

PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

INVESTIGATORY POWERS BILL

Fifteenth Sitting

Tuesday 3 May 2016

(Afternoon)

CONTENTS

CLAUSE 212 agreed to.

SCHEDULE 8 agreed to.

CLAUSE 213 to 222 agreed to, one with an amendment.

Adjourned till this day at Seven o'clock.

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 7 May 2016

© Parliamentary Copyright House of Commons 2016

This publication may be reproduced under the terms of the Open Parliament licence, which is published at www.parliament.uk/site-information/copyright/.

The Committee consisted of the following Members:

Chairs: ALBERT OWEN, †NADINE DORRIES

† Atkins, Victoria (*Louth and Horncastle*) (Con)
 † Buckland, Robert (*Solicitor General*)
 † Burns, Sir Simon (*Chelmsford*) (Con)
 † 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)
 † 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 3 May 2016

(Afternoon)

[NADINE DORRIES *in the Chair*]

Investigatory Powers Bill

4.30 pm

The Chair: Before we begin, this sitting is officially due to finish at 5.30 pm, but we will continue until 6.30 pm, at which point there will be a break. The Committee will reconvene at 7 o'clock with Mr Owen in the Chair.

Clause 212

COMBINATION OF WARRANTS AND AUTHORISATIONS

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

Keir Starmer (Holborn and St Pancras) (Lab): The clause introduces schedule 8. I seek an assurance for the record from the Minister, but if it is not convenient to deal with this point now, it can be dealt with in some other way. Schedule 8 deals with the supplementary provisions for combined warrants. Having been through it, I think its effect is that any of the conditions necessary for any single warrant will apply notwithstanding that there is a combined warrant—in other words, none of the safeguards is lost by virtue of the combination—and the duration of the shortest warrant will apply. I am pretty sure that that is the intention, but it would be helpful to have that confirmed for the record, so that we are clear that none of the safeguards is lost when warrants are combined.

The Minister for Security (Mr John Hayes): With brevity that I know you will welcome, Ms Dorries, I can say that that is certainly so.

Question put and agreed to.

Clause 212 accordingly ordered to stand part of the Bill.

Schedule 8 agreed to.

Clause 213

PAYMENTS TOWARDS CERTAIN COMPLIANCE COSTS

Keir Starmer: I beg to move amendment 844, in clause 213, page 165, line 26, leave out subsection (6) and insert—

“(6) The appropriate contribution shall represent the full amount of the relevant costs, subject to any audit process under subsection (4)”.

This amendment would ensure that the Government meets 100% of the compliance costs and that there is full cost recovery for Communication Service Providers (CSPs) implementing the legislation.

It is a pleasure to serve under your chairmanship, Ms Dorries. The amendment speaks for itself, I think. The clause deals with payments towards certain compliance costs and subsection (1) deals with appropriate

contributions. As the Committee will know, there has been real concern about what the cost of compliance will be for those called upon to comply and what contribution they will receive toward their relevant costs. The clause allows for “an appropriate contribution”. The amendment would ensure that the Government met 100% of the compliance costs and there was full cost recovery for communication service providers implementing the legislation..

There is concern among providers about what they will be expected to do by way of compliance and what the cost will be. It may be convenient for the Minister to deal with the estimated costs, because £170 million was mentioned at one stage but I am not sure that that is a final figure as far as the Government are concerned.

Mr Hayes: The amendment is designed to ensure that the Government’s commitment to cost recovery for providers is explicitly provided for in the Bill. The hon. and learned Gentleman is right to raise this issue again, reflecting what we heard during the witness session when we debated the issue in part. In his evidence, Mark Hughes said he was aware that

“Under the proposals in the Bill—the Home Secretary has made reference to it—we would recover our costs from the Home Office, as we have done under existing legislation.”

He went on to say that

“the proposed regime is more sensible as long as it is clear that we will recover 100% of our costs.”—[*Official Report, Investigatory Powers Public Bill Committee*, 24 March 2016; c. 45-46, Q126.]

And I am clear, quoting the Home Secretary, that

“100% of the compliance costs will be met by the Government.”—[*Official Report*, 15 March 2016; Vol. 607, c. 821.]

The hon. and learned Gentleman asks what that means in practice. The £174 million he mentioned is not a cap, but an estimate. It is dealt with in the impact assessment, and there is no cap in the impact assessment. We will meet costs such as they arise. We are determined to make sure that the Bill works and is not inhibited by any doubts about the cost of its implementation. Clearly, future Governments will inherit this legislation. It is worth emphasising that the current policy has not changed since the passage of the Regulation of Investigatory Powers Act 2000, so it has survived three Governments of different colours or combinations of colours—we used to be more rainbow-like than we are now, which is actually quite welcome, by the way. We are clear that 100% means what it says.

Above and beyond that—the hon. and learned Gentleman did not ask for this, but I will add it—we need to be clear that the providers are consulted on any changes to the cost model and that they will be able to seek review of any variation to the notice that affects the level of their contribution. To sum up: we have an estimate, not a cap; a determination that 100% means 100%; a willingness to have a proper input into this; and an assurance—which I think is what the hon. and learned Gentleman really seeks—that the Government will cover the costs so that the Bill does what it should.

Christian Matheson (City of Chester) (Lab): What a great reassurance it is to see you in the Chair, Ms Dorries. I will be very brief. I welcome the contributions of my hon. and learned Friend the Member for Holborn and St Pancras and the Minister for Security. As Committee members know, I have been banging on about this issue—

Mr Hayes Yes.

Christian Matheson:—rather tediously. The Minister says, “Yes,” but I have to point out that he said it before I said “rather tediously”. I welcome the Minister’s assurance as I have been concerned about communications service provider security since Second Reading. Will the Government consider providing security advice and testing for the smaller communications service providers, in addition to the financial contribution that they are making?

Mr Hayes: I will make only two points in reply to the hon. Gentleman. First, when he describes it as “banging on”, he understates his contribution. I see it more as informed, eloquent and sensible inquiry. Secondly, he is absolutely right that the small providers need to be fully involved at all stages. It may be fair to say that the bigger providers have the mechanisms to implement the requirements for data retention more straightforwardly, so we need to ensure that that does not mean that small providers are in any way disadvantaged. I acknowledge that point, and he is right to make it elegantly. He should never apologise—at least to me—for banging on about anything.

Keir Starmer: I am grateful to the Minister for setting out that assurance for the record. That will reassure those who are concerned about this issue. In those circumstances, I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Clause 213 ordered to stand part of the Bill.

Clauses 214 and 215 ordered to stand part of the Bill.

Clause 216

NATIONAL SECURITY NOTICES

Keir Starmer: I beg to move amendment 853, in clause 216, page 166, line 36, after “State”, insert “following approval by a Judicial Commissioner”.

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

Amendment 854, in clause 216, page 166, line 41, after “State”, insert “and a Judicial Commissioner”.

Amendments 853 and 854 would require judicial authorisation for national security notices. This would also extend the “double lock” standard that is set in other parts of the Bill.

Amendment 845, in clause 217, page 167, leave out lines 20 and 21 and insert—

“(1) The Secretary of State may, following approval by a Judicial Commissioner that the notice is justified, practicable, necessary and proportionate, give a relevant operator a notice (a ‘technical capability notice’)”.

This amendment would require judicial authorisation for Clause 217 and bring the clause in line with other provisions within the bill that require judicial authorisation.

Amendment 855, in clause 217, page 167, line 20, after “State”, insert

“following approval by a Judicial Commissioner”.

This amendment would require judicial authorisation for technical capability notices. This would also extend the “double lock” standard that is set in other parts of the Bill.

Amendment 852, in clause 220, page 171, leave out lines 1 and 2 and insert—

“(9) The Secretary of State may, after considering the conclusions of the Board and the Commissioner, and with approval of a Judicial Commissioner—”

This amendment would require judicial authorisation for these clauses and bring them in line with other parts of the bill.

Amendment 859, in clause 220, page 171, line 4, at end insert—

“(9A) Any variation made under subsection (9) must be approved by a Judicial Commissioner.”

This amendment would require judicial authorisation for the variation and revocation of national security and technical capability notices. This would also extend the “double lock” standard that is set in other parts of the Bill.

Keir Starmer: The amendments go in pairs: amendments 853 and 854 are to clause 216, amendments 845 and 855 to clause 217 and amendments 852 and 859 to clause 220. They all have the same purpose and intent: to subject the powers in the clauses to the double-lock mechanism—in other words, to involve the judicial commissioners in those powers.

