PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

TELECOMMUNICATIONS (SECURITY) BILL

Seventh Sitting

Tuesday 26 January 2021

(Morning)

CONTENTS

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

not later than

Saturday 30 January 2021

The Committee consisted of the following Members:

Chairs: † Mr Philip Hollobone, Steve McCabe

† Britcliffe, Sara *(Hyndburn)* (Con)
† Cates, Miriam *(Penistone and Stocksbridge)* (Con)
† Caulfield, Maria *(Lewes)* (Con)
Clark, Feryal *(Enfield North)* (Lab)
Crawley, Angela *(Lanark and Hamilton East)* (SNP)
† Johnston, David *(Wantage)* (Con)
† Jones, Mr Kevan *(North Durham)* (Lab)
† Lamont, John *(Berwickshire, Roxburgh and Selkirk)* (Con)
† Matheson, Christian *(City of Chester)* (Lab)
† Onwurah, Chi *(Newcastle upon Tyne Central)* (Lab)
† Richardson, Angela *(Guildford)* (Con)
† Russell, Dean *(Watford)* (Con)
† Sunderland, James *(Bracknell)* (Con)
Thomson, Richard *(Gordon)* (SNP)
† Warman, Matt *(Parliamentary Under-Secretary of State for Digital, Culture, Media and Sport)*
West, Catherine *(Hornsey and Wood Green)* (Lab)
† Wild, James *(North West Norfolk)* (Con)

Sarah Thatcher, Huw Yardley, *Committee Clerks*

† attended the Committee

Public Bill Committee

Tuesday 26 January 2021

(Morning)

[Mr Philip Hollobone *in the Chair*]

Telecommunications (Security) Bill

9.25 am

The Chair: Before we begin, I have a few preliminary points. Please switch electronic devices to silent. Tea and coffee are not allowed during sittings. I remind Members about the importance of social distancing. Spaces for Members are clearly marked. I also remind Members that Mr Speaker has stated that masks should be worn in Committee. The *Hansard* reporters would be grateful if Members could email any electronic copies of their speaking notes to hansardnotes@parliament.uk.

Today we continue line-by-line consideration of the Bill. The selection list for today's sitting is available in the room. It shows how the selected amendments have been grouped for debate. Amendments grouped together are generally on the same or a similar issue. Please note that decisions on amendments do not take place in the order they are debated, but in the order they appear on the amendment paper. The selection and grouping list shows the order of debates. Decisions on each amendment are taken when we come to the clause to which the amendment relates.

Clause 6

Powers of OFCOM to assess compliance with security duties

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

The Parliamentary Under-Secretary of State for Digital, Culture, Media and Sport (Matt Warman): It is a pleasure to be back under your chairmanship, Mr Hollobone. As we discussed during the debate on amendments to this clause in our previous sitting, clause 6 inserts proposed new sections 105N to R, providing Ofcom with strengthened powers to assess whether providers of public electronic communications networks and services are complying with their security duty. These powers are vital to enable Ofcom to fulfil its expanded and more active role, giving it the tools to monitor and assess providers' compliance with the new telecoms security framework and providing the basis for commencing any enforcement action.

Proposed new section 105O provides the power to give assessment notices to a provider. Assessment notices may impose a duty on a provider to do a number of different things, which I will briefly summarise. First, providers can be required to carry out, or arrange for another person to carry out, technical testing in relation to their network or service. Secondly, they can be required to make staff available to be interviewed, enabling Ofcom to gain insights into how a provider's security practices and policies are implemented.

Thirdly, providers can be required to allow an Ofcom employee or an assessor authorised by Ofcom to enter their premises to view documents or equipment. I recognise that that is a significant power, but it is necessary. It is subject to certain restrictions to protect legally privileged information and to limit entry to non-domestic premises only. To provide clarity for telecoms providers, Ofcom will also publish guidance setting out how and when it will use the power. Importantly, providers have a right of appeal.

The powers of assessment set out in the clause are key to enabling Ofcom to carry out the effective and extensive monitoring and assessment of providers' security practices that is necessary.

Chi Onwurah (Newcastle upon Tyne Central) (Lab): It is a pleasure to serve under your chairmanship, Mr Hollobone, and to come back to this important Bill. I thank the Minister for writing to me and reassuring me on certain matters relevant to the clause. We accept the need for Ofcom to have powers to require information from vendors, but we would like a specific requirement whereby Ofcom can ask vendors for information on the diversity of their supply chains. I will leave further discussion on that for our new clauses. I will support this clause.

Question put and agreed to.

Clause 6 accordingly ordered to stand part of the Bill.

