PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

INVESTIGATORY POWERS BILL

Third Sitting

Tuesday 12 April 2016

(Morning)

CONTENTS

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

not later than

Saturday 16 April 2016

The Committee consisted of the following Members:

Chairs: Albert Owen, †Nadine Dorries

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

Glenn McKee, Fergus Reid, *Committee Clerks*

† attended the Committee

Public Bill Committee

Tuesday 12 April 2016

(Morning)

[Nadine Dorries *in the Chair*]

Investigatory Powers Bill

9.25 am

The Chair: We now begin line-by-line consideration of the Bill. Would everyone please ensure that all mobile phones and other electronic devices are switched into silent mode?

We first consider a motion to amend the programme motion agreed by the Committee on 24 March. The motion is on the amendment paper in the Minister's name. I remind Members that the Standing Orders provide that a Minister must make such a motion and that if any member of the Committee signifies an objection, the proceedings on the motion will lapse. I call the Whip to move the motion.

Ordered,

That the Order of the Committee of 24 March 2016 be varied so that the Committee shall meet at 4.30 pm and 7.00 pm on Tuesday 3 May instead of at 9.25 am and 2.00 pm on that day.—*(Simon Kirby.)*

The Chair: I should like to tell Members that, as a general rule, I and my fellow Chair do not intend to call starred amendments. The required notice period in Public Bill Committees is three working days, therefore amendments should be tabled by the rise of the House on Monday for consideration on Thursday and by the rise of the House on Thursday for consideration on the following Tuesday.

The selection list for today's sittings is available in the room and on the website. It shows how the selected amendments have been grouped for the debate. Amendments grouped together are generally on the same, or a similar, issue. A Member who has put their name to the leading amendment is called first. Other Members are then free to catch my eye to speak on all or any of the amendments in the group. A Member may speak more than once in a single debate. At the end of the debate I shall call again the Member who moved the leading amendment and, before they sit down, they will need to indicate whether they wish to withdraw the amendment or seek a decision. If any Member wishes to press any other amendments or new clauses in a group to a vote, they need to let me know. I shall work on the assumption that the Minister wishes the Committee to reach a decision on all Government amendments.

Please note that decisions on amendments do not take place in the order in which they are debated but in the order in which they appear on the amendment paper. In other words, the debate occurs according to the selection and grouping list. Decisions are taken when we come to the clause that the amendment affects. New clauses are decided after we have finished with the existing text, so after consideration of clause 232. I shall use my discretion to decide whether to allow a separate stand part debate on individual clauses and schedules, following the debate on the relevant amendments. I hope that that is helpful.

Clause 1

Overview of Act

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

The Minister for Security (Mr John Hayes): I welcome you to the Chair, Ms Dorries. It is a delight to serve under your stewardship. I also welcome all members of the Committee.

Clause 1 provides an overview of the Bill and, for that reason—and with your indulgence, Ms Dorries—it is perhaps worth my setting our consideration in context. The Bill is significant, bringing together as it does for the first time a set of powers currently used by the intelligence agencies and law enforcement. It adds checks and balances regarding authorisation and oversight, and provides a degree of certainty regarding those powers and those checks and balances, which up until now has not been there in that form. It certainly provides greater navigability. Many of the powers are contained in a variety of legislation passed over time, so the point made by the Chairman of the Intelligence and Security Committee on Second Reading of the draft Bill—that it is hard to navigate the legislation that supports the powers—was well made. The Bill provides greater transparency and, I hope, greater clarity.

It is important to understand that privacy is at the very core of the Bill. Clause 1 deals with that core. There have been calls, and we may hear them again during our consideration, for privacy to be defined more explicitly, but my counter view, without wishing to be unnecessarily contentious at this early stage, is that privacy runs through the very fabric of the Bill and that to separate it out—to desiccate it in that way—would weaken the commitment to privacy that is at the heart of the legislation. The protection of private interests and the protection of the public are at the heart of all we seek to do in the Bill. In my view, it is therefore unacceptable to limit the privacy provisions to a single clause.

Perhaps it would be advisable for me to give a little more detail about what the Bill does in respect of privacy. By underpinning the powers and sensitive capabilities available to law enforcement and security services, the Bill provides—as successive Governments have, by the way—an appropriate degree of oversight of those powers. Furthermore, through the change to authorisation—for the first time and in groundbreaking terms—they answer the call of those who have argued that both the political masters who drive these things and the judiciary should play a part in reinforcing those safeguards, based very much on the core principle of necessity and proportionality which applies to all such powers.

It is fair to say that in sweeping away some of the cobwebs that surrounded the powers I have described—certainly in the view of some of their critics—the provisions here shed a light on some of the most sensitive powers available to our intelligence and security agencies. It follows absolutely the direction provided by the independent

reviewer of terrorism legislation, David Anderson QC, that the capability examined in the Corston review of investigatory powers should be avowed and put on a statutory footing.

It is important that the public and Parliament understand that the powers I describe are there to keep us safe. It is also important that those powers are constrained in the way I have briefly described. The Bill places very strict controls on the use of those powers. They reflect the proposals of the 2015 report by Parliament's Intelligence and Security Committee on privacy and security. They include limitations around who can use each of the powers; for what purposes and in what circumstances; how information can be obtained under the powers must be protected; when it can be shared and in what circumstances it must be destroyed; and, perhaps most importantly, the penalties—including criminal sanctions—for improper use of the powers.

In addition, the Bill delivers the strongest possible safeguards for the way the powers are authorised. I have spoken about the groundbreaking introduction of the double lock which means that politicians and the judiciary are involved in authorising powers. This maintains democratic accountability and adds a new element of judicial independence. No doubt we will discuss this in subsequent consideration of the Bill. Indeed, I note that amendments have been tabled that will allow us to do just that. However, I remain of the view that it is very important that this House and Ministers play a key part in the business of authorising these powers. The introduction of judges into the process of issuing warrants represents a highly significant change to the way the security and intelligence agencies operate—perhaps one of the most significant changes since they began in the last century. These things are not done lightly and should not be taken for granted. It is a very important change.

I spoke earlier about oversight and the Bill also introduces world-leading new oversight provisions, drawing together some of what is done already but adding visibility and transparency in the way that I mentioned. This is an opportunity for the new Investigatory Powers Commissioner to be an effective advocate for the public. The commissioner will have unfettered access to the work of the security and intelligence agencies and new powers to inform people who have suffered as a result of serious errors. He or she will leave no question in the minds of the public or that of Parliament that these powers are used within both the letter and the spirit of the law.

Returning to my initial point about the clause, let us reflect on what the privacy safeguards amount to. In essence, they reflect the collective consideration of the three independent reviews and three Parliamentary Committees that preceded the Committee's consideration of the Bill. There have been those who have surprisingly—some might say remarkably or incredibly—argued that the Bill has been rushed in some way. My goodness, I cannot remember a single other piece of legislation in my time in Parliament that has been published in draft preceded by three independent reports; has then been considered by three separate Committees of the House; and published in its full form and debated on Second Reading. The Bill is about to have consideration of the most serious kind—I say that, looking around at the cerebral members of the Committee—and will then, of course, proceed to the other place for similar scrutiny. I hesitate to say that it is unprecedented, but it is quite unusual and reflects the Government's absolute determination to get this right. I hope that the Committee will move ahead as one in our determination to put both these powers and the safeguards—the checks and balances—in place.

The consideration of the Bill that has already taken place covers the vast proportion of the clauses. No doubt we will refer to some of those reports during the next few days and weeks. I am absolutely sure that all members of the Committee want what I want—for this legislation to be in a form that engenders complete confidence that those whose mission is to keep us safe have what they need to do so, but that the checks on the exercise of their powers are rigorous, robust and transparent. In that spirit, and with that hope about the further consideration, I commend clause 1 to the Committee.

Keir Starmer (Holborn and St Pancras) (Lab): I, too, welcome you to the Chair, Ms Dorries. It is a pleasure to serve under your chairmanship.

Our starting position is that in the aftermath of attacks such as those we have recently seen in Brussels, which are only the latest in a series of similar attacks, there can be no doubt that the security and intelligence services and law enforcement agencies need all the powers that are necessary and proportionate to deal with serious threats. That is the starting position on the Bill, so far as the Labour party is concerned.

As the Minister has said, it is a good thing that the powers that had previously been exercised by the security and intelligence services are now avowed on the face of the Bill. That is welcome, but those powers also need to be justified, clearly defined and limited, and there must be proper safeguards. The Opposition's proper role in the process we are about to undertake is to robustly challenge the Bill's provisions where they do not meet those criteria and to push back and probe. Through that process, we hopefully will improve the final product so that the Bill achieves what it needs to achieve, but goes no further than what is necessary and proportionate.

On justification, as the Minister no doubt knows, the shadow Home Secretary wrote to the Home Secretary on 4 April making a number of points, one of which was the need for a better assessment of the operational case and, in particular, an independent assessment of bulk powers. He said:

> "Whilst I accept the broad argument advanced by the authorities that powers to extract information in bulk form may provide the only way of identifying those who pose a risk to the public, the operational case for bulk powers which accompanied the Bill's publication has significant gaps. This was clear from contributions made at Second Reading from both sides of the House."