Clause 216 is concerned with national security notices. Subsections (1) and (2) make the power to issue such notices subject only to the test that they be

“necessary in the interests of national security”

and “proportionate”. There is no specific reference to any operational purposes; it is a very broad power. Once a notice is issued, subsection (3) takes effect:

“A national security notice may...require the operator to whom it is given—

(a) to carry out any conduct, including the provision of services or facilities, for the purpose of—

(i) facilitating anything done by an intelligence service under any enactment other than this Act, or

(ii) dealing with an emergency (within the meaning of...the Civil Contingencies Act 2004);

(b) to provide services or facilities for the purpose of assisting an intelligence service to carry out its functions more securely or more effectively.”

The Secretary of State issues a notice; once that notice is issued, the requirement on the operator is very broad. To be fair, subsection (4) makes it clear that a national security notice cannot be used to sideline or cut across a warrant or authorisation that is required under the Act, but the clause does make a very wide-ranging power available to the Secretary of State and it seems subject to pretty well no check, balance or safeguard.

The amendments would subject the procedure to the double lock mechanism, to ensure that such a notice would go before a judicial commissioner, who would consider whether it was in the interests of national security and proportionate under subsections (1) and (2). The Joint Committee raised concerns about this issue when it looked at the draft Bill, and in particular how the lack of a definition of national security means that the power granted by the clause is very wide indeed.

Joanna Cherry (Edinburgh South West) (SNP): Does the hon. and learned Gentleman agree that, in the absence of a definition of national security, it is difficult to foresee the kinds of activity or intrusion that obligations under the clause could entail? Is it not therefore providing a blank cheque power to the Government?

Keir Starmer: I agree. This is one of the rare occasions on which the Bill does not set out the procedure for what happens before the Secretary of State considers the exercise of her function. In other areas, we have seen particular requirements for what must be set out in the application and in the warrant—there is a bit more detail. Here, the notice procedure does not include any details of the formalities of the Secretary of State's consideration or what must be set out in a notice; nor does the Bill provide any safeguard through the judicial commissioners, so not having a definition of national security means that the power is extremely wide and unchecked.

My amendments go only to the process and not to the substance of clause 216, but if they were made, at least a separate pair of eyes would look at the notice and consider whether the test of necessity and proportionality was met. That in itself would be an important safeguard in keeping with the model that runs through the Bill.

4.45 pm

The Solicitor General (Robert Buckland): It is a pleasure to serve again under your chairmanship, Ms Dorries. I have listened carefully to what the hon. and learned Gentleman and others have said about their concerns regarding the provisions, but may I reassure him and put to bed the notion that somehow this is a back door or a blank cheque to allow the authorities to do what they like when it comes to interference with the privacy of individuals? Far from it. I will explain as far as I can the purpose of the type of warrant, particularly the national security notice, that we are talking about, and indeed the technical proficiency provisions as well.

An example of the type of support that might be required would be the provision of services or facilities to help the intelligence agencies in safeguarding the security of their personnel and operations. A notice might typically require a communications service provider to provide services to support secure communications by the security and intelligence agencies—for example, by arranging for a communication to travel via a particular route in order to improve security. A notice may additionally require the confidential provision of services to the security and intelligence agencies within the communications service providers, such as by maintaining a pool of trusted staff for the management and maintenance of sensitive communications services. I hope that gives the hon. and learned Gentleman some insight into what we are talking about here.

Keir Starmer: I am grateful for that indication, but I am not sure why that is an argument for not subjecting what could be a wide-ranging power to the double-lock mechanism, which has been the preferred safeguard for such powers in the Bill.

The Solicitor General: There are clear reasons for not going down that route. We are talking about the preparatory stage as opposed to the stage of interference with privacy. If the Government's position was that there was a loophole—a gateway—to allow such interference, the hon. and learned Gentleman's argument would have real strength, but that is far from the case. This is all about the preparatory stages—the necessary stages that

need to be taken by communications service providers before we get to the application for what we all accept is an intrusion.

I am afraid I cannot share with hon. Members their analysis that we need a “now and forever” definition of national security in law. There is a good reason why national security is not defined in statute. Any attempt to define it in the Bill runs a real risk of restricting the ability of this country to respond to constantly evolving and unpredictable threats. It is vital that legislation does not, however unintentionally, constrain the ability of our security and intelligence agencies to protect this country. The examples are all around us: who would have imagined a few years ago cyber-attacks of the nature and on the scale that now threaten us? My concern is that if we try to rigidly define what we mean by national security, we run the risk of defeating the means by which we can keep this country safe.

Joanna Cherry: I hear what the Solicitor General says about the measure only facilitating preparatory steps, but under the terms of clause 218(8) we will never know whether the notices exist or their contents, so we will not be able to know whether we are dealing with preparatory steps or whether they could go beyond that.

The Solicitor General: I have gone as far as I can to explain the types of scenarios that the national security notices would be used for. In essence, they deal with the nuts and bolts rather than the intrusion. If somehow there was a gateway into intrusion, the hon. and learned Lady would be absolutely right, but I assure her that there is not, so the worries that she and other people and organisations have about a blank cheque, while understandable, are unfounded. I can assure her in Committee and I am happy to continue to make the assurance that the function of this type of notice is not intrusion.

Indeed, we have oversight because national security notices will be overseen by the Investigatory Powers Commissioner. The commissioner will have a duty to report at least once a year on what he or she has found and to make recommendations on where improvements can be made. The commissioner will also have the power to report on an ad hoc basis on any issue that he or she considers appropriate.

Keir Starmer: I am listening carefully to the Solicitor General. He says that the notices are not a gateway for preparatory steps to become steps that invade privacy, but where in the Bill is the provision that prevents that happening? The only restriction is subsection (4), which does not achieve that end.

The Solicitor General: With respect, I do not think that is necessary because any agency that sought to use this type of notice in order to get around the double-lock provisions in the Bill would soon come a cropper with the commissioner. That important oversight means that organisations are not operating in a vacuum; they will be held to account if they try to misuse these notices in the way that the hon. and learned Gentleman and others fear.

As I have said, we have the powers of review by the IPC. We also have the provision, pursuant to clause 220(5)(b) and (7), that the Secretary of State must consult the commissioner if a notice is reviewed, and the commissioner

will then consider the proportionality of the matter before reporting conclusions to the Secretary of State. We have the checks and balances that the hon. and learned Gentleman rightly wants within the mechanism.

On amendments 853 and 854, I would say this: the role of the Secretary of State in issuing national security notices rightly reflects the responsibility of the Executive in protecting our national security; conversely, the role of the judicial commissioner in approving the issuing of warrants under the Bill reflects the particular and proper sensitivity regarding interference with private communications. We have got the double lock in place to ensure that, before the fact, a senior judge has to be satisfied that any interference with privacy is justified. The Bill explicitly prohibits—this is an important point—the issuing of national security notices for the primary purpose of obtaining private information, and the double lock then applies to the use of the most sensitive powers. We need to focus on the need for the double lock in relation to applications that result in the acquisition of private information. These types of notices do not permit the authorities to do that, so the amendments are unnecessary.

Amendments 845 and 855 deal with technical capability notices. Clause 217 builds on the current power provided for under the Regulation of Investigatory Powers Act 2000, where a company can be obliged to maintain a permanent interception capability in order to ensure that when a warrant is served, a company has the infrastructure in place to give effect to it securely and quickly. Again, any warrant served will have been reviewed by a judicial commissioner; he or she will play an important part in overseeing the operation of technical capability notices and any appeal that may be lodged against them. The commissioner will also be consulted about the making of regulations that will provide more detail about the operation of these types of notices, and those regulations will be put before Parliament for approval. Plenty of the checks and balances that the hon. and learned Member for Holborn and St Pancras, others interested in Bill and I would expect and want to see are here.

I am not persuaded of the need for amendments 852 and 859, because clause 220 already sets out the role of the IPC in the process of review and the actions that the Secretary of State must take in that process. The IPC will be integral to any review, because the Secretary of State must consult the commissioner, who will then consider whether the notice is proportionate. Inevitably, considerable weight will be afforded to the advice of the commissioner. The role of the commissioner provides an opportunity for the person on whom the notice has been served and for the Secretary of State to present evidence. The conclusions of the commissioner will be reported to the Secretary of State and to the person who has made the reference. After consideration of the conclusions, the Secretary of State may decide to confirm the effect of the notice, to change or vary it, or to withdraw it. Until that decision is made, there is no requirement for the person who has referred the notice to comply with the specific obligations under review.

In a nutshell, there are plenty of adequate safeguards to alleviate the concerns expressed by the hon. and learned Gentleman. I urge him to withdraw his amendments.

Keir Starmer: I listened carefully to the Solicitor General, and I am grateful to him for setting out how he envisages the notices operating. The difficulty is that there is a mismatch between what he says is their intended operation, and the safeguards in the clause. For me, subsection (4) does not do what he contends it does.

I am also concerned about clause 217. We will get on to that in more detail in a moment, but it is a wide-ranging clause on the maintenance of technical capability, which again ought to be subject to the double lock.