Clause 7

Powers of OFCOM to enforce compliance with security duties

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

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

Clause 8 stand part.

Clause 9 stand part.

Clause 10 stand part.

Matt Warman: I will seek to move relatively rapidly through these four clauses.

Clause 7 provides Ofcom with enforcement powers in relation to providers' security duties. The Bill gives Ofcom new powers to impose tough financial penalties on providers who breach their security duties. The penalties range to a maximum fine of 10% of a provider's annual turnover, which is in line with the maximum fines available for breaching other regulatory requirements. For continuing contraventions, Ofcom can levy a daily penalty of up to £100,000. Penalties that are generally lower than that but still significant will also apply for contravening information requirements, which are subject to a maximum penalty of £10 million or, for a continuing contravention, a penalty of up to £50,000 per day. These penalties ensure that there will be a real financial deterrent to poor security practices. I should also say that, in the most serious cases, or in cases where a provider repeatedly contravenes its security duties, Ofcom would be able to use existing powers to suspend or restrict the provider's entitlements to provide a network or service. Clearly, that is a step that we hope the regulator will never need to take.

The clause also gives Ofcom an important new power to take action where security is being compromised or is at imminent risk of being compromised. Proposed new sections 105U and 105V of the Communications Act 2003 would enable Ofcom to direct a provider to take interim steps to secure its network or service while Ofcom investigates or pursues further action. This power recognises that contravention of a security duty could result in a security compromise that causes real damage to users of that network or service. Where Ofcom uses that power, it will be required to commence and complete the enforcement process as soon as is reasonably practicable. The clause gives Ofcom the tools it needs to effectively enforce compliance with the new security framework.

Clause 8 sets out the position for bringing civil claims against providers who breach their security duties, which is a matter we touched on in earlier debates. It enables providers to be held accountable not just by Ofcom but by service users, such as members of the public, in cases where loss or damage is sustained by those users as the result of a breach of a duty. Providers owe a duty to any person who may be affected by a contravention of their security duties to take security measures, to comply with specific security duties in any regulations and to inform users of security compromises.

This clause allows any affected person to take legal action should providers breach those security duties. However, any affected person can bring legal proceedings against a provider only with the consent of Ofcom, which may be subject to conditions relating to the conduct of the legal action. This reflects the existing position in the Communications Act 2003 and ensures that providers face legal action only in appropriate circumstances. The clause also makes providers responsible to their users, providing another source of accountability. It allows users to bring legal claims for any losses they have suffered, which is only fair and reasonable.

Clause 9 addresses the interaction between provisions in the Bill and other legislation, specifically national security, law enforcement and prisons legislation. The security duties created by the Bill do not conflict with duties imposed on communications providers by other legislation via these clauses. Equally, we do not want the Bill to affect adversely the important work carried out by our law enforcement agencies, criminal justice authorities and intelligence agencies. The clause gives that clarity to providers about their responsibilities.

Finally, clause 10 requires that Ofcom publish a statement of policy about how it will fulfil its general duty and use specific powers to ensure that providers comply with their security duties. This will provide welcome clarity to industry about the expected use of important new powers. I beg to move that these clauses stand part of the Bill.

Chi Onwurah: I will not detain the Committee long, as we are cracking on through the clauses. I will only emphasise that these clauses give Ofcom broad powers—very broad powers—and measures of enforcement, as well as placing duties on the network operators to all users of their network services. We support these broad powers, but it is incumbent on the Minister and indeed on the Committee to consider whether those powers will receive sufficient scrutiny, and sufficient oversight and input from our security services. We anticipate debating those particular questions in more detail later today. In the meantime, we will not stand in the way of these clauses standing part of the Bill.

Question put and agreed to.

Clause 7 accordingly ordered to stand part of the Bill.

Clauses 8 to 10 ordered to stand part of the Bill.

Clause 11

Reporting on matters related to security

Chi Onwurah: I beg to move amendment 14, in clause 11, page18, line 26, at end insert—

"(aa) an assessment of the impact on security of changes to the diversity of the supply chain for network equipment;"

This amendment requires that network supply chain diversification is included in Ofcom reports on security.

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

Clause stand part.

Clause 12 stand part.

Clause 13 stand part.

Chi Onwurah: We start this debate where we ended our sitting on Thursday, on the diversity of the supply chain. But this is not groundhog day; this is a very different aspect of the diversity of the supply chain. I hope the Minister has noticed that there are three themes to our amendment: national security, diversity of the supply chain and appropriate scrutiny. Those are our key concerns about the Bill as it stands.