Anyone who reads the operational cases will see that they are slim indeed, and more than half the printed case is introductory matter.

The shadow Home Secretary suggests in the letter that

> "the simplest way to proceed would be, firstly, to produce a more detailed operational case and, secondly, to accept the recommendation of the Joint Committee and commission an independent review of all the bulk powers."

The Labour party suggests that that review should conclude in time to inform Report and Third Reading. Obviously the Minister will probably not want to deal

[Keir Starmer]

with the matter here and now, but I ask that a reply to the letter be prepared as soon as possible so that we can move forward on that issue.

The letter also deals with concerns about internet connection records, which we will deal with when we come to the appropriate clauses, but it particularly highlights the problems of definition in clause 54 and the question of the threshold for accessing internet connection records along with other comms data.

The letter also talks about the

"definitions of 'national security' and 'economic well-being'",

which we will probably start to debate today. The letter also raises meaningful judicial authorisation and oversight and the need for an overarching criminal offence of deliberate misuse and for effective protections for sensitive professions. Can a reply to the letter be prepared as soon as possible so that we can move forward, particularly on the operational case? If there is more work to be done, the sooner it starts the better. With luck it can then be finished in time for the next stage, which is Third Reading. Will the Minister ensure that there is a speedy response to that letter?

On the question of privacy provision, I listened carefully to what the Minister said. The recommendation of the Intelligence and Security Committee was that there should be general safeguards on privacy. Clause 1 does not provide that. The Minister says that the safeguards run through the Bill. I will make the cheap point, but I will make it quickly. The only amendment to part 1 in response to the Intelligence and Security Committee was the insertion of the word "privacy" in the title. It used to say "General protections", and it now says "General privacy protections". However, clause 1 in itself is clearly not enough. It is true that there are safeguards in the Bill, but there is also considerable inconsistency, and that is where overarching principles would play their part.

I will flag up for the Committee three examples of that inconsistency. It is the sort of inconsistency that an overarching provision would deal with. The first is in the draft code of practice on the interception of communications that is before the Committee, which we will consider further this morning. There is a strong proposition in paragraph 4.7 of the draft code, under the heading:

"Is the investigatory power under consideration appropriate in the specific circumstances?"

It states:

"No interference with privacy should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means."

So there is a clear proposition on necessity; it is not necessary if information can be obtained by other less intrusive means.

9.45 am

It is welcome in the code of practice. It should be in the statute, but there is an inconsistency. For example, clause 17(4), which we will get to later, sets out the power of the Secretary of State to issue warrants and sets out what the Secretary of State must take into account. Clause 17(1) sets out in clear terms the necessity test and the proportionality test, but subsection 17(4) in this critical clause states:

"The matters to be taken into account in considering whether the conditions in paragraphs (a) and (b) of subsection (1) are met"—

the necessity of proportionality—

"include whether the information which it is considered necessary to obtain under the warrant could reasonably be obtained by other means."

We have an inconsistency that should not be there. The code is clear: a measure cannot be necessary if information could reasonably be obtained by other less intrusive means. On the face of the statute, that is an inconsistency because the Secretary of State is told that it is a matter to take into account, but not an overarching rule. We will obviously debate that, but that is precisely why an overarching provision is needed.

I will give two other examples. The filtering clauses—clause 58 and following—set out how filtering arrangements are intended to work, but there is no reference to privacy or the weight to be given to privacy. It is similar, by way of example, in clause 67, which deals with single points of contact. I use those as examples, but the point is that it is easy to say that privacy runs through the Bill. The question is whether, in its practical application to each section, it is adequately dealt with. In our view, an overarching provision would help in each case where there is either an absence of a specific reference to privacy or in some cases inconsistency. We will table a new clause towards the end of the process, but it may be that in discussions with the Minister and others we can seek to advance this in a way that is acceptable to the whole Committee. However, the inconsistencies are there.

I would like some indication from the Minister as to how the Committee is to approach the code of practice. I say up front that we welcome the fact that the code is available. We asked for it to be available for the Committee—I do not think the Committee could do its work without the code of practice, and I appreciate that a huge amount of effort will have gone in behind the scenes to ensure that the material was available to the Committee on time.

A lot of detail is in the code of practice and the Committee does not have the ability to amend it. It will not be consulted upon until the Bill becomes law, so there is a practical problem. Where we identify a deficiency in the code of practice or suggest an amendment—it is not a formal amendment, of course—how does the Minister propose that we deal with that? To some extent, I suspect that some of my points about definition and clarity and the setting out of powers will be met by the argument that such points are in the code of practice. The problem is that we cannot amend the code of practice in Committee. When it comes to be considered after consultation, the whole of the code will be up for the vote and not the individual provisions, so there is a gap that we need to find a practical way through.

You will have noted, Ms Dorries, that many of the amendments tabled by the Scottish National party and the Labour party are identical. The hon. and learned Member for Edinburgh South West and I have divided up the work on those amendments. I hope that is not objectionable in any way—it at least puts the whole of the amendments before the Committee. One of us will lead on the amendments and the other, with your

permission, will follow immediately on so that we cover the whole of the amendments. Everybody will therefore know the points we are making before we proceed to the open debate. It is intended to assist the Committee and to save time, but I ask your indulgence.

Joanna Cherry (Edinburgh South West) (SNP): I welcome you to the Chair, Ms Dorries and it is a pleasure to serve under your chairwomanship. I would like to make some brief opening remarks on behalf of the Scottish National party in response to the Minister. We acknowledge the attempt to codify and modernise the law, and we think that the attempt is laudable. However, we think that the execution of this attempt is not laudable. We believe that there has been a rush to legislate, and it is not only we who say that. Members will remember that, when evidence was given to the Committee by Jo Cavan, the head of the Interception Commissioner's Office, she spoke of an aggressive timeline for the Bill. When I asked her to elaborate on that, she said:

"It is a really complicated and significant piece of legislation. Although I broadly support the Bill, because it is a good thing to put a number of the powers used by the intelligence agencies on a clearer statutory footing and to try to improve transparency, I do think that the scrutiny process has been very hurried. That is of concern because there are some significant privacy implications to the clauses in the Bill. There is still a long way to go towards strengthening some of the safeguards. Also, a lot of the operational detail is in the codes of practice. It is really important that those are scrutinised properly, line by line."—[Official Report, Investigatory Powers Public Bill Committee, 24 March 2016; c. 70.]

She agreed with me that the time afforded for scrutiny of the Bill is inadequate, particularly with regards to the international legal implications of aspects of the Bill.

Mr Hayes: I have no wish to delay us unduly or indeed to embarrass the hon. and learned Lady, but I remember the evidence that was given. As she will remember, I challenged the witness on it because, as I said earlier, I cannot recall another piece of legislation that has enjoyed such close scrutiny over such a period of time. Can the hon. and learned Lady think of another such piece of legislation?

Joanna Cherry: I do not recall legislation of such detail and such constitutional significance. I have only been in this House for nine months, but I have followed the operation of this House closely since I was a teenager. This is a massive Bill, and it is its constitutional significance that matters. I chaired an event last night at which the chair of the Bar Council of England and Wales spoke. She raised her concerns about the rush to legislate because of the constitutional significance of the legislation and its implications for the rule of law. The Minister does not embarrass me at all. I wholeheartedly stand by what I say. It is a widely held view, across parties and across society, that there is not sufficient time for the scrutiny of this legislation.

Simon Hoare (North Dorset) (Con): Will the hon. and learned Lady give way?

Joanna Cherry: I will make some progress, if I may. I would like to echo the comments of the hon. and learned Member for Holborn and St Pancras about the proper role of the Opposition, which I spoke about on Second Reading. As he said, it is the proper role of the Opposition to robustly challenge the legislation, to push back on it and to probe, hopefully with a view to improving it. That is why my party did not vote the legislation down on Second Reading. We are honestly engaged here in a process of improvement, but if the Government are not prepared to listen to us then we may well vote against the legislation at a later stage.

I echo what the hon. and learned Gentleman said about the failure to amend the draft Bill to deal with the ISC concerns regarding the lack of overarching principles on privacy. I also strongly echo what he said about a request for the Minister to clarify how the Committee is to approach the codes of practice which, as the hon. and learned Gentleman said, this Committee does not have the power to amend, and which contain some enormously important detail. Jo Cavan, the head of the Interception Commissioner's Office, also drew attention to that in her evidence.

On Second Reading on the Floor of the House, I promised to table radical amendments. The SNP has tabled radical amendments to the part of the Bill we will look at today. We want to ensure that surveillance is targeted, that it is based on reasonable suspicion, and that it is permitted only after a warrant has been issued by a judge rather than by a politician. We want to expand the category of information which will be accessible only by warrant, and to ensure that warrants may not be provided without proper justification. We also want to remove the widely drafted provisions of the Bill that would allow modification of warrants and urgent warrants without any judicial oversight. Those provisions, if they remain in the Bill, will drive a coach and horses through the so-called double-lock protection in the legislation.