I apologise to the Committee, but on this occasion I will press the amendments in the group to a vote. In the past, in relation to a number of clauses, I have tested the Committee on the first one, but on this occasion I am not sure that I can do that. I think this will be the only occasion on which I will test the patience of the Committee, but clauses 216 and 217 are conceptually different and do not seem to be run as a group. I am afraid that I will press for a vote—as I say, I will not make a habit of it, and I have not done so before.

Question put, That the amendment be made.

The Committee divided: Ayes 7, Noes 9.

Division No. 122]

AYES

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

NOES

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

Question accordingly negated.

Amendment proposed: 854, in clause 216, page 166, line 41, after “State”, insert “and a Judicial Commissioner”.
—(*Keir Starmer.*)

Amendments 853 and 854 would require judicial authorisation for national security notices. This would also extend the “double lock” standard that is set in other parts of the Bill.

Question put, That the amendment be made.

The Committee divided: Ayes 7, Noes 9.

Division No. 123]

AYES

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

NOES

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

Question accordingly negated.

5 pm

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

The Committee divided: Ayes 10, Noes 2.

Division No. 124]**AYES**

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

NOES

Cherry, Joanna	Newlands, Gavin
----------------	-----------------

Question accordingly agreed to.

Clause 216 ordered to stand part of the Bill.

Clause 217**MAINTENANCE OF TECHNICAL CAPABILITY**

Amendment proposed: 845, in clause 217, page 167, leave out lines 20 and 21 and insert—

“(1) The Secretary of State may, following approval by a Judicial Commissioner that the notice is justified, practicable, necessary and proportionate, give a relevant operator a notice (a “technical capability notice”)

This amendment would require judicial authorisation for Clause 217 and bring the clause in line with other provisions within the bill that require judicial authorisation.—(Keir Starmer.)

Question put, That the amendment be made.

The Committee divided: Ayes 7, Noes 9.

Division No. 125]**AYES**

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

NOES

Atkins, Victoria	Frazer, Lucy
Buckland, Robert	Hayes, rh Mr John
Burns, rh Sir Simon	Kirby, Simon
Davies, Byron	Stephenson, Andrew
Fernandes, Suella	

Question accordingly negated.

Amendment proposed: 855, in clause 217, page 167, line 20, after “State”, insert “following approval by a Judicial Commissioner”.

This amendment would require judicial authorisation for technical capability notices. This would also extend the “double lock” standard that is set in other parts of the Bill.—(Keir Starmer.)

The Committee divided: Ayes 7, Noes 9.

Division No. 126]**AYES**

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

NOES

Atkins, Victoria	Frazer, Lucy
Buckland, Robert	Hayes, rh Mr John
Burns, rh Sir Simon	Kirby, Simon
Davies, Byron	Stephenson, Andrew
Fernandes, Suella	

Question accordingly negated.

Keir Starmer: I beg to move amendment 846, in clause 217, page 168, line 8, at end insert—

“(4A) A notice may not impose upon the relevant operator any obligations relating to the removal of electronic protection applied by or on behalf of that operator to any communications or data unless the relevant operator or a person acting on its behalf retains the technical ability to remove the electronic protection from such communications or data.”

This amendment would provide clarity and legal certainty for industry that the Government will not require back doors to be installed into products and services, is not seeking to weaken or restrict the use of encryption and that companies cannot be required to remove encryption if they do not have the means to do so at their disposal.

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

Amendment 847, in clause 217, page 168, line 16, at end insert—

“(e) persons generally held to be representing users and privacy interests in order to assess the impact of any such Regulations on users.”

This amendment would ensure that privacy protections form an overarching part of the Bill and apply across the full range of investigatory powers afforded to the security services.

Amendment 848, in clause 217, page 168, line 24, leave out subsection (8) and insert—

“(8) A technical capability notice may only be given to persons outside the United Kingdom (and may require things to be done, or not to be done, outside the United Kingdom) where it would not cause the person to act contrary to any laws or restrictions under the law of the country or territory where it is established, for the provision of services.”

This amendment would remove all provisions within the Bill that have extraterritorial reach and undermine the long term objective of creating a long term, international framework for law enforcement to gain access to data held overseas and resolves conflict of laws situations that may otherwise arise by providing the Secretary of State with the power to serve such notices without having to take account of domestic legal obligations to which the recipient is subject.

Amendment 857, in clause 217, page 168, line 30, at end insert—

“(11) A person shall not be liable to have a technical capability notice served on him in accordance with regulations under this section by reason only that he provides, or is proposing to provide, to members of the public a telecommunications service the provision of which is or, as the case may be, will be no more than—

- the means by which he provides a service which is not a telecommunications service; or
- necessarily incidental to the provision by him of a service which is not a telecommunications service.”

This amendment would exclude (under powers in RIPA section 11(4)) those services that have a communications element, but are primarily not a communication service. This limits the very broad range of “telecommunication services” that could be required to build a technical capability under this Part.

Amendment 849, in clause 218, page 168, leave out lines 37 and 38, and insert—

“(3) Before giving a relevant notice, the Secretary of State must provide evidence that the notice is justified, necessary, practicable and proportionate, having, among other matters, taken into account—”

Amendment 850, in clause 218, page 168, line 45, at end insert—

“(f) the effect on the privacy and human rights of people in the United Kingdom and outside the United Kingdom”

Amendments 848 to 850 would make explicit the requirement on the Home Secretary to justify the use of a power as intrusive as a technical capability notice. It will also require the Home Secretary to take account of the full effects of such a notice, particularly on people and companies based overseas.

Amendment 858, in clause 218, page 169, line 7, leave out—

“A technical capability notice may be given to a person outside the United Kingdom”

and insert—

“Where a technical capability notice is to be given to a person outside the United Kingdom, the notice shall be served at that person’s principal office outside the United Kingdom where it is established, for the provision of services. Where it is considered unfeasible or inappropriate in the circumstances”

This amendment would require that a UK agency would only serve a notice on an overseas entity that is capable of providing assistance under the warrant.

Keir Starmer: This important clause is causing a great deal of concern to operators that may be called upon to comply with a notice. The clause provides for a power to be vested in the Secretary of State to give a relevant operator a technical capability notice

“imposing on the relevant operator any applicable obligations specified in the notice,”

and

“requiring the person to take all the steps specified in the notice for the purpose of complying with those obligations”.

That is a very wide power, and the concern is about the extent of it. In a moment, I will refer to the code of practice, which sets out some of the capabilities that might be required.

It is clear that the power includes taking steps relating to encryption. I say that for two reasons. Subsection (4) lists in paragraphs (a) to (e) the obligations that may be specified in regulations. They include obligations

“to provide facilities or services of a specified description”

and obligations relating to

“apparatus owned or operated by a relevant operator”

or to

“the removal by a relevant operator of electronic protection applied by or on behalf of that operator to any communications or data”.

That is clearly veering into encryption. Obligations may also relate to

“the security of any postal or telecommunications services provided by a relevant operator”

or

“the handling or disclosure of any information.”

If one reads ahead, clause 218(4) deals with further provisions on notices under clauses 216 and 217, stating:

“Where the relevant notice would impose any obligations relating to the removal by a person of electronic protection applied by or on behalf of that person to any communications or data, in complying with subsection (3) the Secretary of State must in particular take into account the technical feasibility, and likely cost, of complying with those obligations.”

The concern of many who might be called upon to comply with the obligations is about the wide-ranging nature of the power.

This also goes deep into the debate about encryption. It is absolutely clear that a notice could require protection to be removed, and the clause envisages that being the case. That becomes clearer when one reads the “Interception of Communications” draft code of practice from chapter 8 onwards. If one reads paragraphs 8.1 to 8.94, one sees what is in fact a power that allows the Secretary of State, through this mechanism, effectively to take control of a capability of a service provider. Paragraph 8.1 states:

“The purpose of maintaining a technical capability is to ensure that, when a warrant is served, companies can give effect to it securely and quickly. Small companies (with under 10,000 users) will not be obligated to provide a permanent technical capability”.

Paragraph 8.3 then lists the wide range of obligations that can be imposed in a notice under this clause.

Paragraph 8.4 of the draft code states:

“An obligation placed on a CSP to remove encryption only relates to electronic protections that the company has itself applied to the intercepted communications (and secondary data), or where those protections have been placed on behalf of that CSP, and not to encryption applied by any other party.”

That is very important provision, which I think I am right to say was clarified as a result of a recommendation from prelegislative scrutiny. The difficulty—I am anticipating the discussion we are about to have—is that this crucial issue is dealt with in the code of practice and not in the Bill. The concern expressed in the evidence given to the various prelegislative bodies and to the Committee was that companies will be obliged to remove the protections in their own systems. Paragraph 8.4 is of some comfort to them because it makes it clear that the obligation would only relate

“to electronic protections that the company has itself applied”

and not to other encryption—but the real problem is that paragraph 8.4 is in the code of practice and not in the Bill. That needs to be rectified. We cannot leave something as important as that in the code of practice. It goes to the heart of the power in the clause. It is far and away the biggest cause for concern among CSPs, yet it is not dealt with in the Bill. The Bill provides for a permissive, rather than a restrictive, regime—if I am wrong about that, I will happily take an intervention.