We wish to see the Bill debated as speedily as possible. For the record, I reiterate my concern that, in the midst of a pandemic lockdown, where the advice is to stay at home, the Leader of the House requires that Members of Parliament should congregate in one room for several hours. With that in mind, we are cracking on as quickly as possible, and we have made significant progress only this morning. However, we feel strongly that, given the speed at which we are providing the appropriate scrutiny, more time should be devoted to debating the Bill on the Floor of the House. We are cracking on in order to protect, as far as we can, the public health of Members of Parliament, staff, House officials and Clerks, who are doing an amazing job in the midst of a pandemic.

Clause 11 makes provision for reporting by Ofcom on security matters. That includes a duty to provide an annual security report to the Secretary of State. Amendment 14, in my name and those of my right hon. and hon. Friends, requires that network supply chain diversification is included in Ofcom's report on security. As I said, we anticipate having a broader debate this afternoon on the importance of the diversification of the supply chain to security, as part of the debates on our new clauses, so I will only summarise our key points and concerns now.

This amendment follows amendment 13, which sought to give Ofcom the power to request reports from operators on their supply and the progress of their supply chain diversification. We support steps to remove high-risk vendors from the UK networks, but they must go hand

[Chi Onwurah]

in hand with credible measures to diversify the supply chain. I am afraid it remains the fact that we have no reference to the diversification of the supply chain in the Bill, despite the fact that, as I will briefly outline, both the Secretary of State and experts during our evidence sessions emphasised that we could not have network security without effective diversification.

We cannot have a robust and secure network with only two service providers. Supply chain diversification is absolutely vital to protecting our national security. If a vulnerability exists in one vendor or service provider, that intrusion may be limited to that one vendor or service provider alone. A diversity of suppliers in the supply chain limits the exposure of vital information. This amendment ensures that network supply chain diversification is addressed in Ofcom's report on security. My key question to the Minister is, how can Ofcom report on security if it is not reporting on supply chain diversification?

The Minister may well say that Ofcom has the power to report on supply chain diversification and to request information on supply chain diversification. As I have said on a number of occasions, the powers in the Bill are broad. That is why effective scrutiny requires some specification of what will be reported upon.

The security report to the Secretary of State should be made as

"soon as practicable after the end of each reporting period"

and

"must contain… information and advice… to assist the Secretary of State in the formulation of policy".

It must also include the extent to which providers have complied with security duties. That is as an example of some of what may be included in the security report. Given that the Secretary of State has said on a number of occasions that supply chain diversification goes hand in hand with the security of the network, it is essential that supply chain diversification is specifically mentioned in the Bill, so that we can have accurate and detailed reports from Ofcom on key aspects of network security.

The amendment will help provide the Secretary of State with the information to update Parliament on the progress of the Government's diversification strategy, depending on Ofcom's findings. The Secretary of State has promised to give Parliament such updates, so this is an enabling amendment to ensure that the Secretary of State has the information he needs to provide the reporting that he has committed to.

In support of the amendment, I would like to cite one of the witnesses in our evidence sessions. Dr Alexi Drew, from Kings College, London, was asked whether it was possible to have a secure network without a diverse supply chain, and answered:

"That is a great question that comes with a very simple answer: no. The worst-case scenario for creating a risk in this sense is when monopoly meets supply chain—insecure supply chain in this case. Arguably, the reason why SolarWinds was so successful is that it provided the same service to so many different organisations and departments in the United States. Therefore, if you access one—SolarWinds—you access almost all. That is the risk."—[*Official Report, Telecommunications (Security) Public Bill Committee,* 19 January 2021; c. 87, Q110.]

That is a risk that, I am sorry to say, the Bill currently does not sufficiently address. I hope that, by accepting this amendment, the Minister will recognise that we are, as always, seeking to improve the Bill and to ensure that it provides a credible and effective means to secure our networks.

With regard to clauses 11, 12 and 13 stand part, we recognise the importance of providing Ofcom with the appropriate powers to request information, but also to share information related to security. In that respect, these provisions are ones that we can support.

9.45 am

Matt Warman: I welcome the spirit of the amendment. I think that the hon. Lady and I share the same ambition. I know that she wants to have the proper debate later, so we look forward to that.

Clause 11 inserts into the Communications Act 2003 proposed new section 105Z, which deals with Ofcom's reports on security. It requires Ofcom to produce such reports within two years of the Bill receiving Royal Assent and every 12 months thereafter. As the hon. Lady said, amendment 14 is similar to the amendment to clause 6 that we discussed previously. Ultimately, when considering Ofcom's role and specifically its reporting function, we should note that proposed new section 105Z(2) requires Ofcom security reports to include such information and advice as Ofcom considers may best assist the Secretary of State in the formulation of policy on telecoms security. That could go beyond the list in proposed new subsection (4) to include other relevant information, such as that related to diversification. The Secretary of State can also direct Ofcom to include information that goes beyond that list.