We have also laid amendments to ensure a proper and consistent approach to the safeguards afforded to members of the public who correspond with lawyers, parliamentarians and journalists. We want to put a public interest defence into the offence of disclosure of the existence of a warrant. Those are the sort of radical, principled amendments that we believe are required to render parts 1 and 2 of the Bill compliant with international human rights law, bring the Bill into line with practice in other western democracies and meet the concerns of the UN special rapporteur on the right to privacy. We recognise that the security services and the police require adequate powers to fight terrorism and serious crime, but the powers must be shown to be necessary, proportionate and in accordance with law. If the House is not about the rule of law, it is about nothing.

Simon Hoare: I am very grateful to the hon. Lady for giving way. I do not agree with her and her party that the Bill is the constitutional earthquake they represent it to be. However, she has just referenced a point that would mean constitutional upheaval, if I heard her correctly—namely, to remove any political input, and therefore democratic accountability, to this House and to elected Members, and to bypass it all to unelected, unaccountable judges, though I mean that in no pejorative sense. To effectively create massive cleavage between democratic accountability and the day-to-day action allowing those things to go ahead would be a constitutional upheaval. Have the hon. and learned Lady and her party colleagues considered that viewpoint in that context?

Joanna Cherry: We have considered it in detail and I will be addressing it later in my submissions to the Committee. The hon. Gentleman and I will have to differ in our view on this. I do not consider that there is anything constitutionally unusual in judges being solely responsible for the issue of warrants. That happens in a lot of other western democracies—it is called the separation of powers. The idea that Ministers are democratically accountable to this House for the issuance of warrants on the grounds of national security is nonsense. I will explain later why I consider that to be so.

I was trying to stress that the SNP position is that we recognise the necessity of having adequate powers. I hope to be writing the security policy for an independent Scotland before I am an old lady and I would want to have a responsible, modern security policy that dovetails with that of England and other countries in these islands, but I want to model it on what other western democracies are doing, rather than going as far as this Bill, which, without proper justification, goes beyond what other western democracies do. The SNP intends to table amendments to deal with what I called on Second Reading the fantastically intrusive provisions of this Bill regarding internet connection records and bulk powers. We also want to look at ensuring a proper oversight commission, but that is for a later date. I look forward to addressing amendments on parts 1 and 2 of the Bill.

Mr Hayes: The shadow Minister raised a number of issues, some of which related to the letter he mentioned—I have a copy—which the shadow Home Secretary sent to the Home Secretary. This consideration is an answer to the letter; I might even go so far as to say that I am the personification of the answer to the letter. None the less, it is important that a reply is drawn up, not least because that reply will be useful to the Opposition in helping to frame their further ideas. For that reason, I will ensure that a reply to the letter is sent in good time, so that all members of the Committee, mindful of that response to the original letter, can form their consideration accordingly..

Keir Starmer: I accept that we will deal with most of the points in the letter when we get to specific clauses—that is an appropriate way forward. The issue of most concern in the letter, which I ask the Minister to consider, is that of the independent assessment of bulk powers. The Committee will not be looking at the operational case in the way that is called for in the letter. It is simply a timing issue: if there is to be any movement here, it needs to be quick. A speedy response would be welcome.

10 am

Mr Hayes: Let me deal with that specific point. It is true that there will always be a debate about what is on the face of Bills and what is in supporting documentation. The hon. and learned Gentleman mentioned the codes of practice. I emphasise these are draft codes of practice and, of course, it is important that the consideration by the Committee informs how their final version will be framed. The reason we published them was partly so that we could have a better debate here and learn from it in drawing up the final codes of practice.

The hon. and learned Gentleman will know very well that there is a perennial argument about how much is placed on the face of the Bills because of the problem that creates in terms of rigidity, particularly in highly dynamic circumstances, such as those we face in relation to some of these matters. However, I accept that from a legal perspective what is on the face of the Bill adds additional weight to the protections that the hon. and learned Gentleman seeks. I understand that argument and have no doubt it will permeate much of what we consider. I re-emphasise that the codes of practice are themselves not set in stone and will undoubtedly metamorphose as a result of our considerations.

The hon. and learned Gentleman raised a second point in respect of bulk powers and particularly the operational case that needs to be made for such powers. This is a highly sensitive issue. All Governments of all political persuasions have recognised that, because we are dealing with some matters that cannot be debated publicly. That applies to the operational case that the Security Services might need to make when requesting powers to intercept communications, for example, but it could be the case with a number of other powers.

Furthermore, I accept that there are particular sensitivities in respect of bulk powers. The hon. and learned Gentleman and the Committee have been briefed by the intelligence and security services as part of our considerations. He will know that GCHQ use bulk powers very extensively in a number of highly sensitive operations, and there is a limit to how much of that can be placed on the face of the Bill or even made available more widely.

The hon. and learned Gentleman will also know that the Intelligence and Security Committee has privileged access to more information than the House as a whole. It exists, in part, for that purpose. It provides a means by which the Government can be held to account by a Committee made up of members of all political parties in this House. The case that the shadow Home Secretary makes on the definition of the operational case for exercise of these powers is something that we will consider. However, I emphasise that we are treading on quite sensitive ground here and there may be a limit to how far the Home Secretary or I can go. I am sure the hon. and learned Gentleman will want to acknowledge that.

Keir Starmer: I am grateful that the Minister will give further consideration to the matter. The reason it is of great concern is because, first, we are being asked to approve new powers in the Bill. I accept that some of the powers are obviously avowal of existing powers, but there are new powers and internet connection records is one. Of the avowal powers, this is the first time that Parliament has had the chance to debate them, so they are new to Parliament in that sense.

I take the point that members of the Committee have been briefed and some of us have experience of the operation of some of these powers, but therein lies part of the problem. I think there is a democratic deficit if we proceed only on the basis that a select number of people can know the detail, but the public cannot. Of course there are sensitivities. I do not think anyone is suggesting that a full operational case without any modifications, redactions and so on, could be published. I ask for consideration of something more than what we have that allows for independent assessment, which does not necessarily need to take place in the public domain, but can be viewed through the eyes of the informed member of the public who wants to be assured

about the necessity of the powers without having to listen to politicians or others saying, "We've been briefed; trust us", because in this day and age that approach is no longer acceptable. I hope the Minister and others will try to see this through the eyes of the informed and concerned member of the public who wants to be assured about what the Bill is actually bringing forth for the security and intelligence services and law enforcement.

Mr Hayes: I do not want to get into a great debate about this now because we are at the beginning of the Bill and this will come up again during further consideration. I acknowledge that the hon. and learned Gentleman has recognised there is a sensitivity about how much can be put in the Bill and how much can be debated in a public forum. He is right that we tread a tightrope between making sure that we have public confidence that the system is fit for purpose, but also proportionate, and on the other hand not tying the hands of those wishing to keep us safe. That is the tightrope that every Government of all persuasions has had to walk.

Whether the hon. and learned Gentleman is right about a changing public mood is more debatable. Most surveys of the public mood suggest a very high level of confidence in our intelligence and security services and the powers that they exercise, so I am not sure there is a great public clamour for them not to be able to do some of the things they have to do. Contextually, given the threat we now face, I suspect most of the public would say they need absolutely all the powers necessary to face down that threat, so I am not absolutely sure that we do not occasionally see these things through the prism of a chattering class view of what the public should think, rather than what the public actually think. I am committed to the idea of politicians continuing to be involved in these things, because we have a regular and direct link to the British public and are in a pretty good position to gauge what their attitudes to such matters might be. So the issues are sensitive, but I appreciate the spirit and tone of the hon. and learned Gentleman and I am determined that we get this right in a way that we can both be comfortable with in the end.

The hon. and learned Gentleman asked how we might subsequently deal with issues around authorisation. We will have a chance to debate that at greater length as we go through the Bill, so it would be inappropriate to do so now. That point was made by the hon. and learned Member for Edinburgh South West. I think we are going to disagree about quite a lot of these matters, not because I do not want to move ahead in the spirit of generosity and unanimity where we can possibly do so, but I think that my position is more like that of the former Home Secretaries who gave evidence to the Committee, Lord Reid and Charles Clarke, who were very clear that the involvement of Ministers in authorising powers is an important way in which the public can be represented in these areas. Ministers bring a particular insight to such work. I was unsurprised by their consideration, but pleased that they were able to reinforce the view that I know is held by almost everyone who has been involved in the warranting process in modern times.

We heard from the former Secretary of State for Northern Ireland, my right hon. Friend the Member for North Shropshire (Mr Paterson), in similar vein. Indeed, he was doubtful about giving judges any role in the process at all, and many others take that view. The Government, however—always anxious to achieve balance and compromise—developed the double-lock, which the hon. and learned Gentleman mentioned. It retains the involvement of Ministers, as Lord Reid and others argued we should, but introduces judicial involvement and, one might argue, adds a greater degree of empiricism to the process, as David Anderson recommended in his report.

