draft rules were finally published on 18 February this year, almost a decade after the first draft was published and some 14 years after they were envisaged. That wait does not appear to have produced a version markedly different from earlier versions or particularly tailored to short-term facilities. In those circumstances, it is very far from clear what powers are being given by the current Bill. That shall be the gravamen of my exception to the clause.

In his review of immigration detention, Sir Stephen Shaw paid special attention to the problems of short-term holding facilities and the dreadful conditions in some of them. We have all heard about that on the Floor of the House. His concerns led him to recommend that a discussion draft of the short-term holding facility rules should be published as a matter of urgency. In the meantime, after he had said that, Her Majesty's chief inspector of prisons published a damning report on one particular facility, the Longport freight shed in Dover, describing the dire state of the facilities there. He said:

"on various occasions Home Office staff told us that they did not consider Longport to be a place of detention…despite detainees being in possession of legal authority to detain documentation and obviously being unable to leave. At this facility, the normal mechanisms of internal oversight and accountability that should apply to any form of detention were lacking."

Under such circumstances, the notion of any lawful exercise of the powers contained in clause 44 seems fanciful.

There are also problems with immigration removal centres. The latest version of the detention centre rules dates from 2001. They were last amended in 2005 to update the name of the tribunal hearing immigration cases and bail applications, but by the time that was done the name itself was out of date because it had already been replaced by the immigration and asylum chamber of the first-tier and upper tribunals. The rules contain a broad range of powers from powers to fingerprint individuals and powers of search, to powers to identify survivors of torture or persons with a mental or physical illness; powers on medical information and notification of illness and death; powers to segregate and use force, and powers to carry out compulsory tests for drugs. There are also rules regarding visitors to centres and contractors.

My point is that the rules cover the sorts of matters that would be covered by prison rules but they apply to

a different regime and to people who have not been detained by the courts or by due process of law. The overall effect is a lack of clarity. When one is working against the background of rules that do not exist or, if they do exist, lack clarity, a clause such as clause 44 potentially has a very far-reaching impact on people whose civil liberties are already severely undermined by the circumstances of their detention. The Government do not need to take just my word for that; it is a view widely held, including by a number of Government Back Benchers and peers.

Keir Starmer (Holborn and St Pancras) (Lab): We will not oppose the clause but I wish to put on record our concern about immigration detention and the intercept of communications in immigration detention facilities. There is growing concern, as has already been said, about the fact of that detention, the length of it and the conditions. There have been a number of reports, to which the Government have responded. In those circumstances, it is incumbent on the Government to justify the clause, although we will not seek to delete it.

Mr Hayes: I will be equally brief. There is a misconception about this matter. The Bill as drafted simply ensures that any interception carried out at a detention centre and under detention centre rules is lawful. No purpose is intended other than the maintenance of safety and security of the people in those centres. It is clearly right that officers should be able to intercept attempts to send contraband material, for example, such as drugs, in particularly sensitive environments. The power cannot be used to deal with the outcome of any immigration cases, asylum applications and so on.

The Immigration and Asylum Act 1999 contains the power to make rules for management of immigration detention centres. Clause 44 provides that interception, carried out in accordance with those rules will be within the law. In a sense, it is as simple as that. I can see why the hon. and learned Lady might have misunderstood this, but I can assure her that that is what is in the Bill and, I put on the record, is the Government's position. Rather than detain the Committee now, it might help if I send copies of the detention centre rules to Committee members, as they contain the essence of the argument that I have just made.

Joanna Cherry: My essential objection to the clause is that subsection (1) states:

> "Conduct taking place in immigration detention facilities is authorised by this section if it is conduct in exercise of any power conferred by or under relevant rules",

with the relevant rules described in subsection (2), and the underlying "relevant rules" are wholly inadequate. There has been a long history of problems with the rules, so the clause rests on a very shaky and unsafe foundation. I am concerned to protect the civil liberties of persons who are not criminals, who are not guilty of any violation of the law, but who are detained under immigration rules and whose civil liberties are already severely curtailed.

Mr Hayes: I have a great deal of regard for the hon. and learned Lady's diligence, but she is tilting at windmills. The clause is pretty straightforward. The points she makes about the management of detention centres may be perfectly reasonable debating points for a different Bill at a different time, but this Bill is not really about the management of detention centres and similar places. That matter is rightly dealt with in the relevant legislation. This Bill is merely about the application of certain powers to those centres to ensure that they are lawful. It is not much more complicated than that. On that basis, I commend the clause to the Committee.

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

The Committee divided: Ayes 10, Noes 2.

Division No. 3]

AYES

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

NOES

Cherry, Joanna	Newlands, Gavin

Question accordingly agreed to.

Clause 44 ordered to stand part of the Bill.

Clauses 45 and 46 ordered to stand part of the Bill.

Clause 47

SAFEGUARDS RELATING TO DISCLOSURE OF MATERIAL OVERSEAS

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

Keir Starmer: We do not oppose the clause, but I am duty bound to express the concern that the Joint Committee had—there were Opposition Members on the Joint Committee too—about safeguards in the Bill for the sharing of intelligence with overseas agencies. The Joint Committee was particularly concerned about clause 47 and suggested that safeguards should address concerns about potential human rights violations in other countries with which information might be shared. My question to the Solicitor General is: why did the Government not accept that sensible Joint Committee recommendation in the light of those human rights concerns?

2.15 pm

The Solicitor General (Robert Buckland): Regarding the Joint Committee's recommendation, all I can say at this stage is that my understanding of the clause is that the issuing authority must also ensure that restrictions are in place that would prevent to the extent considered appropriate the material being used in any legal proceedings outside the United Kingdom, which of course would be prohibited by clause 48. There will be other obligations that the agencies will have to follow—for example, consolidated guidance. If the hon. and learned Gentleman would like any further clarification, I would be happy to write to him.

Keir Starmer: I am grateful.

Question put and agreed to.

Clause 47 ordered to stand part of the Bill.

Clause 48

EXCLUSION OF MATTERS FROM LEGAL PROCEEDINGS

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

Joanna Cherry: I oppose the inclusion of the clause in the Bill. Clause 48, with schedule 3, broadly replicates the existing procedure in section 17(1) of the Regulation of Investigatory Powers Act 2000, whereby material obtained by way of an intercept warrant cannot be used as evidence in ordinary criminal proceedings.

Schedule 3 makes a number of exceptions to allow intercept evidence to be considered in civil proceedings where there is a closed material procedure in place—that is where a party and his or her legal team are excluded. Those proceedings would include, for example, proceedings under section 6 of the Justice and Security Act 2013, proceedings in the Special Immigration Appeals Commission or under the Terrorism Prevention and Investigation Measures Act 2011. Schedule 3 makes no exception for criminal proceedings, except in so far as material may be disclosed to the prosecution and to the judge so that the judge might determine whether admissions by the Crown are necessary for the trial to proceed in a manner that is fair. Deleting clause 48 would remove that exclusion, so that there would be an exception for criminal proceedings. It would also permit intercept material to be treated as admissible in both ordinary civil and ordinary criminal proceedings, subject to the ordinary exclusionary rules applicable to other proceedings, including public interest immunity and the provisions of the Justice and Security Act in civil proceedings.

I am indebted to Justice, the human rights group of lawyers that includes members of all parties and none, for its help in formulating my argument for deleting the clause. Justice has long recommended the lifting of the bar on the admission of intercept material as evidence in civil and criminal proceedings. In 2006, it published a document "Intercept Evidence: Lifting the ban", in which it argued that the statutory bar on the use of intercept as evidence was "archaic, unnecessary and counterproductive".

The United Kingdom's ban on intercept evidence in criminal proceedings reflects long-standing Government practice, but it is out of step with the position in many other Commonwealth and European countries, and it has proved increasingly controversial over time. Importantly, the European Court of Human Rights has recognised the value placed on admissible intercept material, in countries where it is available. It has said that admissible intercept material constitutes

"an important safeguard; against arbitrary and unlawful surveillance, as material obtained unlawfully will not be available to found the basis of any prosecution".

Victoria Atkins (Louth and Horncastle) (Con): Has the hon. and learned Lady taken into account the Criminal Procedure and Investigations Act 1996, which ensures fairness of disclosure in English and Welsh courts, as practised by many Members of the Committee, and is at the centre of the arguments against admission of this evidence?

Joanna Cherry: I have considered it, but we are not talking about disclosure, we are talking about the admissibility of evidence. As the hon. Lady will very well know, things may be disclosed to lawyers in the course of proceedings to try, as I said earlier, to make sure that there is a fair trial, but they are not necessarily admissible. I am talking about lifting the ban on the admissibility of intercept evidence.

Victoria Atkins: If there is something under the code that assists the defence or may undermine the prosecution, the prosecutor is obliged to make that known to the judge. A decision is then taken as to whether the disclosure of that material is so necessary that, in effect, the trial cannot continue.

Joanna Cherry: Of course the hon. Lady is absolutely right. I said that that was the case earlier, but that is not the end of the matter. As the European Court of Human Rights has recognised, where intercept material is admissible, its admissibility constitutes

"an important safeguard: against arbitrary and unlawful surveillance".

I know many Government Members are not too keen on the European Court of Human Rights; they might find the Privy Council report published December 2014, "Intercept as Evidence", more palatable. In paragraph 84, it confirmed that a fully funded model for the removal of the ban could result in a

"significant increase in the number of successful prosecutions."

That report also reflected concerns of agencies and law enforcement bodies that removing the ban without full funding could reduce its effectiveness. I acknowledge there is a funding issue and I am sure the Government will want to talk about that.

What I am really saying is that the Bill is a lost opportunity to remove the ban on admissibility of intercept material in criminal proceedings, which could benefit all. The Committee has heard what the Privy Council and the European Court of Human Rights have said on that. Many other countries manage to operate effective surveillance systems in which intercept material is admissible in criminal proceedings in certain circumstances. As I said, there will always be public interest immunity and the provisions of the 2013 Act in civil proceedings to allay some of the concerns Government Members might have.

The Joint Committee on the Draft Investigatory Powers Bill recommended that the matter should remain under review, and in paragraph 675 of its report invited the Government to take note of the "significant perceived benefits" of using intercept material in criminal proceedings. There are other arguments in favour of removing this ban. Members may want to think about how the current bar on the use of targeted intercept material relates to a new focus in the Bill on expanded and untargeted access to communications data.

Victoria Atkins: How would the hon. and learned Lady recommend that prosecuting counsel deal with an application from the defence to reveal the methodology used by the security services in obtaining intercept material? If the ban is removed, how is prosecuting counsel to answer that?

Joanna Cherry: It is not about the methodology; it is about the admissibility of the material itself. Far be it from me to lay down rules, at this stage of proceedings, for the Crown Prosecution Service or the Crown Office

and Procurator Fiscal Service in Scotland. That is something that will have to be worked out, but it will not be worked out in a vacuum, because the Privy Council has looked at this detail and many other countries have a system such as this that works.

It comes back to a continuing theme in my concerns about the Bill. Let us not be inward-looking. Members of my party are sometimes accused of being narrow nationalists, but I often think that is an allegation more accurately directed at the Conservatives. We should look the practice elsewhere in the world. Britain is not uniquely placed to decide how to have the best and fairest surveillance system. Our security services probably are world leading—I recognise that, and I mean no disrespect to them—but we are not here just to please them; we are here to protect our constituents' interests, as well as human rights in general, and to produce legislation that is balanced and fair.

I oppose the clause because I think there are good arguments in favour of making intercept material admissible in criminal proceedings. As the hon. Lady has indicated complex procedural rules would have to be built up—we have had a ban in our two legal systems in Scotland and England for so long that we would have to go back to the drawing board and think very carefully. She is right to say that this is not an easy matter, but we are not starting with a blank slate. If we do not want to look to Europe—I know that people are not too keen on Europe at the moment—we can look to the experience of other Commonwealth countries.