As the Committee and, indeed, Ofcom will be well aware, the Government have recently published a targeted diversification strategy, which will deliver lasting and meaningful change in the 5G supply chain and pave the way for a vibrant, innovative and dynamic supply market. We heard widespread support for the strategy from witnesses during the oral evidence sessions. The strategy demonstrates our commitment to building a healthy supply market and is backed by a £250 million initial investment.

We have publicly announced that the Government will be funding the creation of a UK telecoms lab to research and test new ways of increasing security and interoperability, and we are already partnering with Ofcom and Digital Catapult to fund the industry-facing test facility SONIC—the SmartRAN Open Network Interoperability Centre. Both of those will play a key part in our investment in diversification and demonstrate Ofcom's existing part in it.

As already mentioned, amendment 14 would require Ofcom to include in its security reports

"an assessment of the impact on security of"

any

"changes to the diversity of the supply chain for network equipment".

As that requirement is already essentially covered by Ofcom's existing powers, the amendment is not necessary. The inclusion of any such information is already within Ofcom's discretion, but I am sure that we will discuss it more later on, as the hon. Lady said.

Clause 12 expands Ofcom's information-gathering powers for the purposes of its security functions and enhances its ability to share the information with the Government. It enables Ofcom to require a provider to produce, generate, collect or retain security information,

and then to analyse that information. Any information sought using this power must always be proportionate to how Ofcom will use it.

Clause 13 makes provision in connection with the standard of review applied by the Competition Appeal Tribunal in appeals against certain of Ofcom's security-related decisions. Ofcom's regulatory decisions are subject to a right of appeal to the tribunal, and that will also be the case for most of Ofcom's decisions relating to the exercise of its regulatory powers conferred by the Bill. This clause makes provision to ensure that the tribunal is not required to modify its approach in appeals against relevant security decisions, and should instead apply ordinary judicial review principles.

I hope that I have sufficiently explained to the Committee why amendment 14 is unnecessary and why clauses 11 to 13 as drafted should stand part of the Bill.

Chi Onwurah: I thank the Minister for his comments. Although we agree on many things in many areas, I think that in this case he is trying to have his cake and eat it, inasmuch as he is saying that amendment 14 is not necessary because Ofcom already has the powers, but he is reluctant or is refusing to specify that those powers will be used for the objective of reporting on the progress of diversification of the supply chain. It was good to hear the Minister reiterate the importance of diversification of the supply chain, but I remain confused about whether he agrees with the evidence and, indeed, with his own Secretary of State that diversification of the supply chain is a prerequisite of the security of our networks and, indeed, our national security—that is what we are discussing with regard to our telecoms networks. If diversification is a prerequisite, why is the Minister so reluctant to refer to it? If he is so confident in the plan to diversify our supply chains, why is he so reluctant to insert any requirements to report on the progress of that diversification?

I listened intently: the Minister said that Ofcom has the powers to report on whatever it considers to be relevant to security. During the evidence session, we heard from Ofcom itself, very clearly and repeatedly, that it is not for Ofcom to make decisions on national security. It will not make national security decisions. That is not within its remit and responsibilities; the witnesses from Ofcom stated that repeatedly and clearly. I would be happy to read from *Hansard* if that point is in question. Given that Ofcom will not make security decisions and that the diversification of the supply chain is essential for security, I am at a loss to understand why the Minister will not accept a reference to reporting on the progress of diversification. Although, unfortunately, the pandemic means that we are not at full strength on the Opposition side of the Committee, I wish to test the will of the Committee on the amendment.

Question put, That the amendment be made.

The Committee divided: Ayes 3, Noes 10.

Division No. 1]

AYES

Jones, rh Mr Kevan
Matheson, Christian
Onwurah, Chi

NOES

Britcliffe, Sara
Cates, Miriam
Caulfield, Maria
Johnston, David
Lamont, John
Richardson, Angela
Russell, Dean
Sunderland, James
Warman, Matt
Wild, James

Question accordingly negatived.

Clause 11 ordered to stand part of the Bill.

Clauses 12 and 13 ordered to stand part of the Bill.

Clause 14

REVIEWS OF SECTIONS 1 TO 13

Chi Onwurah: I beg to move amendment 15, in clause 14, page 21, line 28, leave out from beginning to end of line 30 and insert—

"(3) The reports must be published not more than 12 months apart for the first 5 years, then not more than 5 years apart.