Joanna Cherry: The Minister will recall that, under questioning by the hon. and learned Member for Holborn and St Pancras, Lord Judge, in his evidence to this Committee, expressed concern about the phrase "judicial review". He said that it

"is a very easy phrase to use. It sounds convincing, but it means different things to different people…Personally, I think that when Parliament is creating structures such as these, it should define what it means by 'judicial review'. What test will be applied by the judicial…commissioner, so that he knows what his function is, the Secretary of State knows what the areas of responsibility are and the public know exactly who decides what and in what circumstances? I myself do not think that judicial review is a sufficient indication of those matters."—[*Official Report, Investigatory Powers Public Bill Committee,* 24 March 2016; c. 69, Q220.]

What are the Government going to do to take on board what that distinguished judge had to say about this matter?

Mr Hayes: Yes, but Lord Judge also went on to say in the same evidence session that what really matters is what Parliament actually wants. He wanted to be clear about what Parliament wants and to respond accordingly. I heard what Lord Judge said, but I also heard what Lord Reid and Charles Clarke said. Frankly, I see no evidence that the warranting process is not considered carefully by Ministers, that they do not take that work incredibly seriously, that they do not seek all the information they need to exercise reasonable judgment and that they do not apply the tests of necessity and proportionality diligently. Neither this Committee nor the Joint Committee heard evidence to suggest that there is anything faulty in that system.

I am a conservative, so I would be expected to say that if something works there is no good reason for changing it, but because I want to be moderate and reasonable—notwithstanding my conservatism—we introduced the double-lock. My goodness, we have already gone a very long way down the road.

Keir Starmer: We are going to get to this issue in due course. I will not take long, but it is important that I set it up, because the more thinking that can be done now, the more quickly we can deal with it when it comes up. There are two different issues. Lord Reid talked about whether the judiciary should be involved at all. Lord Judge asked, assuming that they are involved, about the test that they are to apply. He was concerned about judicial review because, as everybody knows, there are different forms of judicial review. Sometimes it involves close scrutiny, where the judges virtually make the decision themselves. In other circumstances, there is much more deference. He was concerned that, within that range, it is not clear what the judges are being asked to do.

There were a number of references in the questioning and on Second Reading to the necessity and proportionality tests. Of course, that is what the Secretary of State considers, but the judges' function is different. On the face of the statute, their function is to review. The question is, what does that mean? We tabled amendments to that end. It is important that we do not confuse this

[Keir Starmer]

matter. Lord Judge identified something very important, and when someone as distinguished as him says that what is on the face of the Bill is not clear enough, we have all got to go away and have a good, hard look at what the words are.

Mr Hayes: The hon. and learned Gentleman is right that we should not debate things that are going to be debated later—Ms Dorries, you will draw me to order if I do so anyway. The important issues around judicial review principles will be debated when we come to a subsequent amendment. My hon. and learned Friend the Solicitor General will deal with those matters. Lord Judge drew attention to the basis on which the double-lock will operate. The hon. and learned Gentleman is right about that. My point in response to the hon. and learned Lady's argument was about whether politicians should be involved in the process at all. I do not mean to be unkind to the hon. and learned Gentleman, and I certainly do not want to start off in anything other than a convivial spirit. However, given that the shadow Home Secretary's letter talks about an equal lock, given that he has argued for the simultaneous presentation of the material to both parties and given the great debate about the same information being available to the judicial commissioner and the Home Secretary, I was slightly surprised to find that amendments had been tabled that would take the Home Secretary out of the process altogether.

10.15 am

That is an extraordinary proposal, given that the Government have tried to strike a reasonable balance, as I say. As the hon. and learned Gentleman will say—and if I do not say it I am sure he will recognise that I am avoiding the issue—we did so in part because that is what the independent commissioner recommended. As the hon. and learned Gentleman will know, the commissioner made the argument in his report before the draft Bill that it was important to have judicial involvement in the process. We listened to that. It was not the status quo position, and it was not the position that previous Governments had adopted, but we felt that it was right to use the Bill to add that additional check to the system. It is a very significant change. I repeat what I said earlier, that it is perhaps the most significant change in authorisation since the intelligence and security services began in their modern form.

We are beginning to stray into areas that will be debated later. I will end by saying that it has already become clear that the Committee recognises that we are all doing a highly significant piece of work, because this is a very significant change—indeed, it is a landmark change. It is important that we get this right, and that we come out of this Committee having given the Bill the consideration it requires to allow it to be in as good a form as possible as it continues its passage through this House and beyond. This Bill is iterative, as are all Bills. It must both give the powers that are necessary to those who need them, and put into place those vital checks and balances that guarantee the public interest and maintain proper privacy.

Question put and agreed to.

Clause 1 accordingly ordered to stand part of the Bill.

Clause 2

OFFENCE OF UNLAWFUL INTERCEPTION

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

The Chair: With this it will be convenient to discuss new clause 3—*Tort or delict of unlawful interception—*

"Any interception of a communication which is carried out without lawful authority at any place in the United Kingdom by, or with the express or implied consent of, a person having the right to control the operation or the use of a private telecommunication system shall be actionable by the sender or recipient, or intended recipient, of the communication if it is either—

(a) an interception of that communication in the course of its transmission by means of that private system; or

(b) an interception of that communication in the course of its transmission, by means of a public telecommunication system, to or from apparatus comprised in that private telecommunication system."

This new clause creates a civil wrong of unlawful interception.

Joanna Cherry: I will deal with new clause 3 in fairly short compass. The amendment was suggested to me by the Scottish division of Pen International, which is a world association of writers. It would introduce a tort, or a delict as we call it in Scotland, for unlawful interception. Such a tort or delict exists already as a result of section 1(3) of the Regulation of Investigatory Powers Act 2000, and I am not entirely sure why it has not been replicated in the Bill. I would be interested to hear from the Solicitor General or the Minister for Security why the Government did not include the measure in the Bill, and whether they will give it serious consideration. It would give a meaningful avenue of recourse and act as a motivation to intelligence agencies, police forces and the Government to ensure that all interception is lawfully authorised, on pain of an action for damages if it is not properly authorised. It is really a very simple new clause modelled on section 1(3) of RIPA. I am interested to hear what the Government have to say about this suggestion.

The Solicitor General (Robert Buckland): It is a pleasure to take this first opportunity to say that I am looking forward to serving under your chairmanship, Ms Dorries, and indeed to serving with all colleagues on the Committee.

I am grateful to the hon. and learned Lady for making her observations in a succinct and clear way. I am able to answer her directly about the approach that we are taking. One of the aims of the Bill is to streamline provisions to make them as clear and easy to understand as possible. She is quite right in saying that RIPA had within it this provision—a tort or a delict, as it is called north of the border, that would allow an individual to take action against a person who has the right to control the use or operation of a private telecommunications system and to intercept communication on that system.

The Government have fielded a number of inquiries about the non-inclusion of the RIPA provision in the Bill. The circumstances in which it applies are extremely limited, and as far as we are aware it has never been relied on in the 15 years of RIPA's operation. The provision applies only in limited circumstances because it applies to interception on a private telecommunications system, such as a company's internal email or telephone

system. Where the person with the right to control the use or operation of the system is a public authority, there are of course rights of redress under the Human Rights Act 1998, such as article 8 rights.

The Bill is intended to make the protections enjoyed by the public much clearer and we feel that introducing that course of action or replicating it would not add to that essential clarity, but I have listened carefully to the hon. and learned Lady and we are happy to look again at the issue in the light of her concerns. On that basis, I invite her not to press her new clause and I hope we can return to the matter on Report.

Joanna Cherry: I am grateful to the Solicitor General for his constructive approach. I am happy not to press the new clause at this stage on the basis that the Government will look at it. I am happy to receive any suggestions about the drafting, which is mine. I had some discussions about the terms of the drafting with Michael Clancy of the Law Society of Scotland and James Wolffe, the dean of the Faculty of Advocates, but any infelicities are my fault alone. I would be happy to discuss the drafting with the Government.

Question put and agreed to.

Clause 2 accordingly ordered to stand part of the Bill.

Clause 3

DEFINITION OF "INTERCEPTION" ETC.

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

Keir Starmer: There are no amendments tabled to the clause, which we support, but I say for the record and for clarification that what is welcome in clause 3 is the spelling out in legislation of the extent of an interception—an issue that has bedevilled some recent criminal cases. Importantly, as the explanatory notes make clear, it is now provided in clear terms that voicemails remaining on a system, emails and text messages read but not deleted and draft messages stored on a system will count within the phrase "in the course of transmission" and will therefore be covered by the offence. We welcome that. I wanted to emphasise that point and put it on the record, because a lot of time and effort was spent when that phrase was not so clearly defined.

The Solicitor General: I am extremely grateful to the hon. and learned Gentleman. He is right: we have moved a long way from phone tapping, which he, I and many others understood to be clear interception whereas, for example, the recording and monitoring of communications at either end of the process was not interception. As he rightly says, the internet and email have caught up with us, so as part of the Government's thrust to have greater clarity and simplicity, this essential definition is a welcome part of the statutory framework that now exists.

Question put and agreed to.

Clause 3 accordingly ordered to stand part of the Bill.

Clauses 4 and 5 ordered to stand part of the Bill.