Paragraph 8.6 of the code of practice clarifies that:

“While an obligation to remove encryption may only relate to protections applied by or on behalf of the company...there will also be circumstances where a CSP removes encryption from communications for their own business reasons. Where this is the case, an intercepting agency will also require the CSP, where applicable and when served with a warrant, to provide those communications in an intelligible form.”

The code then makes provision for giving a notice, for the disclosure of technical capability notices, and for their review and variation. Paragraph 8.27 and 8.28 are very wide-ranging. Paragraph 8.28 states:

“CSPs subject to a technical capability notice must notify the Government of new products and services in advance of their launch, in order to allow consideration of whether it is necessary and proportionate to require the CSP to provide a technical capability on the new service.”

That goes deep into territory hitherto unregulated in this way; CSPs will be required to give the Government notice of their new products and services, so that the Government can consider whether to vary a notice that already applies to them. We can see why the service providers are so concerned about that capability.

[Keir Starmer]

Pressing on through the code of practice, we see that the contribution of costs for the maintenance of a technical capability is dealt with from paragraph 8.43. Again, these provisions give an indication of the breadth of the capability covered by the clauses of the Bill. Paragraph 8.43 states:

“Section 213 of the Act recognises that CSPs incur expenses in complying with requirements in the Act, including notices to maintain permanent interception capabilities under Part 9. The Act, therefore, allows for appropriate payments to be made to them to cover these costs.”

In a sense, the requirement for CSPs to give notice when they have new or different services and to maintain permanent interception capabilities when they would not otherwise do so means the taking control of their services for the purposes of the Act.

5.15 pm

The code of practice continues, at paragraph 8.46:

“Costs that may be recovered could include those related to the procurement or design of systems required to intercept communications, their testing, implementation, continued operation and, where appropriate, sanitisation and decommissioning.”

That, again, is an indication of just how wide these powers will be. Paragraphs 8.51 to 8.53 deal with the power to develop compliance systems, suggesting that,

“In certain circumstances it may be more economical for products to be developed centrally, rather than CSPs or public authorities creating multiple different systems”

and stating that clause 214 provides the Secretary of State with that power. Paragraph 8.53 is the inevitable conclusion of that, stating:

“Where such systems are developed for use by CSPs, the Government will work closely with CSPs to ensure the systems can be properly integrated into their networks”,

which is the option of ensuring that the CSP itself develops and maintains the capability. If not, the Secretary of State can do so and then there will inevitably be a requirement to integrate that capability into existing networks, and so on and so forth. That is why, although the detail of paragraphs 8.1 to 8.94 is welcome, it is the clearest evidence one could get of the breadth of the powers.

Amendment 846 would

“provide clarity and legal certainty for industry that the Government will not require back doors to be installed into products and services, is not seeking to weaken or restrict the use of encryption and that companies cannot be required to remove encryption if they do not have the means to do so at their disposal.”

The amendment is intended to deal with the concern of service providers about how the clause would apply to encryption. Amendment 847 would add a requirement to take into account privacy interests. I will not press that amendment to a vote and I will not spend time on it now, because to some extent it is probably overtaken by the overarching privacy provisions, which we will deal with later in a new clause.

Amendment 848 is self-explanatory. There is a continuing concern among service providers about obligations being imposed on them that would put them in breach of the law, or a restriction under the law, in the country or territory in which they are operating. The intention behind the amendment is to remove that conflict by ensuring that no obligation under clause 217 would

“cause the person to act contrary to any laws or restrictions under the law of the country or territory where it is established, for the provision of services.”

Amendment 857 would deal with a sub-clause of service providers by excluding

“those services that have a communications element, but are primarily not a communication service. This limits the very broad range of ‘telecommunication services’ that could be required to build a technical capability under this Part.”

Amendment 849 is probably the most significant of this group of amendments, as it would insert a new requirement into clause 218:

“Before giving a relevant notice, the Secretary of State must provide evidence that the notice is justified, necessary practicable and proportionate”.

It then lists what must be taken into account. I pause there because it is significant that clause 217 is not subject to a necessity and proportionality test. It is subject to a reasonableness test. Clause 217(3) shows that there is no need for the Secretary of State to show necessity or proportionality.

Interestingly, when it comes to variation in clause 219(4), as far as the national security notice is concerned, there is a requirement to demonstrate proportionality. The amendment would build in a new test to be applied under clause 217. Finally, amendment 858 is our old friend “service outside the jurisdiction”, which I have rehearsed already.

Joanna Cherry: I respectfully support everything that the hon. and learned Gentleman has said.

The Solicitor General: In arguing in opposition to the amendments, I first want to address the last point that the hon. and learned Member for Holborn and St Pancras made. I can come back to his point about the tests, but in a nutshell, they are inherent to the Bill. The tests of necessity and proportionality are part and parcel of the decision-making process that the authority will be enjoined to carry out.

Keir Starmer: It is noticeable that, for obvious reasons, necessity and proportionality have been written into relevant clauses throughout the Bill, but here, I think for the first time, we have a wide-ranging power with no such test—unless I have missed it, in which case I will happily concede the point.

The Solicitor General: In strict terms, the hon. and learned Gentleman is right—I am looking at clause 218 in particular. I think that subsection (3) might help him, because although we do not have the words “necessity” and “proportionality” there, the matters to be taken into account lead one to conclusions based on necessity and proportionality, and perhaps do so in a more prescribed way that is more helpful to the decision maker. Subsection (3)(a) to (e) addresses the hon. and learned Gentleman’s point, and I put it clearly on the record that the principles of necessity and proportionality are part and parcel of the tests to be applied.

I also note that necessity is required under clause 217(6), which relates to the steps specified in a technical capability notice. I do not know whether that helps the hon. and learned Gentleman. I will certainly consider the issue carefully, but on the face of it, I do not think there is a worry of the sort that he envisages.

Joanna Cherry: The Intelligence and Security Committee described the clause as a “seemingly open-ended and unconstrained power”.

Does the Solicitor General not agree that it is therefore essential that the tests of necessity and proportionality are spelled out in the clause, as they are in other parts of the Bill?

The Solicitor General: I hear the hon. and learned Lady, but I am not convinced that the basis of her argument is right given the breadth of the power. As I said in the context of national security notices, the technical capability notice is only a preliminary step. It will allow the subsequent implementation of warrant, which will then be subject to the tests of necessity and proportionality. I would not want the Committee to operate under a misapprehension. It is my strong, and I hope clear, assertion that we are dealing with an earlier stage of the process, so we should not be driven to the conclusions that I know critics of the Bill want us to reach.

May I deal with encryption, which, as the hon. and learned Gentleman rightly characterised, is at the heart of the matter? I put it on the record that the Government recognise the vital importance of encryption. It has become part of our daily lives. It keeps our personal data and intellectual property secure and ensures safe online commerce, and the Government work closely with industry and business to improve their cyber-security. I can reassure the Committee that in the preparation of the code of practice, there has been close consultation with the interested parties in the industry to ensure that it comprehensively reflects the realities and needs of those who operate in this sphere. Not only does the code of practice replicate the provisions of RIPA, but it goes further, with a degree of specificity that is not possible in primary legislation. It will be a flexible, living instrument that will form a clear prospectus within which everyone can work. I make no apology for the measure being in a code practice, which is where it should be, rather than in primary legislation. With the best will in the world, we all know that it is difficult to amend primary legislation and ensure that it keeps pace with the somewhat breathtaking changes that occur in this particular field of operation.

I also want to talk about the role of GCHQ, which plays a vital information assurance role and provides advice and guidance to allow the Government, industry and the general public to protect their IT systems and use the internet safely. As the director of GCHQ, Robert Hannigan, made clear in his speech on 8 March:

“I am accountable to our Prime Minister just as much, if not more, for the state of cyber security in the UK as I am for intelligence collection.”

In the past two years the security and intelligence agencies have disclosed vulnerabilities in every major mobile and desktop platform, including some of the big names that underpin business here in the UK. In September 2015, Apple publicly credited CESG, the information assurance arm of GCHQ, with detecting a vulnerability in its operating system for iPhones and iPads, and we all know where that vulnerability could have led. The vulnerability was fixed as a result of that intervention, so the suggestion, which I know has not been advanced in this Committee—and I hope will not be—that the Government are opposed to encryption, or would legislate to undermine it, is wholly wrong.