Victoria Atkins: The reason I keep rising when the hon. and learned Lady mentions other countries is that England and Wales have an extraordinarily thorough—I want to say "generous," but that is not the right word—disclosure regime, which is not mirrored elsewhere in the world. Look at the United States: the disclosure tests that occur in this country have very little relationship to what happens in America, so it is not right to compare the two.

Joanna Cherry: The hon. Lady makes a fair point that England and Wales have very clear disclosure procedures. Now, thank goodness, so does Scotland as a result of a number of Supreme Court decisions. We had a long way to go 10 years ago, but we have since come a long way. This is not about disclosure; it is about admissibility. Those are two very different things, as she well knows. Frequently things are disclosed that are not admissible.

Victoria Atkins: If evidence is admissible, the defence is quite within its rights to ask that question of prosecuting counsel. It is a question that is asked in a different form when a defendant suspects that there is an informant. How is prosecuting counsel to argue against that?

The Chair: Order. If the hon. Lady wishes to make interventions, they are to be short. She has an opportunity to make a contribution afterwards.

Joanna Cherry: At present, in the United Kingdom intercept evidence is not admissible in criminal trials. My purpose in opposing the clause is to make it admissible in criminal trials and proceedings, but there would have to be very careful rules and procedures, and the nature of our disclosure systems both north and south of the border will need to be taken into account.

I invite Members to consider, on the one hand, how the ban on the use of such material balances the new system that the Bill seeks to introduce of expanded and untargeted access to communications data and whether lifting the ban on the admissibility of intercept evidence in criminal trials would, as the Privy Council has said, increase the likelihood of successful prosecutions and, on the other hand, whether it might also reduce the reliance on administrative alternatives to prosecution, such as terrorism prevention and investigation measures, and on the use of untargeted forms of surveillance. Members will also have to consider whether the Government's cost base analysis is accurate and sustainable. We cannot say that the ceiling would fall down on the security surveillance system in this country if we removed the ban, because the system operates effectively in other countries.

Keir Starmer: It is of course the long-standing practice of all Governments to maintain this exclusion. The current form is effectively to continue the regime as it has operated until now. The regime has been reviewed a number of times, and the last review was probably in 2014. As has already been mentioned, the Privy Council said that the regime's removal could lead to an increase in the number of successful prosecutions. The exclusion is frustrating, and I was frustrated in a number of cases when I was Director of Public Prosecutions where, had it been possible to deploy such evidence, individuals who could not be convicted and locked up for serious offences might have been successfully charged and prosecuted. So the ban is a source of frustration because the net result is that, where someone cannot be charged because of this rule, there are only two possibilities in serious cases. One is that they continue to be subjected to surveillance, which can be extremely expensive and resource-intensive. The other is that they are put through some preventive measure, which has advantages and disadvantages but also a shelf life, which is normally shorter than the sort of sentence they might have received if the evidence had been admissible and a conviction had been obtained.

2.30 pm

Having said that, there are disclosure problems in two senses. The first is complying with the requirements of the CPIA. Now, I am not saying that it cannot be done but, although there have been reviews, it is time to look at it again. There are ways in which that could be accommodated. It would have to mean some adjustment of the existing rules because it is difficult to accommodate in the rules as they are. Historically, there has always been a secondary concern, which is disclosure of techniques. It would be difficult to have a regime that did not involve the risk of disclosing techniques. Those have been the most influential factors when this has been reviewed.

We have to accept that, in the past two or three years, something pretty extraordinary has happened in the field. The Bill is partly the result of that because powers and techniques that were not known are now avowed. Therefore, the risk that there once was that some of the techniques that we are now scrutinising—and which it

was thought, two or three years ago, would be extremely risky to disclose—are now out there. That is why I do not support deleting the provision, but I do want to put on the record that there is now room for a review, and it is not the same old review. It is a review on a very different set of circumstances, where at least some of the disclosure arguments as to technique are not as powerful as they once were. My position is to review first. Do not delete until the review has had the chance to consider all the possible options, including keeping the rule as it is.

The Solicitor General: The hon. and learned Gentleman is right about avowal but, of course, evidence pursuant to equipment interference has always been admissible. It is a bit of a mixed picture when you look at the detail of it.

Keir Starmer: I accept that there have been different avowals at different times in the past two years. I was speaking more generally. The argument about techniques is harder to sustain in the current set of circumstances. My view is that if there were a way to get around this exclusion, being able to use the evidence would bring very many benefits. When it comes to those involved in serious crimes, my strong preference is that they should be charged, put before a jury and, if convicted, serve the appropriate sentence, rather than be dealt with in some other way. For reasons that everybody understands, this provision frustrates that process. That is why I think it is time for a review against the current set of circumstances.

The Solicitor General: I am grateful to hon. Members for giving us the chance to have this brief but important debate. The hon. and learned Lady is right to characterise the existence of the prohibition, which has been in existence since the Interception of Communications Act 1985, with good reason.

I accept the points made by the hon. and learned Gentleman about evolution of powers and the avowal of particular techniques. Of course, very often we are talking about the protection of individual capabilities and that is a slightly more nuanced argument than the general points he makes. Therefore, ground No. 2 of the objection to the adduction into evidence of intercept material still remains a strong one, and ground No. 1 has to be acknowledged.

My hon. Friend the Member for Louth and Horncastle made the point well about the need to recast disclosure because it is material and relevant to the debate, and about ensuring that what is now intelligence but what would be evidence is in a form that can therefore be handled and admitted by a court. There is a cost to that, and the estimates given in the 2014 report vary between £4.25 billion and £9.25 billion. Those are not insignificant sums and they cannot be ignored or dismissed when balancing out the merits of taking this step.

The Government take the view—this is iterated in the 2014 report—that the problems outweigh, for the present at the very least, the potential benefit. The potential benefit is not clear, save for the points that the hon. and learned Gentleman makes. As a litigator and a prosecutor myself, I share his frustration and have been in those circumstances many times. I will not repeat the points he makes: I will adopt them.

The Government's position in that report was to say that they will keep under review any changes that might affect the conclusions of their latest review. That remains very much the position. I do not think it is appropriate in this legislation for us to depart, in the absence of any further evidence, from the position that has been iterated in no fewer than eight different reports over the past few years.

Many of us in the room are familiar with this issue. The debate is held regularly and will continue, but in the absence of compelling reasons to depart from the provisions of the 1985 Act I commend the clause to stand part of the Bill.

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

The Committee divided: Ayes 10, Noes 2.

Division No. 4]

AYES

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

NOES

Cherry, Joanna	Newlands, Gavin

Question accordingly agreed to.

Clause 48 ordered to stand part of the Bill.

Schedule 3 agreed to.

Clause 49

DUTY NOT TO MAKE UNAUTHORISED DISCLOSURES

Keir Starmer: I beg to move amendment 77, in clause 49, page 39, line 2, after "not", insert ", without reasonable excuse,"

The Chair: With this it will be convenient to discuss amendment 78, in clause 49, page 39, line 19, at end insert—

"(3A) For the purposes of subsection (1), it is, in particular, a reasonable excuse if the disclosure is made with the permission of the person issuing the warrant or the person to whom it is issued."

This provision adds a "reasonable excuse" defence to the "unauthorised disclosure" offence and expressly provides that the defence applies where the permission is given by the person issuing the warrant or the person to whom it is issued, the equivalent of a similar provision in clause 73(2) in relation to communications data authorisations.

Keir Starmer: I can be brief because the amendments speak for themselves. Amendment 77 is intended to insert a reasonable excuse exception to the duty not to make an unauthorised disclosure, and amendment 78 goes with it by spelling out that it is a reasonable excuse if the disclosure is made with the permission of the person issuing the warrant or the person to whom it is issued.

There are two principal arguments. One is that in this and the following two clauses flexibility is needed for disclosure made in certain circumstances. The second

point is one that some of the service providers are concerned about. They want to have discussions among themselves and with others about how to make the provisions in the Bill work.

At the moment, clause 49 would prohibit them from discussing either particular warrants or steps that they may be asked to take in order to solve some of those difficulties. It is the absolute nature of the prohibition that is the concern. Amendment 78, which allows disclosure if it is made with the permission of the person issuing it or to whom it is issued, seems to me to be a sensible way of getting around that particular problem.

Mr Hayes: As the hon. and learned Gentleman says, amendments 77 and 78 would amend the duty not to make an "unauthorised disclosure" to add the defence of "reasonable excuse". I accept that that would be on par with clause 73(2), which concerns the communications data provisions. I think that it is right that we retain the position that exists under RIPA, which itself reflects the sensitivity of the techniques of intercepting agencies, the fact that material obtained through intercept cannot be used in evidence—unlike communications data—and makes it an offence to disclose the existence of a warrant.

As clause 50 sets out, disclosure is already permitted if

"authorised by the person to whom the warrant is…addressed".

I would therefore argue that amendment 78 is not required.

It is worth adding that clause 50 sets out four categories in which disclosure can be authorised. I will not repeat them; they are pretty self-explanatory and, for the sake of brevity, we need to move on. Those exceptions provide adequate protection and, in my judgment, collectively render this amendment unnecessary, particularly clause 50(2)(b). I see why the amendment has been tabled and why the hon. and learned Gentleman wants to probe on it, but as he has acknowledged during our deliberations, the techniques and details of the capabilities of intercepting agencies must be protected for all kinds of reasons that we do not need to rehearse once again. Disclosure of such details would potentially cause some damage to the ability of those agencies to do their job.

Having said that, I completely accept that, if there is a case of wrongdoing or impropriety, and that case is made public, it is right that justice is done. There is no doubt about that, which is precisely why we have put into the Bill the establishment of a commissioner with the power to look at any aspect of those matters. In the end, it is better that a senior impartial and qualified person should take a view than, say, a junior official or employee of a telecommunications operator.

Nevertheless, I accept that it is important that people can raise concerns without fear of prosecution, which is why—I invite Committee members to look at it—we added clause 203 to the Bill, which we will get to when the Committee considers part 8. You will not let me go into too much detail about that now, Mr Owen, but people will understand that it provides protection for whistleblowers through an information gateway, so that the commissioner that I described will receive information of the kind that I described in a straightforward way.

These clauses combined maintain an important principle: techniques and details of capabilities of intercepting agencies must be protected. Of course, it is important that we caveat that with the checks and balances that I have set out. I am not sure that these amendments would add much—or anything; I was just being polite—and I therefore invite the hon. Gentleman to withdraw them.

Keir Starmer: I listened carefully to what the Minister said about clause 50(2)(b). It may be that that provides a different route but achieves the same objective, and in those circumstances I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Clause 49 ordered to stand part of the Bill.

Clause 50

Section 49: meaning of "excepted disclosure"

2.45 pm

Keir Starmer: I beg to move amendment 65, in clause 50, page 40, line 27, leave out paragraph (7)(a).

The Chair: With this it will be convenient to discuss amendment 66, in clause 50, page 40, line 35, leave out

"under Chapter 1 of this Part"

and insert

"described in sub-paragraphs (2)(a)(i) and (ii) of section 49."

Keir Starmer: There is a substantive point, but that comes under clause stand part, so I will deal with it when we get to that, if I may. Amendments 65 and 66 would bring into alignment—where are we? They are both focused on head 4. I think we have missed an Act out.

Mr Hayes: I think the hon. and learned Gentleman will find that amendment 65 would remove the exception from the duty not to make disclosures about a warrant where a postal operator or a telecommunications operator discloses statistical information about warrants in accordance with requirements set out in regulations made by the Secretary of State. Is that helpful?