(4) The first report must be published within the period of 12 months beginning with the day on which this Act is passed.".

This amendment requires the Secretary of State to report on the impact and effectiveness of clauses 1 to 13 every year for the first five years after the Act is passed, and then every five years following.

The amendment reflects another of our key concerns about the Bill, which is the level and extent of appropriate scrutiny for such broad and sweeping powers. It seeks to ensure appropriate scrutiny. Clause 14 requires the Secretary of State to review the impact and effectiveness of clauses 1 to 13 at least every five years. Our amendment would require the report to be published every year for the first five years after the legislation is passed, and then up to every five years after that.

As we have said, the Bill gives the Secretary of State and Ofcom sweeping powers. We want to ensure both that they are proportionate and that there is accountability. As we have previously emphasised, we are sure that the Minister and the Secretary of State are inclined to exercise the powers in a proportionate and accountable way, but they will not be in their posts forever, and perhaps not for the entire first five years of the legislation's operation, so it is important that the Bill requires that Parliament be able to scrutinise its effectiveness, as that is so important to our national security. In that sense, this amendment follows amendments 5, 9 and 10 with respect to the requirement for appropriate oversight and accountability.

I emphasise—I am sure that you will understand, Mr Hollobone—that in some ways we are here because of a lack of effective parliamentary scrutiny of the presence and growth of high-risk vendors in our networks. It was only when Parliament became aware of and was able to give its full-throated input on concerns about the dominance of high-risk vendors in our telecommunications market that the Government took action. We do not want to be in the position of finding again that there has been a dramatic change in the security of our networks without appropriate scrutiny.

Clause 14 states that the Secretary of State must

"carry out reviews of…impact and effectiveness"

and that the report must be laid before Parliament for parliamentary scrutiny. However, we are to wait up to five years before it will be made possible to give

[Chi Onwurah]

parliamentary scrutiny to a Bill that is so important to national security, as both the Minister and the Secretary of State, and indeed the security services, have emphasised. We are not to review its effectiveness for five years.

Sara Britcliffe (Hyndburn) (Con): Does not the clause state that the period is up to five years? The review could be done during that period; it would not have to be at the five-year mark every time.

Chi Onwurah: The hon. Lady is absolutely right. The clause enables the Minister or Secretary of State to choose to lay a report more frequently. Again, I do not want to impute anything against the Minister or the Secretary of State, but given the importance of the subject and of parliamentary review, why not ensure that it is more frequent?

I am sure that the hon. Lady will agree that Parliament has many things to consider, and so does the Secretary of State. There is competition for parliamentary time, particularly in a pandemic and in view of the challenges that we shall face in the next few years. How can I put this? We have concerns that the priority may slip in the face of, for example, economic challenges, investment challenges and recovery challenges. We want to be sure what is happening. We are the party of national security and we want to ensure that, in this context, national security is brought to Parliament to be debated, discussed and reviewed at least every year.

10 am

I have outlined the importance of parliamentary scrutiny as part of our wish to do that, but we should also consider what might happen in the next five years, before the first review mandated by the Bill. We have seen vast technical, technological and geopolitical shifts in the last five years. We face security challenges from China and Russia, and terrorist threats in a complex security environment. I am sure the Minister does not anticipate that those hostile actors against whom the measures in the Bill securing our networks are primarily directed will not respond; they will do so. We cannot imagine that we will take these measures to secure our networks against those who seek to attack or undermine our telecommunications capability in their own interests and they will not respond in some way. As it stands, the first review of that response could be five years after it has happened.

In addition, specifically with regard to the hope on which the Government might be placing an unjustified amount of assurance in diversifying our supply chains using open radio access network technology, we heard from witnesses that the next five years are key. The next five years will be the period in which we will see—or not see—the maturity of open RAN technology. There was a discussion about whether open RAN will be a viable and credible alternative in the next year, two years, three years or four years. While there are technological changes and the maturity of open RAN is in question, spending the next five years without having a review of its effectiveness seems to me to lack appropriate oversight.

There is support for increased review measures. We heard from Derek McManus, the chief operating officer of O2, about the evolution of open RAN. He said:

> "There are trials in the UK…it will be at least a couple of years before you have a viable technical and commercial product, focused initially on rural."—[*Official Report, Telecommunications (Security) Public Bill Committee,* 14 January 2021; c. 11, Q5.]