We have to ensure that we have the necessary capabilities to keep our systems safe. Encryption is now, in effect, the default setting for most of our IT products and online services, and although it can be a power for good in keeping the law-abiding safe and secure, sadly it is used easily and all too cheaply by terrorists, paedophiles and other criminals. Therefore it can only be right that we retain the ability to require telecommunications operators to remove encryption in strictly limited circumstances, with strong controls and safeguards, so that we can address the increasing technical sophistication of those who would seek to do us harm. If we do not do that, we must simply accept that there are areas online that are beyond the reach of the law, where criminals can go about their business unimpeded and without the risk of detection. I do not accept that, and I know the general public do not accept it either. That is our starting principle.

Joanna Cherry: Clause 218(8) and (9) provides that the recipient of a notice must comply with it but must not disclose either its existence or its contents. Does that mean that if an Apple against the FBI scenario were to occur in the UK, Apple would not be able to disclose even the fact that it had been served with a notice, let alone challenge it in court? That is how I read it.

The Solicitor General: Not without the permission of the Secretary of State. I will return to the mechanism in question, but I am grateful to the hon. and learned Lady for raising that point. I am sure I will be able to provide her with clarity as I develop my remarks.

The starting principle is shared by David Anderson, who in his important review said:

“My first principle is that no-go areas for law enforcement should be minimised as far as possible, whether in the physical or the digital world.”

That view was shared by the Joint Committee on the draft Bill and is shared by the Select Committee on Science and Technology, both of which recognise that, in tightly prescribed circumstances, it should remain possible for our law enforcement and security and intelligence agencies to be able to access decrypted communications or data. That is what clauses 217 and 218 are all about: strong safeguards to ensure that obligations to remove encryption can be imposed only in limited circumstances, subject to rigorous controls.

5.30 pm

Clause 217 relates to technical capability notices. Before such a notice is given, the Secretary of State must specifically consider the technical feasibility and likely cost of complying with it. Clause 218(4), which has been the subject of some debate, provides that that consideration must explicitly take into account any obligations to remove encryption applied by, or on behalf of, a communications service provider. In my submission, that deals with the point about third parties that the hon. and learned Member for Holborn and St Pancras raised.

Keir Starmer: I looked carefully at that subsection, but perhaps the Minister could explain why it is a limiting provision. It is a requirement provision as far as the notice is concerned, but on the face of it, encryption

[Keir Starmer]

is not limited to protection applied by, or on behalf of, the person themselves. It tells us how that situation would be dealt with, but it is not limited to that.

The Solicitor General: I have been interested in the clause for a while, because there are issues about what “relevant notice” means, for example. I assure the hon. and learned Gentleman that that applies only to technical capability notices, not national security notices. I will carefully consider how we can make that absolutely clear, and in that context I will have another look at the how the clause is worded. I want to put beyond any doubt the fact that the clause relates only to a technical capability notice and does not relate to third parties. That has been an important undertaking that we have given.

Mr Hayes: Deliberating on the interesting discourse that has taken place between the Solicitor General and the hon. and learned Member for Holborn and St Pancras, I take the point that the hon. and learned Gentleman makes about necessity and proportionality running as a theme throughout the Bill. My hon. and learned Friend the Solicitor General is of course right that these are preliminary measures, and therefore once an outcome that has been tested for proportionality has been reached, that will not be a problem. I say to him that there is an argument for taking that into account and making it even clearer, either in the supporting documentation or in the Bill.

The Solicitor General: I am grateful to my right hon. Friend, and I will do that.

Before I go further, I will deal with the point that the hon. and learned Member for Edinburgh South West made about Apple. My understanding is that the process will give her some reassurance. In that scenario, Apple, as the recipient of the notice, could refer it back to the Secretary of State, who in turn must then consult the technical advisory board and the IPC before deciding whether to proceed further with the notice. If the Secretary of State proceeded, it would then be judicable in the courts, which would determine whether the notice could be enforced. It is quite similar to the scenario that we discussed in the context of national security notices. I hope that gives her some assistance.

Keir Starmer: I have looked at this issue in the past day or two, and I was concerned about the implication that on the face of it, one could not challenge the provision in court, because there is an absolute bar on disclosure. Am I right in assuming—if I am, it should be on the record—that the Secretary of State will give permission, where appropriate, for a legal challenge to be brought? In other words, there could be disclosure for the purposes of legal proceedings.

The Solicitor General: On the face of it, that has to follow. If any clarification is needed on that, I am sure I can assist as I further develop my remarks.

I was dealing with the process of consultation before the giving of a notice, and we have had the Apple

example. I would like to develop the importance of the draft codes of practice, which the hon. and learned Gentleman has referred to.

Suella Fernandes (Fareham) (Con): The Solicitor General is talking about the power of review in clause 220, which should be read with the power to issue notices. That is important because it obliges the Secretary of State to consult the technical advisory board and the Investigatory Powers Commissioner. That process was endorsed by EE, a communications service provider, in its evidence to the Joint Committee on this very point.

The Solicitor General: I am grateful to my hon. Friend, who provides an example of the sort of dialogue that will be very much part of the process. There will not be mere diktat without further discussion. I was about to develop that point in the context of the draft codes of practice, because they make it clear that should a telecoms operator have concerns about the reasonableness, cost or technical feasibility of any requirements set out in a notice, which of course would include any obligations to remove encryption, they should be raised during the consultation process. That is the dialogue that we have talked about. Also, a telecommunications operator that is given a technical capability notice may refer any aspect of it—again, I gave an example earlier—including obligations relating to removal of encryption, back to the Secretary of State for review. We have dealt with the consultation process set out in the Bill.

The Bill makes it absolutely clear that in line with current practice, obligations placed on telecommunications operators to remove encryption may relate only to encryption by or on behalf of the Government. That is the point I was making about subsection (4).

Lucy Frazer (South East Cambridgeshire) (Con): I wonder whether clause 217(3) is relevant in the context of what we are discussing. It shows that the Secretary of State can impose the requirements only in so far as they are practicable. The Secretary of State will be prevented from requiring a service provider to do something that it cannot do, for example because a third party has encrypted the material and it is not physically capable of assisting.

The Solicitor General: I am grateful to my hon. and learned Friend, who is right to pray in aid that subsection, which sets out the bones on which we flesh out the procedure in the code of practice.

Christian Matheson: I am getting a bit confused. My understanding was that these provisions applied only to communications service providers. I think it was the hon. and learned Member for Edinburgh South West who raised the question of Apple, which to my mind is not a communications service provider, but the Minister responded in the same terms. Will he clarify who exactly we are talking about and who the provision is intended to cover?

The Solicitor General: The hon. Gentleman is right to make that important point and to steer us back on to the straight and narrow. I am not criticising the Committee for trying to bring the Bill to life with some examples.

We are indeed talking about communications service providers, not third parties, which is important in the context of the Bill.

Joanna Cherry: Are we not concerned here with the “relevant operator”, which is defined in clause 217(2) as “a postal operator... a telecommunications operator, or... a person who is proposing to become a postal operator or a telecommunications operator.”?

That definition is the basis of the concern for companies such as Apple.

The Solicitor General: The hon. and learned Lady is absolutely right to bring us back to clause 217(2). The problem that hon. Members are anticipating is that the provisions will somehow catch parties that no one would regard as appropriate. I think I have given clear assurances on that third party problem.

Sir Simon Burns (Chelmsford) (Con): I am very grateful to my hon. and learned Friend, and I do not want to be unhelpful, but I would like some clarification regarding Apple. As he is aware, Apple refused to do what the FBI asked. Although the case was never ultimately determined by the courts, because the FBI managed somehow to break open the machine and retrieve the information, how would the clause affect a similar situation if a provider such as Apple refused point-blank to co-operate, just as it did with the FBI?

The Solicitor General: In endeavouring to answer my right hon. Friend’s point, may I deal first with the question about telecommunications operators? Some assistance may be gained from clause 223(10), where a telecommunications operator is defined in a way that includes Apple. The famous Apple case—the California case—was about the use of a password, which is slightly different from the question of encryption, but it does demonstrate the important tussle between the need to balance public safety and privacy. In that case, the FBI, with an appropriate search warrant, was asking for the chance to try to guess the terrorist’s passcode without the phone essentially self-destructing—after so many tries, everything gets wiped.

We are talking about an attempt to obtain communications data within the robust legal framework that we have set out, with the double lock and all the other mechanisms that my right hon. Friend and the Committee are familiar with. I am grateful to him for raising that case, but there are important differences that it would be wrong to ignore. In a nutshell, without the powers contained in the Bill, a whole swathe of criminal communication would be removed from the reach of the authorities. That is not in the interests of the constituents he has served with distinction for well over a quarter of a century—he will forgive me for saying that—or any other of the constituents we represent.