Keir Starmer: That is helpful and I am grateful to the Minister. Amendment 66 is designed to align clause 50(7)(b) with clause 49(2)(a)(i) and (ii). The duty not to make unauthorised disclosures applies to both a warrant under chapter 1 of this part and a warrant under the relevant part of RIPA. The problem with head 4, unless I have misunderstood it, is that under clause 50(7)(b), it only relates to chapter 1 of this part and does not cross-relate to RIPA. I am happy to withdraw this amendment if it is catered for by other measures.

Mr Hayes: I will deal with this matter as briefly as I can. In the end, if we follow through the logic of the amendment, it would provide additional opacity rather than additional transparency. I think that if the hon. and learned Gentleman thinks through what he has just said and what I am about to say, he will realise that. In life, I am quite keen on opacity, but in legislation I am not keen on it at all.

Just to be absolutely clear, I point out that amendment 66, as the hon. and learned Gentleman said, relates to clause 50(7)(b)—disclosures of a general nature. At present, this subsection allows a disclosure of information that does not relate to any particular warrant under

[Mr John Hayes]

chapter 1 of part 2, but relates to warrants in general. As we understand the intention of the amendment, it would extend this provision to include a warrant under chapter 1 of part 1 of RIPA. Given that the disclosure simply permits disclosures of a general nature, this proposal is one that could be considered, and I think I would consider it. I am happy to take it away to ensure that there is the consistency that the hon. and learned Gentleman calls for, but I think that the amendment as drafted could be unhelpful to the cause that he has articulated. If he is happy for me to do this, I am happy to take it away, because I do take his point about ensuring that there is consistency. That seems to be the essence not quite of the amendment but of the argument that he made.

Keir Starmer: I will happily withdraw the amendment on that basis. It is intended to allow appropriate discussion of warranting in general so that all those with an interest can take part in the relevant discussions and debates. At the moment, head 4, subsection (7)(b) achieves that for warrants under chapter 1, but does not relate to other warrants. If there is a way of amending or otherwise achieving the desired objective, that would be acceptable. I will not press the amendment, but there is a need for a debate about warrants in general to make sure the systems and processes are articulated and dealt with. I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

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

Keir Starmer: I do not oppose clause 50 stand part, but I ask the Minister to clarify how it is anticipated the clause provides for disclosure of the details of a warrant to the Intelligence and Security Committee. On Tuesday, we had a lively debate about the extent to which Committees of this House can question and protest to the Secretary of State on warrants. My understanding is that if that process is to perform the function that was claimed on Tuesday, it must be done under this provision or not at all because there is an absolute prohibition on the disclosure and that covers the existence or content of a warrant, the details and so on. That stops the Secretary of State or anyone else disclosing to the House, a Committee or anyone else, and goes to the heart of the discussion about accountability.

It was argued that the ISC can hold the Secretary of State to account and it is important that, if this Bill passes into law, we understand how that is intended to take place. It would not come under head 1, head 3 does not apply, and head 4 is for a different purpose. Head 2 may be the answer, but to assist all of us in our further scrutiny of the provisions relating to the role of the Secretary of State and the judicial commissioners, it is important to identify the legal route by which the Secretary of State can be held to account and answer questions within the territory demarcated by clause 49(4). At the moment, it would be an offence for her to disclose any of those matters. Unless there is a route that allows her to do so, that seems to be an absolute bar.

The Solicitor General: I am grateful to the hon. and learned Gentleman for the question. Our answer is that, looking at clause 150(3), we say that it would come under head 2 and that the Secretary of State would have discretion to disclose—*[Interruption.]*

Keir Starmer: Sorry. Which clause was that?

The Solicitor General: Sorry. It is clause 50(3), where we have head 2 and:

"(a) in the case of a warrant under Chapter 1 of this Part, a disclosure made to, or authorised by, a judicial Commissioner;

(b) in the case of a warrant under Chapter 1 of Part 1…a disclosure made to, or authorised by, the Interception of Communications Commissioner or a Judicial Commissioner".

The disclosure is made by the Secretary of State. That might not be clear on the face of it, but that is the intention as I understand it of the clause.

Keir Starmer: I am just not sure. I think the Solicitor General has just quoted clause 152 to me.

The Chair: For clarification, will the Minister explain which clause he is referring to?

The Solicitor General: May I correct the record? It is my error. I omitted a number. I was talking about clause 150(3). Page 117 of the Bill states:

"For the purposes of subsection (2) something is necessary for the authorised purposes if, and only if",

and then we have paragraphs (a) to (f). That underpins the discretion of the Secretary of State to make that disclosure.

Keir Starmer: I am happy to pursue this matter outside the Committee if it is more convenient, but I think the provisions in clause 150 apply to bulk acquisition warrants rather than all warrants. Clause 150(1) sets out that it is expressly dealing with bulk acquisition warrants, and subsections 150(2) and 150(3) follow on from that. This is not intended as an exercise. Standing back from this, what I am concerned about is that it—

The Chair: Order. That was a lengthy intervention to help the Minister, who I now think wants to get back and explain the situation to the Committee.

The Solicitor General: What I will do is write to the hon. and learned Gentleman. My initial understanding was the right one, but I hope he will forgive me if I wandered off to the bulk powers provisions within the Bill. I will write to him to clarify the position. I think it is what I have said it is, but I will put it in writing.

The Chair: I will allow the hon. and learned Gentleman to ask further questions, and then the Minister may come back if he wishes.

Keir Starmer: Thank you for your indulgence, Mr Owen. I am grateful to the Solicitor General for indicating that he will write, and I am more than happy to have it in writing. That information is important because it is central to the debate about the roles of the Secretary of State and the judicial commissioner. It is not just me.

Other people need to be assured on the role and accountability of the Secretary of State. It is one thing to say, "She can be asked in a Committee about it", but it is another to point to the legal route by which that can happen in practice in a way that allows a degree of accountability. It is not intended as a trick question, and if it can be dealt with in a letter, I would be grateful.

Question put and agreed to.

Clause 50 accordingly ordered to stand part of the Bill.

Clause 51

Offence of making unauthorised disclosures

Joanna Cherry: I beg to move amendment 79, in clause 51, page 41, line 18, at end insert—

"(4) In proceedings against any person for an offence under this section in respect of any disclosure, it is a defence for the person to show that the disclosure was in the public interest."

This amendment seeks to provide a public interest defence to the offence of disclosure in relation to a warrant issued under this Part.

The amendment is about whistleblower protection and would provide a defence for the criminal offence of disclosure in relation to a warrant issued under this part of the Bill. The offence as framed in clause 51 includes disclosure of the existence and content of a warrant as well as disclosure of the steps taken to implement a warrant.

The offence is subject to a maximum penalty of five years' imprisonment. If committed, it is clearly a serious offence—the maximum penalty reflects that—but there are strong arguments that there should be a defence of disclosure in the public interest. By their very nature, surveillance powers are used in secret, with the vast majority of those subject to them never realising that surveillance has taken place. That means it is vital that sufficient checks, balances and safeguards are in place to ensure that the powers are used appropriately. I know that is why we are here, so apologies for stating the obvious. It is part of the checks, balances and safeguards to ensure that those who, in one way or another, witness or have knowledge of abuse or mistakes are able to bring that to the attention of individuals capable of addressing it, which may on occasion include bringing information to public attention. The provisions in clause 51 that criminalise the disclosure of information relating to the use of interception powers risk shutting down a vital route of ensuring accountability for the use of surveillance powers unless there is the defence of disclosure in the public interest.

3 pm

If the clause stands part of the Bill in its current form, it will help to enshrine an unnecessarily secretive culture that punishes those who seek to reveal wrongdoing, rather than encouraging a robustly honest working environment. Individuals who wish to make reports, even internally, of unlawful or otherwise inappropriate behaviour—we are talking about unlawful behaviour, not just inappropriate behaviour—will know that taking steps to do the right thing could expose them to a significant criminal sanction and a significant period of imprisonment. In a Bill that seeks to bring new levels of transparency to the UK's surveillance regime, introducing such an offence without a defence of disclosure in the public interest is undemocratic and unacceptable.

A number of bodies have expressed concern about the lack of such a defence in the Bill. Public Concern at Work has highlighted that the channels through which intelligence services personnel may report misconduct are uncertain in the Bill, and it suggests that clarity is particularly important in that area in light of the limitations of the protections afforded by the Public Interest Disclosure Act 1998, which protects internal disclosure, disclosure to prescribed bodies and wider disclosures to bodies and organisations not prescribed, applying different safeguards in connection with each type of disclosure. There are exceptions to that, and the relevance to the Bill is that members of the intelligence services are completely excluded from the Public Interest Disclosure Act's protection. The Act's protection also does not extend to workers in other sectors where their disclosure would breach the Official Secrets Act 1989.

The defence would not be a licence for clypes, as we call them in Scotland—people who tell tales. It is a strongly worded defence, and the disclosure would have to be in the public interest. The defence is not just for people—we have all come across them—who want to cause problems or to rattle their employer's cage; it would have to be disclosure in the public interest. The Joint Committee on the draft Bill recommended that it be amended to specify that any disclosure to the Investigatory Powers Commissioner for the purpose of soliciting advice on any matter, or for the purpose of supporting the duty to review, would be an authorised disclosure and not subject to any criminal penalty. The Joint Committee also recommended that a provision should be inserted in the Bill to allow for direct contact to be made between judicial commissioners and both communication service providers and the security and intelligence agencies.

Clauses 49 to 51 authorise the disclosure of information relating to certain matters, but it is unclear whether persons disclosing other information will be subject to the offence. It is far from clear where there are similar statements for whistleblowers. My purpose in moving the amendment is to create a safe route for whistleblowers where their disclosure is in the public interest.

Keir Starmer: The purpose of the amendment is to state clearly on the record what the safe route is for whistleblowers. There are similar versions in other legislation, including the Official Secrets Act, and the absolute prohibition causes great concern to those who want to expose iniquity. In certain cases and places, the safe route for a whistleblower has been explained. The challenge on the table for the Minister is recognising the concerns and anxieties of those who want to disclose wrongdoing where it is in the public interest for them to do so. There must be a safe route for them. If not this, what is the route? In support of that way of putting it, I pray in aid the Joint Committee recommendation that there ought to be amendment to make it clearer for those who need to know what the route is.

Mr Hayes: This is an interesting amendment. It deals with the tension, which I think all Committee members recognise, between allowing the proper opportunity for those who have legitimate concerns to bring them forward to be dealt with and encouraging feckless complaint. Much of what we do in this House in framing law means dealing with that dilemma, and this is a good example.

[Mr John Hayes]

The hon. and learned Gentleman—I think that the hon. and learned Lady said it first, actually—drew particular attention to the Joint Committee report. I refer to paragraph 629, which recommends that

"the Bill should contain an explicit provision for Communication Service Providers and staff in public authorities to refer directly to the Judicial Commissioners any complaint or concern they may have with the use of the powers under the Bill",

and goes on similarly.

That is precisely what we intend and what we have tried to set out. That said, the hon. and learned Lady will understand that it is important to create a duty, as clause 49 does, not to make unauthorised disclosures. Clause 50 sets out the exceptions to that duty, and clause 51 provides for the offence of making an unauthorised disclosure. Providing a public interest defence of the kind that she discussed is unnecessary in light of the exceptions already in the Bill. In my view, it might even encourage feckless or unlawful disclosures.

Joanna Cherry: The defence would not apply to a feckless or unlawful disclosure. If somebody sought to pray in aid that defence, the jury would have to decide, under legal direction from a judge, whether what had been done was in the public interest. Something feckless—which I gather means "without good reason"—would not be in the public interest.