As things stand, that period could pass without any review or report. We also heard from Emily Taylor, the chief executive of Oxford Information Labs, who said:

> "Imagine if we were sitting here, in five or 10 years' time, lamenting the fact that the equipment market is now dominated by Microsoft and Google. I am just making that up as a hypothetical example—I have no knowledge to back that up—but those are the companies that have the sufficient scale and skills, and as Chi Onwurah said in her question we are moving to a more hybrid network, where skills in cloud computing and software are going to define the success of the player."—[*Official Report, Telecommunications (Security) Public Bill Committee,* 19 January 2021; c. 77, Q92.]

I am quoting someone quoting me, who says that

"skills in cloud computing and software are going to define…success"

but we are going to wait five years to review, when, as I am sure the Minister is well aware, given his background, five years could be five technological generations in this area.

The next five years will be key to the maturation of the technologies about which the Minister has so many hopes to help with the diversification of our supply chain and in terms of the global security and geopolitical environment and landscape, yet we have no requirement for reporting or accountability during that time. That is what the amendment is designed to change.

Matt Warman: I listen with interest to the points that the hon. Lady makes, and to the assertion that she is a member of the party of national security. I welcome her to this side of the House, if that is the case. *[Interruption.]* Thank you, but no.

As the hon. Lady says, clause 14 is a review clause requiring the impact and effectiveness of clauses 1 to 13 to be reviewed at least every five years by the Secretary of State. The review report must be published and laid before Parliament, but it is by no means the only source of parliament scrutiny, as she knows. Her amendment would increase the frequency of these reports to every year for the first five years after the Bill is passed and then every five years thereafter.

Increasing the frequency of the reports would bring its own challenges for a number of reasons. First, the framework is considerably different from the previous security regime in the Communications Act 2003. It seems to me that we will not be able fully to assess the impact and effectiveness of the new security regime instituted by clauses 1 to 13 until all parts of the framework, including secondary legislation, codes of practice and other things, have been in place for a reasonable period of time. The code of practice that will provide guidance on the detailed security measures that telecoms could take is intended to set clear implementation timelines. Some measures may require significant operational change, as we heard in the evidence sessions for telecoms providers, and we are aware that that may be costly. For that reason, we cannot reasonably expect all changes to be implemented instantly or, indeed, all necessarily at the same time.

There is a further practical difficulty with the amendment. If the first report is to be produced 12 months after Royal Assent, it will require the review to be undertaken

well in advance of that deadline. That means that the report will represent an incomplete picture of the Bill's impact, even at its very first production. Some measures will not even have been implemented by telecoms providers.

My hon. Friend the Member for Hyndburn was exactly right that the current requirement for publishing reports is at least—rather than at most—every five years. We have been deliberate in our choice of this timeframe because five years is the reasonable point by which we expect the majority of telecoms providers to have implemented most, if not all, changes. It is therefore considered appropriate to require a report on the impact and effectiveness of the framework by that time. I recognise that five years is a long time. That does not mean that the framework will be free from scrutiny in the intervening period. As clause 11(3) sets out, the Bill amends section 134B of the Communications Act so that Ofcom's regular infrastructure reports will include information on public telecoms providers' compliance with the new security framework. Ofcom publishes the reports annually, rendering the amendment unnecessary.

Chi Onwurah: On a point of clarification, I have the impression that the Minister anticipates that the first report under the Bill would only happen once all the requirements had been implemented. I think that that implies that it would only happen once a high-risk vendor, specifically Huawei, had been removed from the network.

Matt Warman: No is the short answer, because while this is a progress report, five years from 2021 is 2026—the deadline is 2027, even at the most extreme end, which is not where we anticipate it will end up—and it would be before the point that she identifies.

The infrastructure reports from Ofcom will help to provide Parliament and the public with a view on how telecoms providers are progressing with compliance with the new framework. As I alluded to earlier, they are not the only means of parliamentary scrutiny. We have the Intelligence and Security Committee and we have Select Committees. I suspect that there might be one or two debates on this matter over the next five years as well. To pretend that this is the only method of parliamentary scrutiny is not accurate.

Chi Onwurah: If the Minister will give way briefly, he may find it saves time. To clarify: for the first report we will not necessarily have to wait until all the provisions of delegated legislation associated with the Bill are in place. As for the infrastructure reports that Ofcom publishes, to which he refers as a form of alternative scrutiny, will they, might they or will they not reflect progress in the diversification of the supply chain?