Clause 6

MONETARY PENALTIES FOR CERTAIN UNLAWFUL INTERCEPTIONS

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

Keir Starmer: Again no amendments are tabled to the clause, but there are some questions that arise from it. The explanatory notes say, and it is clear in the Bill, that the clause creates a power for the Investigatory Powers Commissioner to impose fines where an interception has been carried out, but there was no intention. It relates to action that might otherwise be an offence, but the intention element is not made out. Against that background, I have some questions for the Solicitor General.

If the power applies where an interception is carried out but there was no intention to do so, it is hardly likely to have a deterrent effect because the person did not intend to do it in the first place, so what is the rationale and purpose of this provision? It is clear in schedule 1, which is related to clause 6, that the commissioner has very wide discretion in relation to the operation of the powers under the clause including, in paragraph 13, powers to require information from individuals

"for the purpose of deciding whether to serve"

an enforcement notice. Thus we have a provision that is premised on a non-intentional interception that then triggers quite extensive powers to require information with penalties for failure to provide that information. Schedule 1 states that guidance will be published on how the powers are to be exercised, but what is the real rationale and purpose? Why are the powers as extensive as they are and will the Minister commit to the guidance envisaged under schedule 1 being made public?

In clause 6(3)(c) there is reference to a consideration by the Commissioner that

"the person was not…making an attempt to act in accordance with an interception warrant",

which suggests that that is outside the scheme of the provision. We have also noted that the provision relates only to a public telecommunications system. It is in many ways supplementary or complementary and we are not questioning it in that sense, but there is a number of unanswered questions. If we are to scrutinise and probe, it would be helpful to have those answered now if possible, and if it is not answered in writing.

The Solicitor General: I am grateful to the hon. and learned Gentleman for his questions. I assure him that there is a very good rationale for the inclusion of these powers. They are a replication of powers that were added to RIPA in 2011. Monetary penalty notices followed a letter of formal notice that was issued by the European Commission setting out its view that the UK had not properly transposed article 5(1) of the e-privacy directive and articles of the data protection directive. In particular, the Commission identified:

"By limiting the offence in Section 1(1) RIPA to intentional interception, the UK had failed to create a sanction for all unlawful interception as required by Article 5(1) of the E-Privacy Directive and Article 24 of the Data Protection Directive."

[The Solicitor General]

The Government rightly conceded the defective transposition that had been identified and therefore the monetary penalty notice regime was established to introduce sanctions for the unintentional and unlawful interception in order to remedy the deficiency.

The hon. and learned Gentleman is quite right that it is a step down from a criminal offence, where intention has to be informed, but as my right hon. Friend the Minister for Security said when opening the debate, underpinning all of this is the importance of privacy, and the right to privacy is demonstrated in practical form by the inclusion of clause 6 and schedule 1. It is important so that we cover all aspects of intrusion because, as the hon. and learned Gentleman will know, privacy is not just about confidentiality. That is often misunderstood, particularly in the light of recent debates about injunctions. It is about intrusion into the lives of individuals, and that intrusion by the authorities in particular should be marked in some way by the imposition of some alternative sanction if it cannot be criminal sanctions. Therefore, there is a very sound rationale for the inclusion of these powers and replicating them from RIPA, and therefore I commend the clause to the Committee.

Question put and agreed to.

Clause 6 accordingly ordered to stand part of the Bill.

Schedule 1 agreed to.

Clause 7

RESTRICTION ON REQUESTING INTERCEPTION BY OVERSEAS AUTHORITIES

10.30 am

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

Keir Starmer: I have a probing question. It is right to include a provision that makes it clear that the UK authorities cannot evade the protections and safeguards in the Bill by requesting that a foreign authority carry out on their behalf the interception of materials relating to a person in the UK. That is right in principle and we support that. It may be my limitation in going through the provisions in recent weeks, but I am not sure whether there is a sanction for failure to adhere to the clause's provisions. In other words, it is good that it is there, but I am not sure whether anything formal will happen if it is not followed. Will the Minister answer that now or at least give some consideration to that?

The clause is important and right in principle, but I cannot find a sanction for failing to comply with it and there probably ought to be one. If it is somewhere else in the Bill, I will defer to those who know it better than I do.

Mr Hayes: I am happy to say on behalf of my hon. and learned Friend the Solicitor General that we will give consideration to that.

Question put and agreed to.

Clause 7 accordingly ordered to stand part of the Bill.

Clause 8

RESTRICTION ON REQUESTING ASSISTANCE UNDER MUTUAL ASSISTANCE AGREEMENTS ETC.

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

Keir Starmer: I rise to make essentially the same point as I made on the previous clause, albeit more briefly. This is a good and right in principle clause to ensure that there are restrictions on requesting assistance under mutual assistance agreements, but again the sanction for breach is not entirely clear. That may be something that, under the umbrella that the Minister for Security just indicated, could be taken away to see what the enforcement regime is for these important safeguarding provisions.

The Solicitor General: The hon. and learned Gentleman will know that this mutual legal assistance regime definitely benefits from statutory underpinning. It has become increasingly important. Sadly we have all learnt that relying just on good will or informal arrangements is no longer sufficient, which is why the international work that I know hon. Members are aware of, particularly negotiations with the United States, are so important in speeding up the process and making it ever more efficient, particularly in the light of all the political controversies we have been dealing with in recent days. I undertake to deal with the question that he raises, which I think we can deal with in an umbrella form as he suggests.

Question put and agreed to.

Clause 8 accordingly ordered to stand part of the Bill.

Clause 9

OFFENCE OF UNLAWFULLY OBTAINING COMMUNICATIONS DATA

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

The Chair: With this it will be convenient to discuss new clause 4—*Tort or delict of unlawfully obtaining communications data—*

"The collection of communications data from a telecommunications operator, telecommunications service, telecommunications system or postal operator without lawful authority shall be actionable as a civil wrong by any person who has suffered loss or damage by the collection of the data."

This new clause creates a civil wrong of unlawful obtaining of communications data.

Joanna Cherry: The new clause very much relates to what I said earlier about new clause 3. The intention is to create a civil wrong of unlawfully obtaining communications data as opposed to unlawful interception. Again, the drafting is mine and it could do with some serious tightening up, but my intention is to establish the Government's attitude to the new clause. I hope that the Solicitor General will indicate that.

The Solicitor General: I am grateful to the hon. and learned Lady for the way in which she spoke to her new clause. I see that it very much follows new clause 3.

Our argument with regard to new clause 4 is slightly different because it has a wider ambit than private telecommunication.

We submit that this tort or delict would not be practicable. Communications data are different from the content of communication. For example, one would acquire communications data even by looking at an envelope or searching for a wi-fi hotspot when turning on a particular wi-fi device at home. It would not be appropriate to make ordinary people liable for such activity. With respect to the hon. and learned Lady, its ambit is too wide. That said, it is only right that those holding office within a public authority are held to account for any abuses of power. That is why clause 9 makes it an offence for a person in a public authority to obtain communications data knowingly or recklessly without lawful authority. I place heavy emphasis on the Government's approach to limiting and checking the abuse of power by the authorities.

On the new clause, the interception tool was always intended to address the narrow area that was not covered by the interception offence in RIPA, which is replicated in the Bill. As noted, the communications data offence is intentionally narrower. It would therefore be equally inappropriate to introduce a tort or delict in relation to the obtaining of communications generally or in the areas not covered by the new offence. Under the provisions of the Data Protection Act 1998, communications data often constitute personal data. That act already provides for compensation for damage or distress resulting from non-compliance with the data protection principles and for enforcement in respect of failing to comply with the provisions of the act.

Lucy Frazer (South East Cambridgeshire) (Con): Does my hon. and learned Friend think that the offence of misfeasance in public office would also add a civil remedy for any wrongdoing?

Robert Buckland: I am extremely grateful to my hon. and learned Friend. She is quite right. In fact, not only is there the offence of misconduct in public office, as it is now constituted, having been reformed from the old offence of misfeasance, but we have provisions in the Wireless Telegraphy Act 2006, the Computer Misuse Act 1990 and, as I have already mentioned, the Data Protection Act 1998. I therefore consider that the new offence we are introducing in clause 9, combined with relevant offences in other legislation, in particular the provision in section 13 of the Data Protection Act 1998, provides appropriate safeguards. On that basis, I respectfully invite the hon. and learned Lady to withdraw the amendment.

Christian Matheson (City of Chester) (Lab): It is, as always, a pleasure to see you in the Chair, Ms Dorries. The Solicitor General has given examples of wide-ranging powers that are available to protect the public. I was grateful to listen to his contribution. However, during Second Reading I queried the Home Secretary's position on the new offences that are being created. Many of the offences the Bill refers to, particularly in clause 9, relate to the regulation of investigatory powers. My concern is that later the Bill requires internet service providers, for example, to amass a large amount of personal data, and there is a danger that those data may be stolen rather than intercepted. I gave the example of a newspaper perhaps finding a low-grade technical operator in a telecommunications company, passing a brown envelope to them and stealing a celebrity's internet connection records. I am concerned that the offence in clause 9 of unlawfully obtaining communications data does not go far enough.