Mr Hayes: There is a balance to be struck, of the kind that I described. The hon. and learned Lady is right that the route to the commissioner must be clear and straightforward, allowing people of the kind that the hon. and learned Gentleman described to know how they can bring their concerns to his attention. That is why clause 203 provides the information gateway that I spoke about earlier. That is the point made by the Joint Committee. What we have done in clause 203 is essentially give life to the Committee's recommendations about a direct route to the commissioner.

Joanna Cherry: Does the Minister accept that there might be situations in which an immediate disclosure is required to prevent conduct that is seriously unlawful? That is the situation where the defence is required. Somebody might find themselves in a position of having to make a public disclosure immediately to prevent unlawful conduct. Rather than going around the houses looking for advice or being assured after the fact that what they did was all right, they need to know that there is a defence of public interest to encourage them to make a disclosure immediately to prevent unlawful conduct.

Mr Hayes: Yes, but I am not so sure that, in the modern age, we do not live in precisely the opposite circumstance to the one the hon. and learned Lady sets out. All kinds of information are put into the public domain, whether for right or wrong and whether for good or bad reasons. That information cannot then be withdrawn and it is often taken to be fair and true, when it is anything but. I am not so sure that we do not need a process that is sufficiently rigorous that the commissioner is better placed to take a view on what is, or is not, in the public interest.

I will go further than that. It seems to me that, if we are going to have the commissioner, we have to vest power in his or her hands. If we then created all kinds of other means for dealing with these issues, I suspect that would undermine the commissioner's significance and discourage people from taking their concerns to the commissioner.

However, I think perhaps we can reach a synthesis around the way we make the route known. In clause 203, we have done what the Joint Committee asked us to do—I note that there are distinguished Members sitting behind me who were on that Committee. But I am not sure that we have thought enough about how to inform people about the route they can take under clause 203, so I will ask my officials to look at that again. There is an information challenge here, because it is all very well for the cognoscenti—there are many of them in this room—to know about such things, but I am not sure that that is good enough. So I will meet the hon. and learned Lady halfway—halfway in my judgment, at least, even if not in hers—by ensuring that we look closely at how well informed people are about their ability to go down the route I have set out. On that basis, I ask her to withdraw the amendment.

Joanna Cherry: I wish to insist on the amendment.

Question put, That the amendment be made.

The Committee divided: Ayes 2, Noes 10.

Division No. 5]

AYES

Cherry, Joanna	Newlands, Gavin

NOES

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

Question accordingly negatived.

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

The Committee divided: Ayes 10, Noes 2.

Division No. 6]

AYES

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

NOES

Cherry, Joanna	Newlands, Gavin

Question accordingly agreed to.

Clause 51 ordered to stand part of the Bill.

Clause 52 ordered to stand part of the Bill.

Clause 53

POWER TO GRANT AUTHORISATIONS

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

3.15 pm

Keir Starmer: I beg to move amendment 118, in clause 53, page 42, line 14, leave out subsection (1) and insert—

"(1) A Judicial Commissioner may grant a communications data access warrant where the judicial commissioner considers—

(a) that it is necessary to obtain the data for the purposes of a specific investigation or a specific operation, and

(b) that the conduct authorised by the warrant is proportionate to what is sought to be achieved.

(1A) The grant of a warrant is subject to restrictions set out in the rest of this Part."

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

Amendment 125, in clause 53, page 42, line 25, at end insert—

"(1A) The Judicial Commissioner may grant a warrant on application from—

(a) an officer from a relevant public authority involved in the relevant investigation; or,

(b) an individual designated by the relevant public authority to make applications for warrants to the Judicial Commissioner."

Amendment 126, in clause 53, page 42, line 25, at end insert—

"(1B) A warrant must—

(a) name or otherwise identify the person or persons, organisation, premises, or location to which the warrant relates; and

(b) describe the investigation or operation to which the warrant relates."

Amendment 229, in clause 53, page 42, line 26, leave out from beginning to end of line and insert—

"A warrant granted by a judicial commissioner may authorise the applicant or a telecommunications operator to".

Amendment 119, in clause 53, page 42, line 26, leave out "designated senior officer" and insert "warrant".

Amendment 120, in clause 53, page 42, line 32, leave out subsection (3).

Amendment 121, in clause 53, page 43, line 4, leave out "authorisation" and insert "warrant".

Amendment 122, in clause 53, page 43, line 14, leave out "authorisation" and insert "warrant".

Amendment 123, in clause 53, page 43, line 16, leave out "authorisation" and insert "warrant".

Amendment 124, in clause 53, page 43, line 25, leave out "authorisation" and insert "warrant".

Amendment 130, in clause 55, page 45, line 15, leave out "authorisation" and insert "warrant".

Amendment 128, in clause 55, page 45, line 16, leave out subsection (1)(a).

Amendment 132, in clause 55, page 45, leave out line 31.

Amendment 129, in clause 55, page 45, line 37, leave out subsection (4).

Amendment 133, in clause 57, page 46, line 20, leave out "authorisation" and insert "warrant".

Amendment 134, in clause 57, page 46, line 24, leave out "authorisation" and insert "warrant".

Amendment 146, in clause 72, page 57, line 27, leave out from "by" to "and" in line 29 and insert "a warrant".

Amendment 147, in clause 72, page 57, line 30, leave out "authorisation or notice" and insert "warrant".

Keir Starmer: We are now moving to a different part of the Bill and to a very important provision. I apologise if take some time, but we are moving to a significant set of matters that need to be considered together. The amendments to clause 53 have to be seen in context, and the context is the retention powers later in the Bill, which I will highlight in a moment.

I want to put the position of the Labour party on this and other provisions clearly on the record. It is accepted that there are circumstances in which it is necessary to retain or obtain the data of individuals who are not necessarily targets themselves, so that at a later stage that data can be accessed for a specific purpose or reason—so have a broad retention power and then a much more narrowly defined access provision. Clause 53 is the access provision. The retention provision is clause 78 and I direct the Committee's attention to that clause because that is where this all starts.

Under clause 78 the Secretary of State can require "relevant communications data" to be retained by "any description of operators", and she can require the retention of

"all data or any description of data"

so long as they come within

"one…of the purposes falling within paragraphs (a) to (j) of section 53(7)".

The Secretary of State's very wide retention power is exercised by issuing a notice, the effect of which is to require the retention of potentially wide-ranging and extensive data for 12 months. That is an extensive retention provision. There is some provision for filtering the data, but the power to access the data is in clause 53.

On the face of it, the retention powers are quite wide and will necessarily involve retaining data of individuals who are not targets or subjects, never will be and were never intended to be—in fact, all of our data, in many respects. Our long-standing position is that to justify that potentially very wide power, which is a serious cause for concern to many people, it is critical that at the point of access there is a clearly defined and high threshold and clear safeguards. In other words, if one collects a lot of data, at the point of accessing it one must go through a much more rigorous set of preconditions with effective safeguards. Clause 53 allows such access.

On clause 53(1), the first thing to be observed is the person who is to grant authorisation—the holder of the keys to the gateway—to allow any of the activities in subsection (2), engaging in conduct

"for the purpose of obtaining the data from any person",

and further action under subsection (4), is not the Secretary of State or a judicial commissioner, but a "designated senior officer" of a relevant public authority. That is an immediate cause for concern. There is a very wide power to retain, so it is necessary to have really strict preconditions before access, and the keys are held by a designated senior officer—nobody of higher rank than that.

To understand what that means, I direct Members' attention to schedule 4, although I should perhaps go via clauses 61 to 64, which make further provision in relation to relevant public authorities and designated

[Keir Starmer]

senior officers. The question is: who is a designated senior officer and what are the public authorities concerned? For that, we go to schedule 4 on page 204, where there is a long list of the public authorities and designated officers who can access the relevant data.

There we see some familiar bodies that one would expect to find in such a schedule, but running one's eye down the list brings one to the Royal Navy Police, the Royal Military Police, and, further down, the Department of Health. Across the page are the Ministry of Justice, the Department for Transport, the Competition and Markets Authority, and the Criminal Cases Review Commission. I will pause there. In the Criminal Cases Review Commission, the person who can authorise access to data is an investigations adviser. With all due respect to the investigations advisers in the CCRC, that is a very low level of authorisation to access or obtain data that has been retained.

There are other examples. In the Financial Conduct Authority, any head of department in the enforcement and market oversight division has authorisation. Over the page, in a fire and rescue authority the watch manager provides authorisation, and in the Food Standards Agency it is a grade 6 employee. The Gambling Commission can access data under this provision, as long as a senior manager says so. These are really worrying levels of authorisation in relation to personal data: a senior manager in the Gambling Commission has the role of deciding whether your data or mine can be accessed. Dropping down the page, in a national health service trust it is the director of operations, or a control and communications manager, or the duty manager in ambulance trust control rooms who can authorise access to the relevant data, and so on and so forth. In the Office of Communications, it is the senior associate.

The first thing that is striking about clause 53 is the insufficiently senior level at which authorisation may be granted. Access may be authorised if

"a designated senior officer of a relevant public authority"

thinks

"that it is necessary to obtain communications data for a purpose falling within subsection (7)"

and that it is relevant for

"a specific investigation or a specific operation or…testing…The designated senior officer may authorise any officer of the authority to engage in any conduct which…is for the purpose of obtaining the data from any person",

and so on. That is a real concern. Will the Solicitor General explain why it is thought appropriate to drop from what until now have been quite high levels of authorisation and scrutiny, with strict tests, right down to "a designated senior officer of a relevant public authority"?

I have dealt with who can authorise access; let me turn now to the purpose of gaining access. What is it that the designated senior officer has to be satisfied about? That takes us straight to clause 53(7), which states that

"It is necessary and proportionate to obtain communications data for a purpose falling within this subsection if it is necessary and proportionate to obtain the data—"

Before I go down the list that follows in clause 53(7), I remind the Committee that the case involving David Davis, Tom Watson and others is before the Court of Appeal. We do not know the outcome of that case. Of course, it does not relate to these provisions, because they are not in force, but it relates to provisions that are not dissimilar to these. The question that arises in that case is: what is the true interpretation and effect of the Digital Rights Ireland case, in which it was found that one of the EU directives was invalid? The question before the Court of Appeal, which was critical to the European Court's analysis in the Digital Rights Ireland case, is whether a regime for retention of data—a regime similar to the regime in the Bill—requires safeguards. The two safeguards in the Digital Rights Ireland case of most relevance to this clause are the safeguard that there must be a serious offence threshold for access and the requirement that there must be prior judicial oversight.

I am aware of the submissions and counter-submissions in that case on how those safeguards apply—whether they apply generally across the piece or whether they are case-specific. I am aware of what the divisional court said and what the Court of Appeal has said so far. In addition, I recognise that it would not be right for me to say that on the analysis of the Court of Appeal so far it is established that it is a precondition that the threshold must be a serious offence or that there must be prior judicial oversight. I do not advance an argument on that basis, because any fair reading of the Court of Appeal does not allow me to do so, and I do not do so. However, what it does is set up a challenge, which is what all of the courts have been concerned with in the Tom Watson and David Davis case, namely whether the safeguards are sufficiently rigorous and strict. The question is whether they have to be those particular safeguards or whether other safeguards could achieve the same balance.

3.30 pm

I say that because if we now look at subsection (7), it becomes clear that it is a very long way removed from anything that could be called a serious offence threshold for accessing communications data. Paragraph (a) states that the data can be obtained

"in the interests of national security".

That is familiar, and we have come across it already in our deliberations. Paragraph (b) states that the data can be obtained

"for the purpose of preventing or detecting crime or of preventing disorder".