Matt Warman: The hon. Lady asks me to predict what is in a report that has not been written yet by an organisation that is not a Government Department. I agree with the principle of what she is saying. This is an important aspect and one would reasonably expect it to be reflected in the reports that we have talked about. It is, however, important overall to say that Ofcom's own regular infrastructure reports will, as I have said, include information on public telecoms providers' compliance with the new security framework, which is the broadest interpretation and gives a huge amount of latitude for the sorts of information that she seeks. I hope that those infrastructure reports will help to provide Parliament with the kind of scrutiny that she seeks, and the public with the kind of scrutiny that we all seek. *[Interruption.]* For those reasons I hope that she will withdraw the amendment.

Chi Onwurah: I thank my right hon. Friend the Member for North Durham for an exciting intervention from his phone, and I thank the Minister for his comments. As I think I have said, I spent six years working for Ofcom with the Communications Act 2003 on my desk. I know the importance that our independent regulator places on the words of the Minister during such debates as this. As he has indicated that the reports would do well to include reference to everything that appertains to security, including the diversification of supply chain, I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Clause 14 ordered to stand part of the Bill.

Clause 15

Designated vendor directions

The Chair: With suitable musical introduction, I call Kevan Jones to move amendment 16.

Mr Kevan Jones (North Durham) (Lab): I beg to move amendment 16, in clause 15, page 22, line 12, at end insert—

"(2A) When considering whether a designated vendor direction is necessary in the interests of national security, the Secretary of State must take account of the advice provided by the intelligence services."

This amendment would require the Secretary of State to give due priority to advice provided by the Intelligence Services (including the National Cyber Security Centre as part of GCHQ) when considering when to issue a designated vendor direction.

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

Amendment 17, in clause 16, page 27, line 8, at end insert—

"(3A) When considering whether a designation notice is necessary in the interests of national security, the Secretary of State must take account of the advice provided by the intelligence services."

This amendment would require the Secretary of State to give due priority to advice provided by the Intelligence Services (including the National Cyber Security Centre as part of GCHQ) when considering whether to issue a designation notice.

Amendment 18, in clause 16, page 28, line 3, at end insert—

"(m) the person's control of data flows."

This amendment requires the Secretary of State to consider a person's potential control of data flows when issuing a designation notice.

Clause 16 stand part.

Amendment 19, in clause 17, page 29, line 19, at end insert

", together with an assessment of the impact the designation notice will have on supply chain diversity;".

This amendment requires the Secretary of State to lay before Parliament a report on the impact a designation notice will have on telecoms market supply chain diversity, enabling parliamentary scrutiny.

Mr Jones: I thought I would bring some light relief to the Committee's proceedings. Amendments 16 and 17 are both probing amendments. I might sound like a broken record, but they are really just to ensure that we get a situation where the necessary advice is taken. Amendment 16 states:

"When considering whether a designated vendor direction is necessary in the interests of national security, the Secretary of State must take account of the advice provided by the intelligence services."

I accept that the entire purpose of the Bill is to have national security at its heart, but I still have a nagging doubt about whether Ofcom will be able to put national security at the heart of its considerations.

Amendment 17 states:

"When considering whether a designation notice is necessary in the interests of national security, the Secretary of State must take account of the advice provided by the intelligence services."

This is an attempt to future-proof the Bill. As I mentioned the other day, when we pass legislation in this place it is important that it outlives present Ministers, and us all. Unfortunately, there is form on this—look at the Intelligence and Security Committee's 2013 report on critical national infrastructure. I accept it was then the Cabinet Office, not Ofcom, that dealt with this, but when BT negotiated its contract with Huawei, the Cabinet Office was told about it but did not feel it necessary to tell Ministers for another three years, until 2006. I am concerned that national security will not be at the forefront when people look at such matters. The amendment is really just to ensure that that takes place, and codifies it into law.

I do not wish to criticise civil servants in any way, but having been a Minister myself, I know they sometimes have a tendency not to put forward things that might have a political dimension that they do not recognise. That is why it is important for national security that the Secretary of State has first-hand knowledge and information directly from the security services. We have very effective security services in this country—I pay tribute to them—but we also have the Cabinet Office. I know the Minister might think I am a bit obsessive, but I am sure he has come up against the buffer of the Cabinet Office, which seems to want to intervene in everything and anything that does not really concern it.

10.15 am

The Secretary of State should have access directly to the security information and should not have to go through the filter of the Cabinet Office or Ofcom. I accept the assurances that the Minister gave about Ofcom's ability to give advice and work closely with the security services, and these are probing amendments. I am interested in what he says about how we can ensure that when the Secretary of State takes a decision, national security is at its heart, and that he or she got it straight from the horse's mouth—in other words, from the security services—rather than its being filtered through the membrane that sometimes exists in Whitehall.