I bear in mind the Solicitor General's comments on other protections that are available, but would he or the Government consider an offence of not just obtaining but being in possession of unlawfully obtained communications data, which would strengthen the protections given to members of the public? We all know that the kind of scenario that I am expressing concern about has not been unknown in the last few years, as various court cases have demonstrated—though I should not discuss their details. Is the Minister satisfied that the protections he has outlined and those raised by the hon. Member for South East Cambridgeshire are sufficient, or should we take this clause a bit further, to give the public broader and wider protection of their privacy and the security of their internet and telecommunications transmissions?

Keir Starmer: It is a pleasure to follow my hon. Friend because I want to develop the point. This is a welcome clause, it is right that it is here, and we support it. However, we question whether it goes far enough. It only covers obtaining communications data. We think that serious consideration should be given to an overarching offence of misuse of the powers in the Bill. At the moment, there are specific provisions in relation to intercept which are replicated frim RIPA and we now have this welcome provision, but there is no overarching offence of misuse of the powers in the Bill.

It is all very well to say that there is the tort of misfeasance in public office. That is not the equivalent of a criminal offence. It has all sorts of tricky complications when one tries to apply it in practice. It is fair to say that there are other bits of legislation that might be made to fit in a given case, but it would be preferable and in the spirit of David Anderson's approach for a comprehensive piece of legislation for an overarching criminal offence to be drafted, either out of clause 9 or in some other way, relating to misuse of powers in the Bill. It has been a source of considerable concern in the past and I ask the Government to think about a wider offence that would cover all the powers, because comms data are only one small subset of the issues and material information we are concerned with.

I have two short supplementary points. In subsection (3) there is a reasonable belief defence. It would be helpful if the Minister said a bit more about that. May I also foreshadow the inconsistency that we will need to pick up as we go along in the way reasonable excuse and reasonable belief are dealt with in the Bill? It is set out in subsection (3), but there is an inconsistency in other provisions that I will point to when we get there.

My other point is to ask the Minister to consider whether obtaining communications data unlawfully is a sufficient definition to make the offence workable in practice. I put my questions in the spirit of supporting the clause, but I also invite Ministers to go further and consider drafting a clause that covers the misuse of powers in the Bill, rather than simply saying that if we fish about in other bits of legislation or common law we

[Keir Starmer]

might find something that fits on a good day. In my experience, that is not a particularly helpful way of proceeding.

The Solicitor General: Thank you, Ms Dorries, for allowing me to reply to a stand part debate on clause 9. I think we have elided the this and the previous clause, but I crave your indulgence to deal with everything in a global way. May I deal properly with clause 9 and set out the Government's thinking on this?

The measure is all about making sure once again that those who hold office within a public authority are properly held to account for any abuses of power. The clause will make it an offence knowingly or recklessly to obtain communications data from a communications service provider without lawful authority. Somebody found guilty of that offence might receive a custodial sentence or a fine. The maximum punishment will vary according to whether the offence was committed in England and Wales, or in the jurisdiction of Scotland or Northern Ireland.

The hon. and learned Gentleman is right to point out the reasonable belief defence. The offence will not have been committed if it can be demonstrated that a person holding office acted in the reasonable belief that they had lawful authority to obtain the data. Where a communications service provider willingly consents to the disclosure of the data, including by making it publicly or commercially available, that would constitute a lawful authority.

The question about reasonable belief is about making sure that genuine error is not penalised, because there will be occasions when genuine errors are made. In the absence of such a defence, public authorities could be deterred by notifying genuine errors to the IPC. It is important that the Investigatory Powers Commission is an effective body monitoring failure and lack of best practice, and preventing future errors.

I think the hon. and learned Gentleman will agree that we both have fairly considerable criminal litigation experience. In this area, I think a regulatory approach will be just as effective, and in some ways more effective, than a criminal sanction. I am grateful to the hon. Member for City of Chester for reiterating the remarks that I remember him making on Second Reading, when he made some powerful points, but I caution that we are in danger of creating an entirely new criminal framework, catching people further down the line, which ultimately will only lead to more confusion and, I worry, the replication of existing offences.

An unauthorised disclosure by someone in a communications service provider would be covered by the Data Protection Act 1998, because those providers have duties and obligations under that Act just like any other holder of data. I hear what the hon. and learned Gentleman says, and I will consider the matter, but my initial reaction to his question and that of the hon. Member for City of Chester is that the Data Protection Act covers such a disclosure.

10.45 am

Victoria Atkins (Louth and Horncastle) (Con): I have heard Opposition Members' arguments. Some thought has been given to this point and clause 49 puts a duty not only on people who work in public services but on postal operators, telecommunications operators and any person employed therein to not make unauthorised disclosures in relation to intercept warrants. That might help.

The Solicitor General: I am grateful to my hon. Friend, who served with distinction on the Joint Committee. That provision relates to creating a statutory duty, which, with respect to her, is slightly different from some of the arguments we are having about criminal sanctions. However, it is important to pray that in aid, bearing in mind the mixed approach we need to take in order to hold public office holders and public authorities to account when dealing with this sensitive area.

The Bill provides a great opportunity for us to put into statute a new offence, which will, together with the other agencies, provide a robust regime that will add to the checks and balances needed in this area in order to ensure that our rights to privacy are maintained wherever possible, consistent with the Government's duty towards the protection of our national security and the detection and prevention of crime.

Christian Matheson: I am grateful to the Solicitor General for that clarification. My concern about his reliance on, for example, the Data Protection Act is what happens in the scenario I described, which I do not believe is so unbelievable, bearing in mind the experiences that hon. Members of this House have had in the past few years with the theft of their information. One problem that his solution presents is that if, for example, my personal data were stolen and published, the only recourse I would have is to the telecommunications provider, which is in a sense a victim itself. The real villains and culprits—the people who stole the information and published it—would not be covered by the Data Protection Act, which is why I seek consideration of extending the clause or guidance from the Solicitor General.

The Solicitor General: I hear what the hon. Gentleman says. I have already indicated that I will consider the matter further. I will simply give this solution. He mentioned the stealing of information. Information is property, like anything else, and of course we have the law of theft to deal with such matters. I do not want to be glib, but we must ensure we do not overcomplicate the statute book when it comes to criminal law. I will consider the matter further, and I am extremely grateful for his observations.

Question put and agreed to.

Clause 9 accordingly ordered to stand part of the Bill.

Joanna Cherry: On a point of order, Ms Dorries, may I seek clarification on my position on new clause 4, which the Minister invited me to withdraw? I am minded to do so, having regard to what the Solicitor General said about the Data Protection Act and what the hon. and learned Member for South East Cambridgeshire said about misfeasance in public office, but as a novice in these Committees I seek some guidance. If I press the new clause to a vote now and it is voted down, does that prevent me bringing it back to the Floor of the House?

The Chair: As I made clear at the beginning of our sitting, you could move the motion at the end of consideration, but that does not prevent you from bringing the new clause back on Report. This point in the proceedings is not the time for it.

Joanna Cherry: I realise that, but my point is about the conflicting information on the issue. If an amendment is pressed to a vote and voted down in Committee, some people tell me that it cannot then be brought before the House at a later stage; others tell me that that is not the case. I am anxious to have the Chair's clarification.

The Chair: It is not normal, but it does sometimes happen; it is at the Speaker's discretion. If voted down, you would have to retable the amendment and it would be up to the Speaker, who would know that it had been heard in Committee and voted down.

Joanna Cherry: I am grateful. So if I withdraw the new clause now, I cannot be prevented from bringing it back later—I will withdraw it in Committee.

Clause 10 ordered to stand part of the Bill.

Schedule 2 agreed to.

Clause 11

MANDATORY USE OF EQUIPMENT INTERFERENCE WARRANTS

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

Keir Starmer: I will be very quick. The clause is welcome and we support it, but again my concern is that there is no enforcement mechanism or sanction. Will the Minister take it under the umbrella of these clauses that are intended to ensure good governance, effectiveness and that the proper routes are used, and look in an overarching way at what their sanction might be? I am asking a similar question to one I made before: what is the sanction if what should happen does not happen?

The Solicitor General: Yes, of course, we will do as the hon. and learned Gentleman asks. I welcome his endorsement of the importance of the clause, bearing in mind what it sets out and the clarity we are achieving through its introduction.

Question put and agreed to.

Clause 11 accordingly ordered to stand part of the Bill.

Clause 12

RESTRICTION ON USE OF SECTION 93 OF THE POLICE ACT 1997

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

Keir Starmer: I make the same point again: the clause is a good provision but appears to lack any enforcement mechanism or sanction, so if it could go into the basket of clauses that are being looked at in relation to sanction, I will be grateful.

The Solicitor General: The clause confirms that section 93 of the Police Act 1997 may not be used to authorise conduct where the purpose of the proposed interference is to obtain communications, private information or equipment data and the applicant believes the conduct would otherwise constitute an offence under the Computer Misuse Act 1990, and the conduct can be authorised under an equipment interference warrant issued under part 5 of the Bill. So it does not prevent equipment interference being authorised under the Police Act where the purpose of the interference is not to obtain communications and other data—for example, interference might be authorised under the Act if the purpose is to disable a device, rather than to acquire information from it.