I was going to come back to the obligations imposed under a technical capability notice, with particular regard to the removal of encryption. The obligations imposed under such a notice will require the relevant operator to maintain the capability to remove encryption when it is later served with a warrant notice or authorisation. That is different from merely requiring it to remove

encryption. In other words, it must maintain the capability, but there then needs to be the next stage, which is the warrant application and the notice of authorisation, where there is of course the double lock. The company on which the warrant is served will not be required to take any steps, such as to remove encryption, that are not reasonably practicable.

In a nutshell, this measure is about not an interference with privacy but sets out the preparatory stage before a warrant can be applied for. The safeguards provide the strict controls that I assure the Committee are needed in this sphere of activity. We are maintaining and clarifying the existing legal position.

Joanna Cherry: I am anxious to clarify what the Solicitor General said about the justiciability of the issuing of such a technical notice. As far as I can see, the Secretary of State is the gatekeeper to justiciability, because the contents of a notice can be revealed only with his or her permission. Where does it say that that can be justiciable, because I cannot find it?

The Solicitor General: I think it is clause 220, but I will get some further assistance on that point for the hon. and learned Lady before I resume my seat. I am grateful for that intervention.

The Bill does not drive a coach and horses through encryption. It does not ban it or do anything to limit its use. A national security notice—we debated this matter on clause 216—cannot require the removal of encryption, which further supports my argument that there is no blank cheque in the context of these notices. On the issue of civility, rather than keep this Committee waiting, I will write to the hon. and learned Lady to clarify the point that she rightly raised.

5.45 pm

Victoria Atkins (Louth and Horncastle) (Con): This is a general point. Although we are examining this Bill in detail, there will of course be an ongoing debate, particularly as the technical companies tussle with the public, about what the public find acceptable. Those companies should not think that the debate ends here; they will have to justify their actions to the public in future.

The Solicitor General: My hon. Friend is absolutely right. The code of practice has been drafted in that real-life context. It will no doubt be amended and looked at—it will be a living document—as this technology develops and as we move forward. With this clause, we are trying—I do not like this phrase, but I have to use it—to future-proof the legislation to make it resilient so that it lasts and to ensure that this House does not have to return to it time and again to respond to the challenges that increased and enhanced IT present.

Lucy Frazer: My hon. and learned Friend referred to clause 220, which indeed does give the person who receives the notice the power to give it back to the Secretary of State, who then has to consult the Technical Advisory Board and the Investigatory Powers Commissioner, who will then take evidence from those people.

The Solicitor General: I am glad that my hon. and learned Friend has reminded us of that. I referred earlier to that consultation process. The next stage is when the Secretary of State decides to proceed. I will consider that issue even more carefully to ensure that the Committee is furnished with as much information as possible before Report.

Let me deal with the amendments tabled in the name of the hon. and learned Member for Holborn and St Pancras and others. On amendment 846, the Bill already makes it absolutely clear that a communications service provider will not be obligated to remove encryption where it is not reasonably practicable for them to do so. I do not think the amendment adds anything, and in many cases it would have the effect of inhibiting law enforcement agencies and the security and intelligence services from working constructively with telecommunications operators as the technology develops. I am sure that that is not the intention of the amendment. Depending on the individual company and the individual circumstances, it may be entirely sensible for the Government to work with a company to determine whether it would be reasonably practicable for it to take steps to develop and maintain the technical capability to remove the encryption it has applied to communications or data.

My worry about the amendment is that we would end up with communications services that can be used by criminals and others to communicate with each other unimpeded. We know that internet gambling sites, which have chat room provisions, are used by criminals for entirely unrelated criminal activities. I am sure that that is not the intention behind the amendment. Therefore, with respect, I urge hon. Members to reconsider it.

I will not deal in detail with amendment 847, because I do not think the hon. and learned Gentleman seeks to press it. Although I oppose it, I will move on without argument to amendments 848 and 858. We have discussed similar amendments on extraterritoriality in relation to other powers in the Bill. I pray in aid the arguments I used earlier. The provisions in the Bill allow a notice to be given in the most appropriate manner, taking into account the preferences of each company, which is an example of the adaptability of the legislation to the real world.

Amendment 848 is unnecessary because the clause is about not the acquisition but the development and maintenance of a technical capability. Conflict of law issues are much more likely to arise in respect of giving effect to a warrant, and we already have protection in the Bill for such cases. Admirable though the amendment may seem, it is therefore unnecessary.

Amendment 849 is unnecessary because it duplicates provisions in clauses 218, 216 and 217. I have discussed clause 218(3), which stipulates that the Secretary of State must consider a wide range of matters before giving a notice. That detailed assessment already speaks to the issues raised by the amendment. The Secretary of State has to be satisfied that the conduct is proportionate, justified, necessary and practicable.

Joanna Cherry: I am sorry to interrupt the Solicitor General's flow, but I sense he is coming to the end of his argument. Will he clarify something? Am I right in understanding that there is nothing in the clause to

prevent someone who is intent on evading surveillance from using open-source encryption software that is personally generated by the user? That would mean they could encrypt files and email communications themselves, independent of any provider, and therefore remain untouched by this legislation.

The Solicitor General: That question is about the definition of the provider. I am sure we will be able to provide some clarity on that before I draw my remarks to a conclusion. I am grateful to the hon. and learned Lady for raising that point.

Amendment 850 relates to consideration by the Secretary of State of the effect of a notice on the privacy and human rights of people both here and outside the kingdom. The amendment is unnecessary because of the point I made before, which I will reiterate: the clause is not about notices authorising an interference with privacy. A warrant provided for elsewhere in the Bill is required to do that, and we have already considered the potency of the double lock and the test to be applied. A point that is relevant to all the amendments in this group is the statutory function of the Investigatory Powers Commissioner to oversee the use of notices. I raised that in the context of national security notices, and I pray it in aid here again.

Amendment 857 seeks to narrow the category of operators to whom a technical capability notice can be given. I am worried that that would limit the effects of law enforcement. We know about the diversification of criminality and terrorism in order to find new ways to avoid protection. I am concerned that narrowing the legislation would allow loopholes to get larger. It is therefore important that the obligations relating to the technical capabilities for a range of operators can be imposed by the Government in order to ensure we keep ahead of the curve.

The hon. and learned Lady made the powerful point that the clause does not relate to personally applied encryption. However, measures in part 3 of RIPA 2000 provide for where law enforcement agencies can require an individual to remove encryption that he or she has applied themselves. We know that the Bill generally does not cover all the agencies' powers. This is perhaps a welcome opportunity to remind ourselves of the existing provisions in part 3, so I am grateful to her.

Of course we accept that it may well be appropriate to exclude certain categories of operator from obligations under the clause—I am thinking, for example, of small businesses; we are always mindful of the burden of regulation on small businesses—but it is our intention to use secondary legislation to achieve that. It would not be appropriate in primary legislation to impose blanket exemptions on services with a communications element that are not primarily communications services. To do so would send a rather alarming and clear message to terrorists and criminals that communications over certain systems will not be monitored. That sort of carve-out recalls the point that I made about the use by criminals of seemingly unrelated or innocuous communications channels in other internet facilities or apps, in order to hide their illicit enterprises.

I know that I have taken up an inordinate amount of the Committee's time. I am obliged to the Committee and to you, Ms Dorries, for your indulgence. I hope that

I have set out the reasons why I urge hon. Members to withdraw the amendment, and I pray in aid my arguments as advancing the case that the clause should stand part of the Bill. I urge the hon. and learned Gentleman to withdraw the amendment.

Keir Starmer: I have only three issues to address. The first, which requires more attention from the Solicitor General—I say so with no disrespect—is the question of the extent of the prohibition on disclosure and, essentially, access to the courts or appropriate tribunals. On the face of it, clause 218(8) is a prohibition on disclosure, save with the permission of the Secretary of State. With respect to Committee members, I do not think that clause 220 provides the answer, because that deals with the consultation exercise where a notice is being reviewed.

I have no doubt that, if the Secretary of State exercised her power under clause 218(8) to prevent access to the courts, it would run straight into an article 6 access to courts argument that would succeed on judicial review. I had assumed that one could read into the clause by implication that permission would not be refused in a bona fide and proper case where access to court—or the relevant tribunal, which may be a better way of putting it—was an issue. If that were made clear for the record or by some redrafting of the clause, it would help. As I said, I think that, in practice, any court in this jurisdiction would strike down pretty quickly a Secretary of State who sought to prevent access to the court.

The Solicitor General: I think that the hon. and learned Gentleman is right about that. On that basis, I will have another look at clause 218(8), to get it absolutely right. I reassure him that it is not the Government's intention to preclude access to the court.

Keir Starmer: I am reassured. I am sure that that would not be the case, but it might be sensible to clarify that rather than relying on clause 220, because I am not sure that that is the right way to do it. However, I will say no more about that.