There, for the first time in the Bill, the word "serious" is gone; there is no "serious" threshold. Access to communications data by the designated senior officer is permitted if it is necessary for preventing or detecting any crime, with no threshold, and for preventing disorder. The most petty crime therefore comes within paragraph (b); there is simply no threshold. I am not making the point that it is a requirement under the Court of Appeal ruling so far—it is not final—that the crime must be serious, but to have no threshold at all for the crime in subsection (7)(b) is surprising, to say the least. We then have our old friend in the next paragraph:

"the interests of …economic well-being".

Joanna Cherry: Where we have encountered the phrase "economic wellbeing of the UK" before, there has been another subsection to say that that only applies to persons outside the British islands, but there is no such corollary in clause 53. Does the hon. and learned Gentleman agree that that is worrying? If I am wrong, no doubt I will be corrected by the Government.

Keir Starmer: I am grateful for that intervention. If the Solicitor General can point to such a provision, I would be interested to see it. On the face of it, the clause allows designated senior officers within a public authority to obtain communications data in the interests of the economic wellbeing of the UK without that further qualification.

Subsection (7) then states that data can be obtained

"in the interests of public safety…for the purpose of protecting public health"

or,

"for the purpose of assessing or collecting any tax".

We then come to paragraph (g), on which I want to spend some time. It states that data can be obtained

"for the purpose of preventing death"—

that would obviously be a high threshold—

"or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health".

The threshold is way, way down. There are many ways in which a person's physical or mental health could be damaged. The Bill, if passed, will authorise access to communications data without any threshold as to the level of damage or injury.

Suella Fernandes (Fareham) (Con): I appreciate the hon. and learned Gentleman's analysis, but does he agree that obtaining communications data is one of the less intrusive powers contained in the legislation, but such data are very helpful for setting the scene and planting the seed for investigations? That has to be borne in mind when looking at the authorisation regime, because this is different from other powers.

Keir Starmer: Let me take that in stages. I accept that accessing communications data is in a different category and order from, say, the interception of the contents of communications. I also accept the proposition that communications data are used in many cases involving serious crime. I will go further than that: it is rarely possible to bring and to conclude cases of serious criminality without reliance on communications data. I have no in-principle objection to communications data being made available and being used. My concern is the very low level of sign-off required to access those data and the lack of any meaningful threshold in subsection (7); there simply is not one. Whether or not a meaningful threshold is achieved by the insertion of the word "serious", as I propose in my amendment, or some other word, if we simply say that it could be necessary and proportionate to access communications data to prevent any crime or damage, we are proceeding on a basis for which it is very hard to think of any circumstances in which it would be difficult or impossible to justify obtaining communications data. It just is not a set of thresholds.

Dealing with miscarriages of justice and situations in which a person has died and so on, and

"for the purpose of exercising functions"

are listed in the subsequent paragraphs. My central point is obvious but important. I realise how necessity and proportionality apply, but on any reading of subsection (7) there is no threshold. I think there is a risk for the Government here. I appreciate the direction of travel of the Court of Appeal, but does anybody seriously think that the jurisprudence is not going to develop to a point where there is a threshold that is thought to be appropriate? It is one thing to say that we do not necessarily have to have a threshold of serious crime, but to go from that to saying that we do not have to have any threshold at all is to invite problems, if these provisions are passed.

Suella Fernandes: It appears that the hon. and learned Gentleman is dismissing the necessary hurdles of necessity and proportionality in satisfying the tests. They are obviously going to relate to and be thresholds, so is it not wrong to say that there is no threshold in the clause?

Keir Starmer: I appreciate that the necessity and proportionality test has to be applied—in any given case there will always be an argument about whether it is necessary and proportionate—but as ever with necessity and proportionality the question is: what are we assessing necessity against and how are we arguing that it is proportionate? Is it necessary to do what? We get that only from the face of the statute. In other words, necessity does not give us anything unless we have some subject matter that it bites on, which is why the subject matter that it bites on is so important. Whether it is necessary for serious crime is one question; whether it is necessary for crime is another.

There are many, many things that one could say were necessary to prevent or detect crime. I absolutely accept that in practice those two tests are applied at all times, but the question is: what are they applied to? The question that the designated senior officer has to ask him or herself is: "Am I satisfied that it is necessary to prevent crime?" That would be good enough under the clause. It is, in principle, an inadequate threshold. I also think it will invite challenge in due course, because I do not think for one moment that, in the long run, the European Court and our courts are going to be satisfied with a scheme that does not have any threshold, even though there will be and are arguments about the precise threshold. We can see what the divisional court said in the Tom Watson case, so it is not just counsel's argument that was never accepted by anybody. In that case in the divisional court, counsel's argument that the serious crime threshold was an important safeguard was accepted. Thankfully, the writing is therefore on the wall if the clause is not taken back and reconsidered.

I shall move on to the second "who". The first "who" I focused on was who can issue the necessary authorisation, which is the designated senior officer. Under clause 53(2), that person can

"authorise any officer of the authority to engage in any conduct".

It goes from a relatively low-level authorisation to somebody even further down in the authority having to get on with the job of obtaining data.

The breadth of what can be done is outlined in clause 53(5), which states:

"An authorisation…may relate to data whether or not in existence at the time…may authorise the obtaining or disclosure of data by a person who is not an authorised officer, or any other conduct by such a person, which enables or facilitates the obtaining of the communications data"—

so it goes beyond the specific authorisation to the facilitation—

"and…may, in particular, require a telecommunications operator who controls or provides a telecommunication system to obtain or disclose data relating to the use of a telecommunications service provided by another telecommunications operator in relation to that system."

It is a very broad provision.

[Keir Starmer]

That enables us to see the amendments in their proper context. There are three categories of amendment. The first category is to be taken as a set and would insert some rigour and independence into the process by requiring judicial commissioners to sign off the necessary authorisations. The second set of amendments, which we will come to in due course, seeks to amend the threshold to provide a meaningful threshold for the judicial commissioner. To call clause 53 as drafted a set of safeguards is to mis-describe the words on the page.

The Solicitor General: It is with this amendment, I am afraid, that we have a strong disagreement. To say that there are no thresholds is a misrepresentation of the situation. Putting it bluntly, the Government's worry is that creating a serious crime threshold will miss a whole panoply of crimes that are extremely serious to victims. I am thinking in particular about crimes relating to harassment, stalking and other types of offences that would not fall within the threshold of serious criminality.

It is important that we couch our remarks carefully—the hon. and learned Gentleman has tried to do that, and I respect him for it. We are not talking about targeted interception here; we are talking about the retention of evidential leads—information that could, not of itself build a case, but which, in combination with other material, could allow investigators to build a case against a suspect. The analogy is with existing comms data, namely telephonic records and mobile phone records—the sort of material that he, I and others on the Committee have regular use and an understanding of, as prescribed by the RIPA regime. We are all familiar with it. The difficulty is that, as the days go by, the reliance by criminals on conventional methods of telecommunication changes.

The old system, where the SMS message would be the way things would be done, is increasingly falling into disuse. WhatsApp, internet chat forums and all sorts of encrypted means of communication are now being used. There is no doubt that the ability of the agencies—the security and intelligence agencies, the police and other agencies—to obtain even those evidential threads is therefore becoming more difficult. We are not talking about content, nor should we be. I draw an analogy with the sort of drugs observance case where the police officers can see people coming and going from a house that is of interest, but cannot see what is going on inside that house. That is what we are talking about here. Adopting these amendments would be entirely the wrong step to take.

Joanna Cherry: It is interesting that the Solicitor General chooses the example of surveillance in a drugs operation to tell us what we are talking about. That would be a serious crime, but as the shadow Minister has drawn attention to, clause 53(7) allows authorisations to obtain data not just for serious crimes, but for a whole plethora of things, including protecting public health, taxes, duties, levies and so on. Notwithstanding his opening comments, does he not accept that it is telling that the example he chooses is one of serious crime?

The Solicitor General: Not all drugs supply is necessarily serious. We might be talking about a particular class of drugs, which might not qualify within the criteria. Is the hon. and learned Lady seriously suggesting that we should not have the capability to draw evidential leads on cases of harassment, stalking or other offences that we all know are a particular problem when it comes to the abuse of victims?

Joanna Cherry: Stalking is, in my respectful submission, a serious crime. The thrust of these amendments is that the authorisation should be for serious crime, and by a judge.

The Solicitor General: The hon. and learned Lady wants to have her cake and eat it. The hon. and learned Member for Holborn and St Pancras said he wants a much higher threshold. I am sorry, but we cannot play around with this. The Committee is dancing dangerously on the edge if it seeks, in an ad hoc way, to try to subjectively define what serious crime is.

3.45 pm

Keir Starmer: I want to be clear with the Committee. In fairness to the Solicitor General, I can see the argument that, for harassment, there can be serious consequences for the individual. I had to deal with a number people in that situation and I do not underestimate for a moment the serious consequence that a series of minor actions can have. I do not think that necessarily means that we cannot have a serious crime threshold. I would be willing to work on what that threshold would look like, but I should not be taken as thinking that harassment, for example, cannot have serious consequences.

The Solicitor General: I am grateful to the hon. and learned Gentleman for that concession. It is important and it is not straightforward, and that is why I am afraid, as currently constructed, these amendments are deficient.

If I can develop my argument, I would like to give an example from Gwent police—a force that I know very well and have prosecuted on behalf of for the Gwent CPS on many occasions. Last November, a female victim returning home from a night out was approached by an unknown male who proceeded to sexually assault her. As a result of her cries, two witnesses approached and, thankfully, the male fled the scene before the offence was completed, serious though it was. An urgent press release was issued, along with CCTV footage of the offender. As a result, a member of the public called the police stating that she recognised the offender, who had given her his number. Investigators acquired subscriber data on that number and identified a suspect, who was subsequently arrested. In court, the offender pleaded guilty and received a 12-week prison sentence that was suspended for 12 months, and was placed on the sex offenders register for five years. I think we would all agree that that sounds very serious.

Keir Starmer: It is.

The Solicitor General: But is it? We have got to be absolutely clear. None of us would want that type of offence to fall outwith any of the criteria in these provisions—I am sure that would be the case.

Peter Kyle (Hove) (Lab): Proportionality was a central part of the discussion on Second Reading, and we received many reassurances from the Government.

My hon. and learned Friend the Member for Holborn and St Pancras has made a powerful point about the use of these powers in minor crimes. The Bill lowers the threshold to

"damage to a person's physical or mental health"

or the potential thereof. Will the Minister tell us what crime or potential crime does not pose damage to a person's physical or mental health, or have the potential thereof?

The Solicitor General: Of course, there are plenty of offences that do not involve violence or the threat of violence, such as fraud, although I understand that the potential consequences of some fraud can cause stress. May I reassure him that the test of necessity and proportionality in clause 53(7) remains very much at the centre of everything? I would not want him to be misled into thinking, as has perhaps been suggested by some of his Front Bench colleagues, that this is a free-for-all; far from it.

Keir Starmer: Will the Minister give way?

The Solicitor General: No, because I want to develop the argument. It is vital that we look at the underpinning of all this. None of the three reports that informed the drawing up of the Bill, nor the three reports arising from the pre-legislative scrutiny of the draft Bill, recommended any changes whatever to the authorisation regime for communications data. For example, David Anderson, QC, recommends authorisation of the acquisition of communications data by a designated person in a public authority. RUSI recommended:

"For the acquisition of communications data otherwise than in bulk, an authorisation by the relevant public authority. Communications data should only be acquired after the authorisation is granted by a designated person."

Prior to that, the report from the Joint Scrutiny Committee on the draft Communications Data Bill 2012 looked into the authorisation regime in depth and concluded that it was indeed the right model.

I entirely accept that anything that can sensibly be done to improve the already strongly regulated regime should be done. That is precisely why we have, for instance, provided for a new criminal offence that applies to persons in public authorities who knowingly or recklessly obtain communications data from a communications service provider without lawful authority. We have made the highly regarded SPOC—single point of contact—regime, which provides expert advice and guidance to authorising officers, a mandatory requirement in the Bill.