That reflects the focus of this Bill. We are trying to bring together existing powers available to obtain communications and communications data. I emphasise that the measure does not prevent law enforcement agencies from using other legislation to authorise interference with equipment that might otherwise constitute an offence under the Computer Misuse Act. For example, law enforcement agencies will continue to exercise powers under the Police and Criminal Evidence Act 1984 to examine equipment that they possess as evidence. The result of this clause is that all relevant activity conducted by law enforcement agencies will need to be authorised by a warrant issued under part 5 of the Bill.

Keir Starmer: Based on what the Minister has just said, it may be that it is anticipated that any attempt to use other legislation in breach of this provision would automatically be refused. That is the bit where there might need to be some clarity, because in effect it will not be an application under this legislation; it would be an application under different provisions, so does this operate as a direction to any decision maker that that is an unlawful use of another statute? That is not entirely clear. I think that that is what is intended. If it is, that is a good thing, but I am not entirely sure that a decision maker would say, "I am prohibited by law from exercising powers available to me under other legislation." I leave that with the Minister because it may be something that can be improved by further drafting.

The Solicitor General: I thank the hon. and learned Gentleman for that intervention. While I will answer the specific question, I think it is important that I set out the fact that this provision is not the only means. What we are dealing with here is part 5 and the double lock and the enhanced safeguards. If any agency or authority fails to use new part 5 or PACE, for example, in other circumstances, they will be committing an offence under the Computer Misuse Act. Public authorities are no different from any other individual or body: if they are not complying with the existing legal framework by this or other means, they fall foul of the law themselves. I will endeavour to answer the other points raised about sanction but I urge the Committee to agree that the clause stand part of the Bill.

Question put and agreed to.

Clause 12 accordingly ordered to stand part of the Bill.

Clause 13

WARRANTS THAT MAY BE ISSUED UNDER THIS CHAPTER

Keir Starmer: I beg to move amendment 57, in clause 13, page 10, line 16, after "content", insert "or secondary data"

[Keir Starmer]

This amendment, and others to Clause 13, seek to expand the requirement of targeted examination warrants to cover the examination of all information or material obtained through bulk interception warrant, or bulk equipment interference warrant, irrespective of whether the information is referable to an individual in the British Islands. They would also expand the requirement of targeted examination warrants to cover the examination of "secondary data" obtained through bulk interception warrants and "equipment data" and "information" obtained through bulk equipment interference warrants.

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

Amendment 58, in clause 13, page 10, line 17, leave out from "examination" to end of line 18

Amendment 59, in clause 13, page 10, line 17, leave out from "examination." to end of line 18 and insert

"of material referable to an individual known to be in the British Islands at that time, or British citizen outside the British Islands at that time."

Amendment 60, in clause 13, page 10, line 17, leave out from "examination." to end of line 18 and insert

"of material referable to an individual known to be in the British Islands at that time, or British, Canadian, American, New Zealand or Australian citizen outside the British Islands at that time."

Amendment 83, in clause 13, page 10, line 22, after "6", insert—

"In this Part "secondary data" means—

(a) in relation to a communication transmitted by means of a postal service, means any data falling within subsection (5);

(b) in relation to a communication transmitted by means of a telecommunication system, means any data falling within subsection (5) or (6)."

Keir Starmer: I rise to speak to amendments 57, 59 and 60. Amendment 57 deals with secondary data; amendments 59 and 60 deal with place and whether someone is in the British Isles. I apologise, Ms Dorries: the provision and the amendment are complicated. With your permission I will take some time to set the context so that the amendment can be understood.

Clause 13 deals with warrants. Subsection (1) deals with targeted interception warrants, targeted examination warrants and mutual assistance warrants. Subsection (2) states:

"A targeted interception warrant is a warrant which authorises or requires the person to whom it is addressed to secure, by any conduct described in the warrant, any one or more of the following",

and paragraph (a) deals with the interception of communications. That is content; paragraph (b) deals with secondary data from the communication; and paragraph (c) deals with disclosure. For targeted warrants under clause 13 there are specific provisions in relation to the content, secondary data and disclosure.

Secondary data for these purposes is further defined in clause 14, subsection (5) of which states:

"The data falling within this subsection is systems data which is comprised in, included as part of, attached to or logically associated with the communication",

so it has an integral link to the communication and thus to the content.

11 am

The Chair: Order. Mr Starmer, if you could keep your comments to clause 13 with just passing reference to clause 14 and further clauses, that would be great.

Keir Starmer: I will, but on this particular occasion, I really think it is almost impossible to understand clause 13(3) without going into clause 14 and then, I am afraid, to a further provision, before coming back.

The Chair: You can only do so in passing reference.

Keir Starmer: In passing, this is just really to explain what the amendment is intended to achieve. In order to understand what is in clause 13(2), we need to look to clause 14(4) to (6), which set out what secondary data means for the purposes of this part and, thus, is to be read into clause 13.

Clause 14(6) states:

"The data falling within this subsection is identifying data which…is comprised in, included as part of, attached to or logically associated with…is capable of being logically separated…and if it were so separated, would not reveal anything of what might reasonably be considered to be the meaning",

so it is integrally bound up with the content of the communication but capable of being separated from it.

So far as clause 13 is concerned, if there is a targeted interception warrant, the warrant deals specifically with content and secondary data, recognising the integral link between the two. That is right and we do not quarrel with that.

Clause 13(3) is different, providing that:

"A targeted examination warrant is a warrant which authorises the person to whom it is addressed to carry out the selection of relevant content for examination, in breach of the prohibition in section 134(4) (prohibition on seeking to identify communications of individuals in the British Islands)."

The purpose of clause 13(3) is different. We move from the targeted warrant to the bulk warrant—an examination warrant that provides authority to examine the content that would otherwise be in breach of clause 134(4). In order to understand that, I take the Committee to clause 119, to which that relates.

Clause 119 deals with bulk interception warrants, which can be issued if conditions A and B are satisfied. Condition A deals with

"the interception of overseas-related communications"

and with "obtaining…secondary data". The definition of secondary data is the same in that part of the Bill as it is in the part that we have just looked at. I will not test the Committee's patience by going to that definition, but it is a consistent definition of secondary data.

Condition B sets out that the bulk warrant authorises "the interception", which is the content,

"the obtaining of secondary data",

which is the same as a targeted warrant but in relation to the bulk powers, and

"the selection for examination, in any manner described…of…content or secondary data"

and "disclosure". The bulk warrant allows the interception of the content and secondary data. In and of itself, it provides for the examination on the face of the same warrant.

For content, it becomes more complicated because there is a safeguard, which is in clause 134(4)—safeguards in relation to examination materials. Having provided a broad examination power, there is then a safeguard for that examination power in clause 134(4). A number of conditions are set for examining material that has been obtained under a bulk interception warrant. They are set out in subsection (3) and the first is that

"the selection of the intercepted content for examination does not reach the prohibition in subsection(4)"

which is that

"intercepted content may not…be selected for examination if—any criteria used for the selection of the intercepted content…are referable to an individual known to be in the British Islands at that time, and the purpose of using those criteria is to identify the content".

The long and short of it is that, going back to clause 13, a targeted intercept warrant authorises the examination of both content and secondary data.

For a bulk warrant—this is where clause 13(3) kicks in—there is provision for an examination warrant which provides an ability to look at the content, which in all other circumstances would be a breach of the prohibition in clause 134. The content of communications of individuals in the British Isles can be looked at when it has been captured by a bulk provision, but only when there is a targeted examination warrant. That is a good thing.

What the amendment gets at is this. What is not in clause 13(3) is any provision for an examination warrant in relation to secondary data, so for the targeted provisions these two are treated as one: secondary data integral to the content of communication. When it comes to bulk, they are separated and only the content is subject to the further provision in clause 13(3).

That is a material provision and is a big part of the legislation because, unless amendment 57 is accepted, a targeted examination warrant is not required for secondary data, which are capable of being examined simply under the bulk powers. The purpose of the amendment is to align subsections (2) and (3) and ensure that the targeted examination warrant is not required for both content and secondary data in relation to individuals in the British Isles. The result otherwise would be that, for someone in the British Isles, their secondary data could be looked at as long as it was captured under a bulk provision without a targeted warrant. That is a serious drafting issue of substance.

Our approach to some of the wider retention of bulk powers is this. Although we accept that a case can be made for retaining data that will be looked at later, the wide powers of retentional bulk are a cause of concern on both sides of the House. When it comes to examining what has been caught within the wider net, there are specific safeguards. In other words, as long as there is a specific targeted safeguard when someone wants to look at bulk or retained data, that is an important safeguard when they are harvesting wide-ranging data. That is a very important provision in relation to secondary data.

Amendments 59 and 60 go to a different issue. They are separate and I ask the Government to treat them as separate. The first is about content and secondary data as a hom-set and whether they should be protected in the same way throughout the regime of the legislation, however they are initially intercepted. That is an important point of principle that I ask the Government to consider seriously because it goes to the heart of the question of targeted access.