I was going to press for votes on amendments 846 and 849, but I have listened carefully to what the Solicitor General said and to what the Minister said when he rose to make some observations earlier. They are by far the two most important amendments. Amendment 846 deals with encryption. I think I heard the Solicitor General say that he will look again at the wording of clause 218(4) to see whether it is possible to make clear what is clear in the code of practice, namely, that an obligation placed on a CSP to remove encryption relates only to electronic protections that the company itself has applied to intercepted communications and secondary data. That is clearly the position that the Government adopt, because it is now set out in the code. I think that the Solicitor General might accept that, at the moment, clause 218(4) does not quite achieve that objective. On the basis that he is prepared at least to look at that again, I will not press amendment 846.

6 pm

Equally, amendment 849 relates to the test. I listened carefully to what the Minister said. It would be more sensible if the clauses were aligned with the other provisions

in the Bill and made clear the necessity and proportionality test. The Minister's intervention appeared to make clear what the expectation would be in any event; he made it clear that at least some consideration would be given to whether that expectation can be reflected in some way that is not apparent in the Bill. The observations made by the Solicitor General and the Minister persuaded me not to press the amendments to a vote, so I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

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

Joanna Cherry: The Scottish National party is not happy with this clause without amendment. I was going to press it to a vote, but having heard what the Solicitor General said about the clause, and pending his writing to me, I am willing not to press it. I just lay down a marker in that respect.

Question put and agreed to.

Clause 217 accordingly ordered to stand part of the Bill.

Clause 218

FURTHER PROVISION ABOUT NOTICES UNDER SECTION
216 OR 217

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

Joanna Cherry: The SNP takes the same position as it did on the previous clause.

Question put and agreed to.

Clause 218 accordingly ordered to stand part of the Bill.

Clause 219

VARIATION AND REVOCATION OF NOTICES

Mr Hayes: I beg to move amendment 734, in clause 219, page 170, line 8, at end insert

“(and in the application of section 218(3) and (4) in relation to varying a relevant notice, references to the notice are to be read as references to the notice as varied).”

This is a technical amendment. Ms Dorries, I should have welcomed you to the Chair earlier, but I do so now. The amendment is uncontentious and makes a drafting correction to clause 219. On that basis, it should not cause the Committee any undue concern, and I move it in that spirit.

Amendment 734 agreed to.

Clause 219, as amended, ordered to stand part of the Bill.

Clause 220

REVIEW BY THE SECRETARY OF STATE

Keir Starmer: I beg to move amendment 851, in clause 220, page 170, line 31, leave out subsection (6) and insert—

“(6) The Board must consider the technical requirements and the consequences, for the person who has made the reference and for others likely to be affected, of the notice so far as referred.”
This amendment would require the Technical Advisory Board to look at more than just an implementation of cost measure and instead examine the full costs of the notice.

[Keir Starmer]

Our discussions have already strayed on to clause 220. This short amendment is reasonably clear. Subsection (6) makes it clear that the technical advisory board, referred to in subsection (5)(a),

“must consider the technical requirements and the financial consequences, for the person who has made the reference, of the notice so far as referred.”

That is where the person served with the notice has referred the notice back to the Secretary of State, which then triggers a consultation exercise. The board must be consulted; subsection (6) sets out what the board must consider. The amendment is fairly self-explanatory; it would serve the limited purpose of requiring the technical advisory board to look at more than just the implementation of cost measure, and instead examine the full costs of the notice.

Mr Hayes: As the hon. and learned Gentleman said, the amendment would broaden the scope of the technical advisory board by requiring it to consider other matters as part of any review of the obligations imposed by the Secretary of State in a notice. Under the amendment, the board would be required to consider the consequences for others likely to be affected by the obligations imposed by a notice. That is understandable—I can see why the hon. and learned Gentleman tabled the amendment—but unnecessary.

The technical advisory board is essentially a committee of experts. It has a very specific role to play in advising the Secretary of State on cost and technical matters. That role is reflected in its membership: a group of experts drawn from communications service providers and from those entitled to apply for warrants and authorisations under the Bill. Such people are well placed to consider the technical requirements and the financial consequences. If they consider it appropriate, they may look beyond cost and technical feasibility, but those matters, rightly, are the board’s central purpose and are at the core of its work. The board is also required to consider evidence or representations made by communications service providers and must report its conclusions to them and to the Secretary of State.

In my view, responsibility for considering the broader effects of the notice on the communications service provider to whom it has been given should sit with the Investigatory Powers Commissioner. While it is absolutely right that the board considers both the technical aspects and the cost, the broader matters that the hon. and learned Gentleman is rightly concerned about should fall within the scope of the commissioner, as they do in the Bill. As part of any review of the obligations set out in the notice, the commissioner must report on the proportionality of those obligations; that will include an assessment of the consequences of the notice, both on the persons seeking the review and on anyone else affected—which is essentially the argument the hon. and learned Gentleman made for the amendment.

Furthermore, the clause requires the commissioner to seek out the views of the person who has received the notice, who will have the opportunity to raise any concerns about the effect of the notice with the commissioner for consideration; the commissioner must report his or her conclusions to that person and to the

Secretary of State. Essentially, combining the role and responsibilities of the board with the role and responsibilities of the commissioner means that each of them will provide a function central to the hon. and learned Gentleman’s concerns, so the amendment is unnecessary. I should add that the commissioner is properly and well placed to consider the proportionality of the matter as a whole, after careful assessment. The amendment’s wording would introduce duplication and, frankly, a degree of ambiguity about the respective roles of the board and the commissioner and about what each of them is considering. With that reassurance, I hope the hon. and learned Gentleman will withdraw the amendment.

Keir Starmer: The Minister says that the Bill places no inhibition on the wider technical consequences looked at by the board, and that other consequences rightly come under the remit of the commissioner. I am grateful for that clarification; I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Amendment proposed: 852, in clause 220, page 171, leave out lines 1 and 2 and insert—

“(9) The Secretary of State may, after considering the conclusions of the Board and the Commissioner, and with approval of a Judicial Commissioner—”.—(Keir Starmer.)

This amendment would require judicial authorisation for these clauses and bring them in line with other parts of the bill.

Question put, That the amendment be made.

The Committee divided: Ayes 7, Noes 10.

Division No. 127]

AYES

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

NOES

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

Question accordingly negated.

Amendment proposed: 859, in clause 220, page 171, line 4, at end insert—

“(9A) Any variation made under subsection (9) must be approved by a Judicial Commissioner.”—(Keir Starmer.)

This amendment would require judicial authorisation for the variation and revocation of national security and technical capability notices. This would also extend the “double lock” standard that is set in other parts of the Bill.

Question put, That the amendment be made.

The Committee divided: Ayes 7, Noes 10.

Division No. 128]

AYES

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

NOES

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

Question accordingly negated.

Clauses 220 and 221 ordered to stand part of the Bill.

Clause 222

REVIEW OF OPERATION OF ACT

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

The Chair: With this it will be convenient to consider new clause 23—*Review of the Operation of this Act*—

“(1) The Secretary of State shall appoint an Independent Reviewer to prepare the first report on the operation of this Act within a period of six months beginning with the end of the initial period.

(2) In subsection (1) “the initial period” is the period of four years and six months beginning with the day on which this Act is passed.

(3) Subsequent reports will be prepared every five years after the first report in subsection (1).

(4) Any report prepared by the Independent Reviewer must be laid before Parliament by the Secretary of State as soon as the Secretary of State is satisfied it will not prejudice any criminal proceedings.

(5) The Secretary of State may, out of money provided by Parliament, pay a person appointed under subsection (1), both his expenses and also such allowances as the Secretary of State determines.”

I inform the Committee that I consider clause 222 and new clause 23 to be alternatives. If the Committee decides that clause 222 should stand part of the Bill, I will not put the Question on new clause 23. If the Committee decides that clause 222 should not stand part, when the Committee comes to decisions on new clauses, I will put the necessary Questions on new clause 23 without debate.

Joanna Cherry: I take it, Ms Dorries, that I am entitled to make a submission as to why the clause should not stand part of the Bill, and should instead be replaced with new clause 23.

The Chair: Exactly.

Joanna Cherry: In short, it is welcome that following the recommendation of the Joint Committee on the draft Bill, there is now some sort of sunset provision in the Bill. Those who sat on the Joint Committee or read its report will recall that various people who gave evidence made a strong case for a sunset provision in the legislation. The Information Commissioner summarised that case by saying:

“The draft Bill is far reaching and has the power to affect the lives of all citizens to differing degrees. For these reasons, the bill should include a sunset clause or other provisions requiring effective post legislative scrutiny. This would ensure that measures of this magnitude remain necessary, are targeted on the right areas and are effective in practice. To fail to make this provision risks undermining public trust and confidence. It will also enable the legislation to be considered in the light of the latest jurisprudence from the”

Court of Justice of the European Union and the European Court of Human Rights. Various variations on the Information Commissioner’s proposal were put to the Joint Committee by other witnesses, including medConfidential, Dr Paul Bernal, the right hon. Member for Haltemprice and Howden (Mr Davis), Privacy International and the Interception of Communications Commissioner’s Office.