Lucy Frazer (South East Cambridgeshire) (Con): Does the Solicitor General think that one of the reasons that David Anderson supported these clauses is the benefit of communications data in Operation Magpie, to which he refers specifically in his report, when Cambridgeshire County Council protected more than 100 elderly and vulnerable persons from attempts to defraud them by using communications data powers?

The Solicitor General: I am grateful for that powerful example provided by my hon. and learned Friend.

It is important to note that in the report on the draft Bill—I am looking at paragraph 11 of the summary of conclusions and recommendations—the Joint Committee stated:

"We believe that law enforcement should be able to apply for all types of communications data for the purposes of 'saving life'. We recommend that the Home Office should undertake further consultation with law enforcement to determine"—

the report then makes references to various things in the draft Bill that would not necessarily not read over to the Bill that is before the Committee.

The point I am seeking to make, in the round, is that we have a tried and tested system, which is being replicated—indeed, enhanced—by the Bill, that deals with a very large number of applications. According to the latest annual report by the interception of communications commissioner, in 2013 there were 517,236 authorisations and notices for communications data in total. That contrasts that with warrantry and intrusive and limited interception of communications—in the same period, there were 2,795—so we are talking about a very different set of parameters, with a large volume of requests. My worry is that, however well-intentioned the amendment is, it is wholly unrealistic when it comes to fighting crime.

Keir Starmer: I rise only because this is an important point about how the powers will come to be exercised. It is of course possible to say that the precise wording of the amendment might not work in certain circumstances—all but sentences of 10 weeks or less are serious cases, and so on—but I do not want us to miss the point. The challenge to the Solicitor General is that there is no threshold. It is perfectly all right to say that the amendment does not necessarily achieve in precise terms the right level of seriousness, but it is not right simply to push back at the notion that there must be some threshold in the measure that is meaningful, which at the moment there is not.

The Solicitor General: I hear what the hon. and learned Gentleman says, but I do not agree with him about the threshold. It is set out in subsection (7). I can give another example: what about a missing person inquiry? We would not know whether it was a crime; it might well be a young person who has run away. We all have some direct or indirect experience of that.

I will address the point, but I have to be careful, because the case to which the hon. and learned Gentleman has referred is sub judice. I do not disagree with any of his characterisation, by the way, and of course I have read with care the Court of Appeal judgment of Lord Justice Lloyd Jones, but the hearing in the Court of Justice of the European Union is this week, I think. We will have to see how that develops.

I am very conscious of how case law develops in this area, and I am mindful of it, bearing in mind my duty as a Law Officer to uphold the rule of law. I am sure the hon. and learned Gentleman understands that, but where we are is in a sensible place. My worry is that if we start to get too restrictive, we will in effect end up in a position in which many serious matters—matters that are serious to the victim, but might not be serious according to other criteria—are lost or missed.

I have already mentioned necessity and proportionality. I should also pray in aid the fact that there will have to be compliance with a detailed code of practice and independent oversight and inspection of the regime by a senior judge, currently the Interception of Communications Commissioner. The current internal authorisation regime

[The Solicitor General]

is working well. No deliberate abuse of it has been identified in any ICC reports, which speaks volumes for the integrity of the current system.

Joanna Cherry: Will the Solicitor General accept that there have been severe concerns lately about what turned out to be rather destructive surveillance activities by the Metropolitan police in relation to covert human intelligence sources? Does he agree that it is highly unlikely that such practices would have occurred if there had been a system of prior judicial authorisation, rather than internal authorisations?

The Solicitor General: The hon. and learned Lady knows, of course, that that matter is now being investigated, in an inquiry led by Lord Justice Pitchford. I am not saying that she is not entitled to mention it, but it really is a different set of circumstances. That particular means—the covert use of human intelligence sources—is not what we are talking about, with the greatest respect. We are talking about ensuring that authorities prescribed by statute have the capability to continue finding the sorts of evidential lead that until now have been almost exclusively the province of conventional telecommunications.

Joanna Cherry: Perhaps I can put another example to the Solicitor General. Towards the end of last year, it was revealed that, due to what a judge labelled systemic internal failings in how the National Crime Agency applied for a warrant, a number of trials were at risk of collapse. Earlier in the year, Mr Justice Hickinbottom lamented what he called an

"egregious disregard for constitutional safeguards"

within the NCA, in the case of Chatwani and others *v.* the National Crime Agency and others. Those are examples of where the system is not working.

The Solicitor General: I am familiar with what the hon. and learned Lady is talking about, but again, that involves a particular failure by the NCA on warrantry. Here we are talking about various agencies' abilities. With respect to her, it is not the same. We are discussing a different regime. Tempting though it is to read over, that would be to frustrate the important work of many law, detection and investigative agencies in our country.

I do not see the purposes within the Bill as inconsistent in any way with the purposes set out in the exemptions from and limitations of the right to privacy in article 8.2 of the European convention on human rights. There has never been a serious crime threshold for the acquisition of communications data. No such limit is placed in article 8.2, which is why the Government's position on this issue—I will not mention the case—is legally respectable and sustainable. That is why the provisions in the clause meet the challenge that faces the agencies in a way that is proportionate and necessary, and that keeps pace with the breathtaking rate of change of technology being taken advantage of by many people of good will, but also by people of less than good will. For that reason, I ask that the amendment be withdrawn.

Keir Starmer: I will not repeat the concerns that we raised. Proceeding with a clause that has no seriousness threshold, however expressed, is fraught with difficulties, but the Minister has indicated that he will consider some of the issues and I want to reserve this issue for a later stage, so I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

4 pm

Joanna Cherry: I beg to move amendment 228, in clause 53, page 42, line 21, leave out subsection (1)(b)(ii).

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

Amendment 231, in clause 53, page 43, line 5, leave out subsection (4)(d).

These amendments to Clause 53 provide that in order to access communications data, a relevant public authority must seek a warrant from a Judicial Commissioner rather than undertake a system of internal authorisation. These amendments also provide for warrants to authorise conduct of a relevant public authority and require steps be taken by a telecommunications operator, removing the need for separate "authorisations" to public authorities and "authorisation notices" to telecommunications operators.

Amendment 131, in clause 55, page 45, line 24, leave out subsection (2).

Joanna Cherry: I am very much in agreement with everything that the hon. and learned Gentleman said on the last group. The Scottish National party's position is that access to communications data should be by means of a judicial warrant. We share the concerns that he articulated about the lack of a proper threshold in clause 53(7). I do not intend to press these amendments to a vote. I associate myself with the learned Gentleman's position, and I reserve my position on this matter for a later stage. This is an absolutely crucial clause, and it is extremely concerning, as he said, that there is no proper threshold in it.

The Solicitor General: I am grateful to the hon. and learned Lady for her succinct remarks. I will simply make the following observations about her amendment. It would remove the ability of the relevant public authorities to apply for communications data authorisation to test equipment or for technology development purposes. It is vital that those who are authorised to acquire communications data are able to test existing systems and to assist the development of new equipment or systems. Without that ability, we will not know whether the equipment will provide the required information in a real-life investigation, and nor will we be able to fix errors in systems where they are detected. We fear that that could have a seriously detrimental effect on our law enforcement agencies' ability to prevent and detect crime and may lead to mistakes, which are in nobody's interest—least of all that of the public, whom we serve. Therefore, this is a vital further safeguard. With respect, we are somewhat puzzled about why the amendment was tabled, but we heard the hon. and learned Lady and we respect her position. For those reasons, we oppose the amendment.

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

Amendment, by leave, withdrawn.

Keir Starmer: I beg to move amendment 110, in clause 53, page 43, line 39, after "detecting", insert "serious".

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

Amendment 109, in clause 53, page 43, line 39, leave out "or of preventing disorder".

Amendment 111, in clause 53, page 43, line 40, at end insert

"which includes to assist in investigations into alleged miscarriages of justice".

Amendment 112, in clause 53, page 43, line 41, leave out subsections (7)(c) to (f).

Amendment 114, in clause 53, page 44, line 1, after first "or", insert "serious".

Amendment 115, in clause 53, page 44, line 1, after "any", insert "serious".

Amendment 116, in clause 53, page 44, line 2, after "any", insert "serious".

Amendment 117, in clause 53, page 44, line 3, at beginning insert "serious".

Amendment 113, in clause 53, page 44, line 5, leave out subsections (7)(i) and (j).

Keir Starmer: I have covered my concerns that relate to these amendments, and the Solicitor General has dealt with them in his submissions. For the same reasons as on the first group of amendments, I want to take this matter away and I reserve my position. I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Clause 53 ordered to stand part of the Bill.

Clause 54

ADDITIONAL RESTRICTIONS ON GRANT OF AUTHORISATIONS

Keir Starmer: I beg to move amendment 127, in clause 54, page 44, line 20, leave out subsections (1), (2) and (3).

This is formally my amendment and therefore my embarrassment, because I do not think it achieves its intended purpose. I do not intend to press it to a vote. When I looked at it again in the early hours of this morning, I could see that it does not achieve whatever I hoped to achieve.

Mr Hayes: I wish to put on the record that I think the hon. and learned Gentleman deserves a big mark for honesty.

Keir Starmer: I will make such comments as I have during the clause stand part debate.

The Solicitor General: I am grateful to the hon. and learned Gentleman. It was puzzling me, and he has solved the mystery. The amendment seemed to remove the safeguard, which I am sure he does not want to do.

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

Amendment, by leave, withdrawn.

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

Joanna Cherry: I do not oppose the removal of safeguards from the Bill. However, this is the first time that internet connection records have raised their head in the Bill and I feel compelled to foreshadow the more detailed arguments that will be made when we reach clause 78.

The collection of internet connection records is one of the fundamental changes that the Bill seeks to introduce, and subsections (4), (5) and (6) of the clause contain the first mention in the Bill of such records. I think that I am correct in saying that they are in fact only mentioned in one further clause—clause 78.

Clause 54(6) sets out to define an internet connection record but fails spectacularly to do so because of its widely-drawn language, which clearly attempts to cover every imaginable base. The Scottish National party understands that the police and other authorities need powers befitting the digital age but, as legislators, we cannot pass a clause with such a significant impact on civil liberties—on personal privacy—without a clear definition in the Bill.

The industry has made it clear that it is willing to work with the Government to try to help implement ICRs. The trouble is that the industry does not know what ICRs are—and it looks like the Government do not know either. I addressed that point in quite a lot of detail on Second Reading. It is interesting that 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 very much associate myself with those comments.

We cannot legislate in a vacuum and if the Government cannot provide further detail and clarity so we all know what an internet connection record is and what we are legislating for, we will have no option but to try to remove the collection of such records from the Bill through our amendment to clause 78. But the Scottish National party objects to the inclusion of internet connection records not just because of the difficulty of defining them—in my speech on Second Reading, I suggested that they are not at all a sort of internet replication of a phone record, as the Home Secretary seemed to think they were—but because of their intrusiveness. They would provide a detailed record of every internet connection of every person in the UK over 12 months, with a log of websites visited, communications software used, systems updates downloaded, desktop widgets used and every mobile app used, and logs of any other device connected to the internet, such as games consoles or baby monitors. I said in that speech that that would be "fantastically intrusive" and I stand by that.

Law enforcement bodies can currently obtain similarly extensive internet connection data for specific surveillance targets in several ways. First, they can request that telecommunications operators in the future retain the data of specific targets. Secondly, they can request retrospective internet connection data on specific targets from operators who temporarily store such data for their own business purposes. Thirdly, if they are seeking to prevent or detect serious crime, they can request data or assistance from GCHQ, which has a remit to provide intelligence for those purposes. Intelligence sharing to tackle online child sexual exploitation will be fortified

[Joanna Cherry]

by the establishment in November last year of the National Crime Agency and GCHQ joint operations cell.