The second amendment relates to individuals in the British Isles. At the moment, clause 13(3) provides specific protection in relation to the content of communications for people in the British Isles. It is clear from clause 134(4) that that means not residing in the British Isles, but actually in the British Isles. Under clause 13(3), once I get to Calais, I fall out of the protection of that provision, as does everybody else in this Committee, because it is a question of whether someone is physically in the British islands. Therefore, a targeted examination warrant for the content of my communications gathered by bulk powers would not be needed once I got halfway across the channel. Until I went through the analysis, I did not fully appreciate that, and serious consideration is required for both content and secondary data. More generally within amendment 59 are provisions relating to individuals not normally in the British islands or within the countries specified in amendment 60.

I am sorry to have referred to other clauses, but I could not work this out until I went through that torturous route. The net result is a disconnect between content and secondary data, which goes to the heart of protection when it comes to bulk powers. Clause 13(3) is really important for bulk powers and is one of the most important provisions in the Bill, so we have to get it right.

The limit of clause 13(3) to individuals in the British islands is unsustainable and needs further thought. Amendments 59 and 60 intend to remedy that defect. If there is an appetite in the Government to look carefully at those provisions, there may be a different way of coming at the problem, but it is a real flaw in the regime as it is currently set out. I apologise for taking so long to get to that, Ms Dorries. It required a cold wet towel on one afternoon last week to work my way through this, but once we go through the exercise, we realise there is a fundamental problem that either has to be fixed or adequately answered.

Joanna Cherry: I am 100% with the hon. and learned Gentleman in his description of the clause. Indeed, many clauses of the Bill require the application of a cold wet towel or a bag of ice to the head followed by copious amounts of alcohol later in the evening.

Amendments 57 and 83 bear my name and that of my hon. Friend the Member for Paisley and Renfrewshire North. I wish to emphasise the importance of those amendments, which foreshadow important amendments in respect of bulk powers that the Scottish National party intends to table at a later stage. Our amendments would apply the same processes and safeguards for the examination of information or material obtained through bulk interception warrants and bulk equipment interference warrants, irrespective of whether the information or material pertains to individuals in the British Isles, and to require a targeted examination warrant to be obtained whenever secondary data obtained through bulk interception warrants and equipment data and information obtained through bulk interference warrants are to be examined.

In order to gain an understanding of the background to this amendment, I invite hon. Members to look back at the evidence of Eric King to the Committee on

[Joanna Cherry]

24 March. He explained to us how GCHQ examines bulk material. The targeted examination warrant available on the face of the Bill fails to cover the aspect of communication that is most used by agencies such as GCHQ: metadata, or secondary data, as it is referred to in the Bill.

Simon Hoare: The hon. and learned Lady might have chosen a better witness. If I recall, the gentleman in question admitted in answer to my hon. Friend the Member for Louth and Horncastle that he had had no experience at all in the application for or determination of any warrants. He had never had any security clearance either, so I am uncertain why he is being prayed in aid.

Joanna Cherry: I must say that I do not like the approach of traducing witnesses. If I do not like a witness's evidence, I will not traduce them; I will just try to forensically dissect their evidence. This is a distinguished witness with significant experience in this field.

Victoria Atkins: Will the hon. and learned Lady give way?

11.15 am

Joanna Cherry: No, I will not give way. I am going to finish. Because of his technical expertise, Mr King has been of enormous assistance to myself and my hon. Friends in the Labour party in drafting amendments.

Hon. Members: Ah!

Joanna Cherry: Hon. Members may "Ah" and "Um", but Mr King has relevant technical expertise. I invite hon. Members to consider his CV.

Victoria Atkins: Will the hon. and learned Lady give way on that point?

Joanna Cherry: No, I will not. I will continue to make my point. The amendment was tabled because there should be a requirement to apply for an examination warrant when seeking to examine secondary data. That would protect the privacy of our constituents—I am looking at Government Members—and us. It is not some idle attempt of the chattering classes to be difficult about the Bill; it is an attempt to make the Bill compliant with the rule of law and with the requirement to protect the privacy of our constituents. That is all it is about. Criticising and making ad hominem comments about a witness are not going to undermine the moderate—

Victoria Atkins: Will the hon. and learned Lady give way?

Joanna Cherry: No, I will not give way. There will be plenty of opportunity for the hon. Lady to contribute later. I am conscious of the time, Chair, so I will briefly—

Simon Hoare: Will the hon. and learned Lady give way on that point?

Joanna Cherry: No, I will not. I want to continue making my point. Without the amendment, which we support, a GCHQ analyst would be able to search for and view non-content material of anyone in the United Kingdom without a warrant. I do not believe that that is right, necessary or proportionate.

Let us look at what the Intelligence and Security Committee said. If Government Members do not like Mr King's evidence, let us set him to one side and look at the ISC. Government Members might find its approach more palatable or less easy to criticise. In the ISC's response to the draft Bill, it highlighted the significant concern that the secondary data, including that derived from content, would not be protected. It said:

"To provide protection for any such material incidentally collected, there is a prohibition on searching for and examining any material that relates to a person known to be in the UK (therefore, even if it is collected, it cannot be examined unless additional authorisation is obtained). However, these safeguards only relate to the content of these communications. The RCD relating to the communications of people in the UK is unprotected if it is collected via Bulk Interception. In direct contrast, if the same material were collected and examined through other means (for example, a direct request to a CSP) then the draft Bill sets out how it must be authorised".

The ISC expressed a concern that the amendment attempts to address. Because no examination warrant is required for secondary data, a variety of highly intrusive acts could be undertaken without additional authorisation by individual analysts. That is all that the amendment is seeking to address. In my respectful submission, it is appropriate, necessary and proportionate.

Mr Hayes: As the hon. and learned Gentleman was speaking—he recalled having a cold towel placed upon him last week—I wondered, as his peroration ranged across so many different clauses of the Bill, whether he wished the same fate for the whole Committee, although I fully appreciate his point on the complexities of this particular area of our consideration. They are such that, to get to the basis of why he tabled the amendments, it is necessary to look across a range of parts of the Bill.

In essence, this is probably the difference between us—perhaps it is not, but let me present that at least as my hypothesis. We recognise, as the Bill reflects, that different levels of authorisation should apply in relation to different investigative techniques. I think the hon. and learned Gentleman is with us that far, but it is important to say why those different levels should apply. The differences plainly reflect the different operational contexts in which the powers are exercised, and that includes the different organisations, how they use the capabilities, and the statutory purposes for which those capabilities are utilised. We are absolutely clear that those differences are necessary, and that the safeguards that apply to different powers are satisfactory, coherent and effective.

Keir Starmer: I have checked the evidence, and perhaps the Minister can tell the Committee why it is necessary to distinguish between the protection offered to content and secondary data in relation to bulk warrants, when it is not necessary for targeted warrants. They are treated exactly the same for targeted warrants, but he says that it is necessary to distinguish between them for bulk warrants. What is the necessity? Can he spell it out, please?

Mr Hayes: I will try to do that during my response. If one recognises that a different process should apply in the exercise of different powers, contextualised around the operational function of the organisations that are exercising the powers and the purposes for which the powers are being exercised, one begins to appreciate that what might, at first reading, look like inconsistency is not an error or an inconsistency but is a necessary application of different sets of both powers and safeguards for different needs. I will address the hon. and learned Gentleman's specific point as I go through my response.

Amendment 57 would extend the requirement to obtain a targeted examination warrant to circumstances in which an agency wishes to select for examination the secondary data, as opposed to content, relating to the communications of an individual who is known to be in the UK when the data have been obtained under a bulk interception warrant. Essentially, secondary data are less intrusive than content; their collection and the circumstances in which they may be examined are directly subject to double-lock authorisation. Furthermore, it is necessary to say that it is sometimes important, indeed essential, to examine secondary data to determine whether someone is in the UK. That does not provide an entire answer to the hon. and learned Gentleman's question on the difference, but it provides some answer to the argument about where someone resides at a given point in time.

The targeted acquisition of communications data, provided for in part 3 of the Bill, including data relating to individuals in the United Kingdom, currently requires the designation of an authorised person within an organisation. The hon. and learned Gentleman acknowledged that we have taken further steps, which I will talk about later, following the recommendations of David Anderson—forgive me, but this is quite a complex area, and I need to go into it in some detail.

In contrast, bulk interception warrants, which authorise the collection of communications in bulk and set out the circumstances in which material that has been collected can be selected for examination, are subject to the double-lock authorisation of both the Secretary of State and a judicial commissioner. That means that the acquisition of content and secondary data, and the operational purposes for which any of the data can be selected for examination, is explicitly authorised by the Secretary of State and a judicial commissioner when the warrant is approved. The agencies can only select material for examination when it is necessary and proportionate to do so, in line with one or more operational purposes authorised when the warrant is granted.

Where the security and intelligence agencies wish to look at the content of the communications of an individual in the United Kingdom under a bulk interception warrant, they will need to obtain a targeted examination warrant, which reflects the recommendations from the independent reviewer, David Anderson. I draw attention to his report, "A Question of Trust," with which members of the Committee will be familiar. The report addresses precisely this point in recommendations 79 and 80 on the use of material recovered under bulk warrants. The regime reflects the well-recognised distinction between less intrusive data obtained through these powers and content—

11.25 am

The Chair adjourned the Committee without Question put (Standing Order No. 88).

Adjourned till this day at Two o'clock.