The Home Secretary expressed reservations about having a sunset provision, but it is good to see that there is now some such provision in the Bill. What is missing from it, however, is an independent element.

6.15 pm

Clause 222 provides that at the relevant time, which is roughly five years after the legislation has been passed, the Secretary of State

“must...prepare a report on the operation of this Act.”

It goes on to say that he or she

“must...take account of any report on the operation of this Act made by a Select Committee of either House of Parliament (whether acting alone or jointly).”

To an extent, that follows up on recommendation 86 of the Joint Committee, because it recommended that a provision be added to the Bill for post-legislative scrutiny by a Committee of the two Houses within six months of the end of the fifth year after the Bill was enacted. However, an independent element is missing from this sunset clause.

Throughout the deliberations of this Committee, much reference has been made to the report of the independent reviewer of terrorism legislation, David Anderson, QC. I think we can all see the benefit of having that sort of independent input. The purpose of new clause 23 is to transform this sunset clause into one that will have the necessary element of independence to ensure the sort of public confidence that is required for a sunset clause.

I remind members of the Committee that the Information Commissioner said that a sunset clause should be there to shore up public trust and confidence. Without the independent element, it is less likely that such public trust and confidence will be ensured. The purpose of new clause 23 is to provide that

“The Secretary of State shall appoint an Independent Reviewer” to prepare the report, rather than it being done by the Secretary of State or persons acting under their auspices. The new clause would also provide that the necessary financial wherewithal was made available to enable that job to be done properly.

Keir Starmer: I shall speak briefly in support of new clause 23. The essential difference between this new clause and clause 222 is, of course, that the new clause would provide for a review within an initial period of five years and for subsequent five-yearly reviews, and for the reviews to be carried out by the independent reviewer, which we submit is more appropriate.

I understand why this new clause has been tabled, but it puts me in a bit of a dilemma. Is a review by the Secretary of State a good thing? Yes. I would therefore support clause 222 if I could not get anything better. I would not want to vote against the Secretary of State reviewing the Act if I lost on new clause 23, because it is sensible to have a Secretary of State review it. In other words, clause 222 is good, but new clause 23 is better;

[*Keir Starmer*]

that is the way I would put it. I am in a dilemma, because if I vote against clause 222, I am voting against a good clause that I would naturally support in principle, but if the vote on new clause 23 was not carried—and having looked at the voting record so far, I am not confident that it would be—

The Chair: Order. Mr Starmer, would it be helpful to say that you could table amendments to clause 222 on Report, if you wished to?

Keir Starmer: Yes, that is probably the way out of my dilemma, but really this is more for the record. I will not vote against clause 222, but that is not because I think it is preferable to new clause 23; I would like to have the new clause as well. We will reflect on how we deal with that apparent dilemma.

Mr Hayes: That was the most heartwarming qualified advocacy of an amendment that I have ever heard in Committee; I was quite touched by it. I could not help thinking that there must be countless Tory voters in Holborn and St Pancras who feel about the hon. and learned Gentleman as he feels about this clause. I know that he bathes in their generous acclamation on a daily basis. It was very decent of him to put his case in the way he did.

I will deal with the substance of the new clause and its purpose. The hon. and learned Gentleman is right that new clause 23 would replace the Government's proposals for a review of the operation of the Act as set out in clause 222, and he is also right that the clause obliges the Secretary of State to report to Parliament on the operation of the Act within four to five years. He described the detail, and I will not tire Committee members by quoting it more specifically. The new clause proposes instead the appointment of an independent reviewer to report on the operation of the Act every five years, beginning five years after the Act is passed.

Where we find common cause is in thinking that both pre-legislative and post-legislative scrutiny are essential. One could make that argument for most legislation, but particularly for legislation in this field, for two reasons: first, its import; and, secondly, the changing circumstances that will doubtless apply, as regards both technology, which the Bill deals with expansively, and the threat we face. All we know about the changes that have taken place over recent years suggests that those changes will continue and may grow in character and speed.

I fully understand why the hon. and learned Gentleman wants the whole House to take a close look at these matters over time. Indeed, the Home Secretary, in her evidence to the Joint Committee on the draft Bill, said:

“As technology advances, it may be necessary to revisit the powers, the legislative framework and the safeguards that are available”.

That is eminently sensible, and something that the Government wholeheartedly support.

As I said, clause 222 provides for judicial review. The hon. and learned Gentleman did not mention it, but he will know that the Joint Committee looked at that, and said that

“the appropriate vehicle to do this would be a specially constituted joint committee of the two Houses. This work should begin within six months of the end of the fifth year after which the Bill is enacted. Although the appointment of such a committee would be a matter for the two Houses, a provision in the Bill would provide a clear mandate and guarantee the timescale for this review.”

The Joint Committee gave that quite careful consideration. The members of this Committee who were also members of that one will recall that they did so because of the shared determination, which the hon. and learned Gentleman has articulated well, that we should not assume that as time goes on we will not need to be reasonably flexible about the application of the powers.

The Solicitor General made a point about providing legislation that looks as far into the future as possible. Certainly, the purpose of the Bill is to not only draw existing legislation into a single place but, as far as one reasonably can, prepare for the future. However, in doing so, it is important to be mindful of what the Joint Committee said, reflecting the Home Secretary's evidence.

The hon. and learned Member for Holborn and St Pancras will know that the Joint Committee went on to recognise that the Government cannot, in statute, require Parliament to appoint a post-legislative scrutiny Committee. Let me explain that a little more. Ms Dorries, as you will understand with your experience in the House, it is not for the Government to say what Select Committees might look at over time. It certainly would not be for the Government to dictate to the Intelligence and Security Committee, for example, how it should regard or review the legislation within its scope or purview. It would be a dangerous precedent to set to say that any particular Select Committee should, statutorily, consider matters at a particular point in time, or in a particular way.

The clause says that the report should take account of any other report on the operation of the Act, mindful of what I have just described—that is, that the ISC, other Select Committees, or Committees of both Houses could bring evidence to bear that would inform that review. In essence, it would be a matter for Parliament to decide precisely what was looked at and when, within the confines determined in the Bill, but it is essential that the Secretary of State is missioned to report on the Bill's implementation in the timetable described. That is something that legislation can quite properly do; it both gives all kinds of powers to the Secretary of State, and confirms those powers.

While I can see why the hon. and learned Gentleman supports the new clause, it is unnecessary, not because of the intent, but because of the detail. Essentially, we are offering two different models in order to achieve the same end. A parliamentary Committee would be just as independent as a separately appointed reviewer—and it would avoid the argument, which I know Opposition Members would be quick to have, about who should be responsible for appointing the reviewer.

Keir Starmer: This may be blindingly obvious, and any Secretary of State, including the current one, would almost certainly take this into account anyway, but could we amend subsection (3) to make it absolutely clear that the Secretary of State must take into account reports of the independent reviewer in addition to those

of Select Committees? While that is not precisely what the new clause would achieve, and while I am absolutely sure that any Secretary of State would do that in any event, it would weave in an element of the new clause's intention. It would not presuppose that there would necessarily be a report, but if there were one, it would be taken into account.

Mr Hayes: I am not unsympathetic to that suggestion, but let me qualify that slightly. There is an argument to say that we would want another reviewer involved in the process, because what we want is as much empiricism as possible. We have neither the time nor the patience for a long debate about the philosophical character of empiricism, and I am not an empiricist, philosophically, but in terms of legislation, it matters. There is an argument for introducing still more independence into the process.

The hon. and learned Gentleman is right to say that, of course, the Secretary of State would want to take into account the views of all those in positions of authority who have taken a view on the Bill and its implementation and effects in her or his report. I certainly would not want to exclude from that consideration any of the authoritative reports published on the Bill. I think that probably meets the hon. and learned Gentleman halfway, and perhaps a little more than halfway.

Any parliamentary review would take evidence from a range of witnesses. It is, again, almost inconceivable that the independent reviewer would not be a key witness, as our current independent reviewer was to the Joint Committee and other Committees of the House. It would—again, as the Joint Committee did—be likely to appoint technical advisers, who would inform the process and work in concert with the ISC. While the Government support a post-legislative review of the Bill, that review should be conducted by Parliament—by legislators drawing on external expertise and evidence, as the Joint Committee recommended. I therefore invite hon. Members not to press the new clause to a vote.

Joanna Cherry: I will not press new clause 23 to a vote.

Question put and agreed to.

Clause 222 accordingly ordered to stand part of the Bill.

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

6.30 pm

Adjourned till this day at Seven o'clock.