The Intelligence and Security Committee noted in recommendation I of its report on the draft Bill that the delivery of ICR proposals

"could be interpreted as being the only way in which Internet Connection Records may be obtained. However, this is misleading: the Agencies have told the Committee that they have a range of other capabilities which enable them to obtain equivalent data."

The ISC recommended that the Bill be amended in the interests of transparency, but no transparency has been provided.

The Scottish National party believes that the case supporting this huge expansion of data collection by internet service providers and its benefit to law enforcement is deeply flawed and contradicted by the available evidence, and that it has been accurately described as overstated and misunderstood.

I reiterate that there are no other "Five Eyes" countries in which operators are or have been forced to retain similar internet connection data. In Europe, as we heard the Danish tried it and decided that it was not of any utility. They thought about trying it again recently, but decided not to repeat the experiment. David Anderson noted in his report "A Question of Trust", on page 265, about the collection of that sort of internet connection data that

"Such obligations were not considered politically conceivable by my interlocutors in Germany, Canada or the US."

He therefore said that a "high degree of caution" should be in order.

There is also a legal issue with the mooted collection of internet connection records, because in 2014 the Court of Justice of the European Union ruled in the Digital Rights Ireland case that indiscriminate collection and storage of communications data is a disproportionate interference with a citizen's right to privacy. I therefore argue it is unacceptable that the Government are attempting to bypass that ruling to extend their policy of blanket data retention.

It will no doubt be argued that, provided there are sufficient safeguards, the Court's concerns from that case do not apply. However, as we just heard, there are not independent safeguards because we do not have judicial authorisation for access to internet connection records. We have instead a long list of public officials who have access to such records through internal procedures. I want to make it clear that I do not seek to impugn the integrity of public officials, but the reality is that their primary concern will relate to the operational capacity of their agency. That is a perfectly understandable matter of organisational culture, but that is also a reality that mitigates in favour of independent third-party authorisation.

If we collect internet connection records, we face falling foul of European Union law. We will also face falling foul of European Union law if we collect them without proper independent authorisation. I oppose clause 54 because it is the first point at which internet connection records rear their head in the Bill and the Scottish National party is not convinced that the Government have made a case for internet connection records. We are not convinced that there are not alternative routes to get at the necessary information and we are concerned that the collection of such records will be in violation of the law and of civil liberties.

Keir Starmer: We shall not seek to vote down the clause, but I want to raise some serious concerns about internet connection records because, as has been said, I think this the first time that they appear in the Bill. Subsection (6) is important because that provides the definition that

"'internet connection record' means communications data which…may be used to identify, or assist in identifying, a telecommunications service to which a communication is transmitted by means of a telecommunication system for the purpose of obtaining access to, or running, a computer file or computer program, and…comprises data generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication".

That is a wide definition. I listened carefully to the evidence of senior law enforcement officials about their ask on internet connection records, and they made it clear that they were concerned to have the who, the how, the when and the location.

I appreciate that there are other provisions—in fairness, I will come to those—but my concern is that that definition is much wider than their ask. That is important because subsection (4) deals with the point of access to internet connection records and what the designated senior officer can authorise. I accept that that subsection contains the restriction that internet connection records cannot be obtained or accessed unless one of the purposes identified is complied with—

"which person…which internet communications service…where or when".

That has a resemblance to what senior law enforcement told us was their ask, but the problem is that the definition in subsection (4) is much wider. It might be asked whether that matters. Well, it does matter because clause 78—the retention clause—as we have observed, provides that the Secretary of State may issue a retention notice in relation to relevant communications data. Clause 78(9) makes it clear that relevant communications data may be used to do a list of things—I will return to the list—and that internet connection records are included. That definition of internet connection records crops up again in clause 78(9). Therefore, anything within that description, so long as it also complies with the other bits of the subsection, may be retained.

4.15 pm

The important point I am trying to make is that it is one thing to say that designated senior officers can only access internet connection records if the preconditions in clause 54(4) are complied with, but it is another, more difficult argument to sustain that only internet connection records that go to the issues of which, why, when, who and location, and so on, are caught within the retention, because the retention is for any internet connection record that comes within the wider definition. It is true to say that clause 78(9) states:

"'communications data' means…data which may be used to identify, or assist in identifying, any of the following—the sender or recipient…the time or duration of a communication; the type, method or pattern, or fact, of communication; the telecommunication system…from, to or through which…a communication is…transmitted; or the location".

But that definition is, by no means, as tight as the definition in clause 54(4), so we are back to the situation of, "Let's assess what is caught, or retained, and what is later accessed." The suggestion that what is caught or retained is as tightly constrained as the description that law enforcement favours is wrong: it is a much wider definition of internet connection records.

On web browsing, as members of the Committee will know, the issue of internet connection records is a real concern among the public. When I talk to people about the Bill and the discussion gets to internet connection records, they have a keen interest in just what the Bill can do, because there is real concern about anything that retains the web browsing history of ordinary members of the public. The comms data code of practice has a heading dealing with web browsing and communications data, and it describes uniform resource locators. Paragraph 2.53 sets out the standardised structure of a URL, which is usually what comes up in the bar when one is searching on the internet—that is in the code of practice for a reason, because it potentially comes within the scope of the Bill. Paragraph 2.54 states:

"These elements of a URL are necessary to route a communication to the intended recipient and are therefore communications data."

To be clear, that means that uniform resource locators come within the definition of communications data. Paragraph 2.54 also states that

"fully qualified domain names provide an indication of the type of content that the server being accessed contains".

Paragraph 2.55 sets out further information about what

"URLs may, but do not always, contain".

Paragraph 2.57 states:

"An authorisation under Part 3 of the Act"—

which is what we are concerned with—

"or retention notice under Part 4"—

which I have mentioned—

"may only authorise the acquisition or retention of those elements of a URL which constitute communications data."

URLs are not excluded: they can come within a retention notice, so long as they constitute communications data. We are in the territory of web browsing history, and we have to tread carefully to ensure that the system is as tight as it is claimed to be.

To get to what constitutes communications data, we have to go to the definitions in the Bill. Clause 225(1) helpfully points out that

"'systems data' has the meaning given by subsection (4)".

Clause 223(5) states:

"'Communications data', in relation to a telecommunications operator, telecommunications service or telecommunication system, means entity data or events data which is (or…is capable of being) held or obtained by, or on behalf of, a telecommunications operator".

The definition goes on to refer to data

"which is available directly from a telecommunication system".

It is true that the end of clause 223(5) makes clear that it is not about content in its own right, but members of the public, the Labour party and other Opposition parties are concerned that simply excluding content is not a sufficient safeguard. In other words, it may well be that the content and the sub-content of one's web browsing history are not caught by the provisions, but there may be a route map. This is not a direct analogy, but it is almost a reading list of what people have been looking at. Although it may only give the title of the book, that reading list reveals a great deal about the private lives of individuals, in a way that goes beyond other forms of communications data.

The Solicitor General: It is important that we go through this carefully. The shadow Minister talked about browsing history. The full history does not constitute comms data; it is not an ICR for the purposes of this legislation. It is like looking at everything after the forward slash. Let us take the example of a website such as telegraph.co.uk: the fact that a person visited the website may be one thing, but everything after the forward slash—the detail of what the person is doing—is not an internet connection record for the purposes of the Bill.

Keir Starmer: I am grateful to the Solicitor General for that reply. The same point was made on Second Reading by the Home Secretary and was also made in Committee, but I have a difficulty with it that is important to put on the record. Where are the words in the Bill that result in what the Solicitor General said? I am concerned, because I cannot see them.

I accept that, when it comes to accessing internet connection records, there is the further test in clause 54(4). At the moment, a constituent might say, "Will my internet connection records and browsing history be kept?" People are concerned about whether there is a record of what they have looked at on the internet. They feel very chilled by that. The Solicitor General says that it goes so far but no further. That is to give people comfort and I understand why it is said. The difficulty I have is finding the precise words in the Bill that give effect to that proposition.

The Solicitor General: Is not the real question whether the authorities will have access to that history without due process? Therein lies the rub. As I have said to the hon. and learned Gentleman, the full browsing history will not be capable of being accessed without further warrantry.

Keir Starmer: I understand the Solicitor General's point, which is that when it comes to access, there is a further, stricter test. I absolutely understand that and I accept that clause 54(4) is there for a purpose. The question that my constituents and I, and others, want answered is, "What about what is being retained?" There is a chilling feeling if it is being retained. The comfort of the Government saying, "Well, we are keeping everything but we will not look without a stricter test", is, of course, a comfort, but it is not that much comfort to many concerned individuals.

Mr Hayes: I support the Solicitor General's view—I do not want the hon. and learned Gentleman to be caught in a pincer movement by the way. None the less, clause 223(6) is pretty clear, is it not? It mentions anything that

"might reasonably be considered to be the meaning (if any) of the communication".

That seems very helpful. I know that that clause is in the other part of the Bill but, of course, it relates to the content in exactly the way he describes.

Keir Starmer: I am grateful to the Minister for pointing that out but that was the route that I trod a few days ago

[Keir Starmer]

when I was preparing my submissions. The problem is that content is given the description that he just set out, but it also says,

"any meaning arising from the fact of the communication or from any data relating to the transmission of the communication is to be disregarded, and (b) anything which is systems data is not content."

That obviously led me to have a look at what systems data are, for which we have to go to clause 225(4), which states that systems data

"means any data that enables or facilitates, or identifies or describes anything connected with enabling or facilitating, the functioning of…a telecommunication system".

It is true, and I accept, that an internet connection record does not include content in the form set out in 223(6), but then one gets to systems data, and part of it comes back out again. It would be very helpful if someone were to attempt to describe, by reference to the Bill's provisions, why it is said that, at the point of retention, the provision does not include web browsing history. That is a question that many people would like answered. I leave that challenge on the table for the Government.

I rose to say that at this late hour and it is a complicated point, but it goes to the heart of the question about ICRs. At the moment, it is being framed in the sense of, "Well, they won't look at it unless", but people are genuinely concerned about the retention of their browser history.

The Solicitor General: As a preface to my remarks, which will have to be succinct, I do not want to stray into the debate on clause 78. I do not want to criticise the hon. and learned Member for Edinburgh South West, but she has made points that will properly be answered when we come to that debate. She is right to raise the point about the Danish experience and, like me, she has read the evidence in the Committees, but there are significant differences between what we are trying to do in the UK and what happened in Denmark. The Danish experience was not a great one. There are significant operational, financial and other differences that mean that the Danish Government are looking carefully and with a great interest at what we are attempting to do in the UK. This is not straightforward and it is not easy, but it is our duty as legislators to get ahead of the curve when it comes to the development of technology and to make sure we are not playing catch-up when it comes to criminals' increasingly sophisticated use of the digital sphere.

Joanna Cherry: Setting the Danish experiment to one side, can the Solicitor General tell us why the other "Five Eyes" countries are not requiring operators to retain similar internet connection data? Why are no other western democracies doing that?

4.30 pm

The Solicitor General: The simple answer is that they know there are technological challenges and that someone must start somewhere. I am proud that the United Kingdom is trying to set the correct example. It may be that the detail is more than we can do and this is why we are having scrutiny and debate—I warmly welcome that—but to suggest that because it is difficult we should not take a lead is a counsel of despair. That is not good enough when it comes to the challenges facing us with the development of technology.

The hon. and learned Member for Holborn and St Pancras asked some proper and detailed questions, and rightly contrasted and compared various parts of the Bill. As lawyers and legislators, we must be careful not to become too prescriptive when defining the technology, which is why the combination of the framework in the Bill and the code of practice to which the hon. and learned Member for Edinburgh South West referred—paragraph 2.63 helpfully sets out what an ICR might consist of—gives sufficient clarity and flexibility operationally to keep pace with developments in technology. We must necessarily be technology neutral and careful when making definitions.

We worked extremely closely with law enforcement agencies about their needs, including the Joint Committee's work, and they have been clear that the Bill now reflects those needs. Communication service providers have also developed their views in recent months. They confirmed in evidence to the Committee that they understand exactly what they are being asked for. My strong contention is that what we have now is a clear definition of internet connection records and helpful support from the codes of practice.

Let me deal with clause 54 directly. It sets out clearly the four operational purposes for which a designated senior officer may grant an authorisation for a relevant public authority to obtain an internet connection record. All those purposes have been endorsed by the Joint Committee. Importantly, it specifically advanced the fourth purpose in its conclusions. That fourth purpose covers connections that do not disclose a crime or nefarious purpose, but with other material can help to build up a series of evidential leads to the effective detection of crime.

I am grateful for the examples that the Digital-Trust gave to all members of the Committee. Many of us are familiar with the organisation and it is supported by, among others, Harry Fletcher, who was deputy general secretary of the National Association of Probation Officers. His work, with that of others, to combat stalking and harassment is well known to me. I worked closely with him on the draft Bill that became law as the Protection of Freedoms Act 2012, and now on the work that addresses stalking. The trust's example is powerful. Many stalkers sadly indulge in sending unwanted gifts to their victims. For example, they may habitually order flowers to make the point that they are still there. The victim may not want such gifts, but they are part of the stalking behaviour.

The internet connection record that discloses that someone had gone to a florist is innocuous, but it could be vital lead evidence in building a picture of someone's stalking and harassing behaviour. That is why the Digital-Trust strongly supports clause 54(4). It can see the operational merit in ensuring that such purposes are included. It is a stark and clear example of the dangers of over-limiting the criteria within which the investigating authorities can act.

The hon. and learned Gentleman is quite right to talk about the concerns we all share about the unwarranted retention of masses of information that would constitute an intrusion into the lives of millions of people. Let us not forget that the Government will not be retaining the

information. The information will be at arm's length from Government. There is a filter system designed not only to screen out but to destroy data that is extraneous to the investigation. Crucially, the full web browsing history does not constitute an internet connection record. It is therefore not covered by the provisions and would have to be subject to the sort of warrantry that Members of this House understand to be necessary to protect the privacy of the people we serve. For those reasons, I strongly commend clause 54 to the Committee.

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

The Committee divided: Ayes 10, Noes 2.

Division No. 7]

AYES

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

NOES

Cherry, Joanna	Newlands, Gavin

Question accordingly agreed to.

Clause 54 ordered to stand part of the Bill.

Clauses 55 to 57 ordered to stand part of the Bill.

Clause 58

Filtering arrangements for obtaining data

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

Joanna Cherry: I wish to speak briefly on clause 58. I indicate that I will also cover clauses 59 and 60, which I also oppose. The clauses provide for the establishment and use of a filter to gather and analyse communications data. They provide for a communications data request filter, which was a feature previously proposed in almost identical terms in the rather unpopular draft Communications Data Bill. The only change made is that under clause 58(5), which states that the Secretary of State

"must consult the Investigatory Powers Commissioner about the principles on the basis of which the Secretary of State intends to establish"

the filter.

The request filter essentially is a search mechanism that allows public authorities to conduct simple searches and complex queries of the databases that telecommunications operators will be required to build and hold. The Joint Committee on the Draft Communications Data Bill described the request filter in that Bill as

"a Government owned and operated data mining device",

which, significantly, positions the Government at the centre of the data retention and disclosure regime. Access to the filter and the data it produces would be subject to the same self-authorisation processes as all communications data. In practice, the request filter would be a search engine over an enormous federated database of each and every citizen's calls, text records, email records, location data and internet connection records. Those would be made available to hundreds of public authorities.

I am sure the Government will, as they have in the past, be keen to portray the request filter as a safeguard for privacy. However, the processing of such a huge amount of personal data, as permitted by the request filter, is a significant privacy intrusion. It is not only me who thinks that; the Joint Committee on this Bill noted that there were

"privacy risks inherent in any system which facilitates access to large amounts of data in this manner."

When I asked the Solicitor General why other countries do not do that, he said that the lead must start somewhere, but I do not want my constituents to be guinea pigs for such a system. I can tell from my mailbox that many of my constituents are very concerned about such huge amounts of personal, private data being held and analysed in that way. They want to see serious crime tackled, but not at the expense of their privacy.

A balance has to be struck, and I fear that the request filter is more of an intrusion into privacy than a safeguard for it. It is a portal with the power to put together a comprehensive picture of each of our lives. We should not misunderstand that that is what the filter can do. It raises many of the same concerns as a large and centralised store, with the added security concerns of protecting multiple distributed databases.

Public authorities will have a permanent ability to access the request filter, which will make it an enticing and powerful tool that could be used for a broad range of statutory purposes. The ability to conduct the complex queries that the request filter will allow for could increase the temptation to go on fishing expeditions—that is, to sift data in search of relationships and infer that concurrences are meaningful. That was one of the many concerns expressed by the Joint Committee on the Draft Communications Data Bill about the request filter proposal.

With the request filter power, authorities could use communications data to identify attendees at a demonstration and correlate that with attendance at other public or private locations in a 12-month period, or identify those regularly attending a place of worship and correlate that with access to online radio websites, inferring risk. Those examples show that the new ability risks casting undue suspicion on thousands of innocent citizens and mining their personal contacts for patterns, which is an unacceptable intrusion into the privacy and civil liberties of our constituents and British citizens generally.

Keir Starmer: I will not be long, but I want to raise some concerns about the provisions. It is clear—the Minister will correct me if I am wrong—that the arrangements are to assist a designated senior officer who is considering whether to grant an authorisation, and therefore has got to that stage of the exercise, and more broadly to provide for effective ways of obtaining communications long before there is serious consideration of a particular authorisation. Subsection (1)(a) applies in relation to the contemplation of a possible authorisation, whereas subsection (1)(b) is a much wider way of organising the data so that someone can later find what they want more easily.

[Keir Starmer]

The arrangements are made by the Secretary of State but then exercised by the designated senior officer, and we have discussed who will be doing that. It is so concerning because the provision allows for the designated senior officer, who in many cases will be not a high-ranking individual in a public authority, to start to organise the data that have been obtained under a retention power. It is therefore a very wide ranging power indeed.

4.45 pm

I accept the argument that anything that allows the authorities to get to the data they need and moves out of the way data that are irrelevant to any possible exercise has real use. We will not oppose the clause because if the idea is effectively to deselect data on individuals who are not of interest, the sooner that is done the better. Nevertheless, I echo the concerns that have already been expressed that it is a very wide power that will in the end be exercised by relatively low-ranking individuals in an authority to look at and organise a huge amount of data. I have real concerns about the clause, but, for the reasons I have identified, we will not be voting against it.

Mr Hayes: We can probably satisfy the need to address the concerns that have been raised. First, let us be clear about privacy. To restate what I said when we began our consideration of the Bill, because there is no one's canon that I like to draw on more than my own,

"privacy…is at the heart"—[*Official Report, Investigatory Powers Public Bill Committee,* 12 April 2016; c. 90.]

of all we do. The defence of private interests and the protection of the public are the essence of the Bill. This filter is, of course, an additional safeguard. It will allow public authorities, when they are dealing with such a request, to consider on a case-by-case basis what needs to be released and, by implication, what does not.

The Joint Committee on the Bill considered this matter in some detail and concluded at paragraph 38:

"We welcome the amendments that have been made to the Request Filter proposal. They constitute an improvement on that which was included in the Draft Communications Data Bill."

There is, however, an argument about the process once a request has been made, and that is the argument made by the hon. and learned Member for Holborn and St Pancras.

The code of practice goes a long way towards making things clearer in chapter 9, paragraphs 9.1 to 9.4. Indeed, that chapter describes the request filter as

"an additional safeguard on the acquisition of communications data"

that will work in tandem with other safeguards to

"limit the volume of communications data being provided to a public authority."

Therefore, the filter is a way of eliminating unnecessary data from release.

Nevertheless, I hear what the hon. and learned Gentleman says about ensuring that the permission to do that is in the hands of the right people and dealt with in the right way. It might be that we can say a little more about that in the code of practice. I will take a look at that, because there is an argument for refining that part of the code.

In response to the hon. and learned Member for Edinburgh South West, it is clear that public authorities will sometimes need to make complex inquiries. For example, they may ask multiple questions of multiple communications service providers for data to identify an unknown person who is suspected of having committed a crime at different places and at different times. The complexity of the requests is the context in which the application of the filter will be applied.

Currently, public authorities might approach communications service providers for location data to identify the mobile phones in specific locations at the relevant times to determine whether a particular phone and a particular individual is linked to three offences. To get to the end that I have described, very large amounts of data would be required, so the filter process is both a safeguard—a protection—and a way of making the system more practicable. For all of those reasons, it is an important part of the Bill. Having said that, I hear what is being said about the process rather than the principle of it. Maybe we could look at the process, but I am absolutely committed to the principle and on that basis I commend the clause to the Committee.

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

The Committee divided: Ayes 10, Noes 2.

Division No. 8]

AYES

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

NOES

Cherry, Joanna	Newlands, Gavin

Question accordingly agreed to.

Clause 58 ordered to stand part of the Bill.

Clause 59

USE OF FILTERING ARRANGEMENTS IN PURSUANCE OF AN AUTHORISATION

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

Joanna Cherry: I oppose the clause for the same reasons and I do not think I need to elaborate further.

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

The Committee divided: Ayes 10, Noes 2.

Division No. 9]

AYES

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

NOES

Cherry, Joanna	Newlands, Gavin

Question accordingly agreed to.

Clause 59 ordered to stand part of the Bill.

Clause 60

DUTIES IN CONNECTION WITH OPERATION OF FILTERING ARRANGEMENTS

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

Joanna Cherry: I oppose the clause for the same reasons.

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

The Committee divided: Ayes 10, Noes 2.

Division No. 10]

AYES

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

NOES

Cherry, Joanna	Newlands, Gavin

Question accordingly agreed to.

Clause 60 ordered to stand part of the Bill.

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

4.54 pm

Adjourned till Tuesday 19 April at twenty-five minutes past Nine o'clock.

Written evidence to be reported to the House

IPB 40 Interception of Communications Commissioner's Office

IPB 41 Local Government Association

IPB 42 Med Confidential

IPB 43 Dr Lindsey Bell

IPB 44 Public Concern at work

IPB 45 Ted Marynicz

IPB 46 David Anderson QC

IPB 47 Christopher Pidgeon

IPB 48 Ray McClure

IPB 49 Graham Seaman

IPB 50 Alison Saunders, Director of Public Prosecution

IPB 51 Dr C. N. M. Pounder, Amberhawk Training Limited

IPB 52 Labour campaign for Human Rights

IPB 53 HUBS CIC

IPB 54 Jisc Technologies

IPB 55 Remote Control Project

IPB 56 Immigration Law Practitioners' Association

IPB 57 techUK further submission

IPB 58 The Law Society

IPB 59 Open Rights Group

IPB 60 National Union of Journalists

IPB 61 The Law Society of Scotland

IPB 62 Media Lawyers Association

IPB 63 Chris Farrimond, National Crime Agency, Simon Grunwell, HM Revenue & Customs and Richard Berry, National Police Chiefs Council

IPB 64 Dr Nora Ni Loideain, Research Associate, Technology and Democracy Project, CRASSH University of Cambridge

IPB 65 Letter from the Home Office regarding Government amendments