Matt Warman: I thank the right hon. Gentleman for his contribution to the debate. He has talked so much about my impermanence that I felt lucky to come back today, never mind any time in the future. He makes a reasonable point, with which I broadly sympathise. As this is a broad grouping that covers clauses 15 and 16 and the amendments to clauses 15, 16 and 17, I will discuss the policy intention behind the clauses in sequence, and address the amendments.

As the right hon. Gentleman said, it is obviously an opportune moment to pay tribute to the heroic work of our national security services. The Bill emphasises the importance of their advice, and it empowers the Government to manage the presence of high-risk vendors in our networks. The report to which he refers is important, but it is also important to say that it was published, as he said, in 2013. It related almost entirely to events that took place under Labour, and it predates the existence of the National Cyber Security Centre, so we are dealing to some extent with a different world. I will go into a bit of detail on that.

As the right hon. Gentleman knows, the Government announced in January last year that new restrictions should be placed on the use of high-risk vendors in the UK's 5G and full-fibre networks. In July 2020, the Government worked with the NCSC to update the guidance following action taken by the US Government in relation to Huawei. Clauses 15 to 17 provide the principal powers that the Government need to manage the risks posed by high-risk vendors. Without such powers, the guidance issued to industry will remain unenforceable and therefore present a risk to national security.

Mr Jones: I accept what the Minister says about the report, but its key point was that civil servants basically decided not to tell Ministers. On his explanation and the way forward, or what has changed since, how can we avoid a situation whereby Cabinet Office civil servants take the decision not to tell Ministers? How can we ensure that that will not happen again?

Matt Warman: In short, the right hon. Gentleman is challenging the fundamental effectiveness of Government and the judgments that were made by officials at the time. I simply say that it is the duty of Government to ensure that such errors are not made in future. That cannot be done solely by legislative means; it must be done by custom and practice. The right hon. Gentleman understands, through his work on the ISC, that the role of those close working relationships is in some ways far more important in the day-to-day security issues that we are dealing with. Perhaps we can return to that point later.

The Bill will allow the Secretary of State to issue designated vendor directions, imposing controls on the use of goods, services or facilities that are supplied, provided or made available by designated vendors. The Secretary of State may issue such directions only where it is necessary to do so in the interests of national security and proportionate to the aims sought to be achieved.

Amendment 16, which would amend clause 15, seeks to place a statutory requirement on the Secretary of State to take into account advice from our intelligence services when considering whether to issue a designated vendor direction. Amendment 17, which would amend clause 16, seeks to place a similar requirement when considering a designation notice.

I should reassure hon. Members that the Secretary of State, as the right hon. Member for North Durham knows, has every intention of seeking the advice of our

security and intelligence services, as would any Secretary of State, in particular the NCSC, when considering whether to issue a designated vendor direction or designation notice.

It is also worth saying, from a scrutiny point of view, that the Department for Digital, Culture, Media and Sport maintains an excellent relationship with the NCSC. We are scrutinised by the Select Committee on Digital, Culture, Media and Sport and I have appeared before the Intelligence and Security Committee, as the right hon. Gentleman knows. There are many examples in the Bill where the NCSC's expert advice has been taken into account.

The UK telecoms supply chain review, on which the Bill is based, was the product of the close working relationship between the Department for Digital, Culture, Media and Sport and the NCSC. In a sense, that close working relationship demonstrates that matters have moved on substantively since 2013.

I draw hon. Members' attention to the illustrative notices that we published in November last year. The NCSC was closely involved in the drafting of those illustrative notices. It will also be involved in the drafting of direction and designation notices once the Bill has been enacted . Given the demonstrable success of our collaboration with the NCSC thus far, I hope that the right hon. Gentleman will be satisfied with that explanation, although I appreciate that he introduced a probing amendment.

Clause 15 would create the new power for the Secretary of State to issue designated vendor directions to public communications providers, in the interests of national security. Although clauses 15 and 16 are distinct, they are complementary. Directions cannot be issued without identification of a designated vendor and designations have no effect unless directions are given to public communications providers. Clause 15 inserts new sections 105Z1 to 105Z7 into the Communications Act 2003 and amends section 151 for that purpose.

The clause will enable the Government's announcements in 2020 on the use of high-risk vendors to be given legal effect. Those announcements include advice that require a public telecoms provider to exclude Huawei from their 5G networks by 2027, and stop installing new Huawei goods, services or facilities in 5G networks from September 2021. It will also enable the Government to address risks that might be posed by future high-risk vendors, helping to ensure our telecoms networks are safe and secure.

Proposed new section 105Z1 sets out the direction power. It would allow the Secretary of State to give a designated vendor direction to a provider, imposing requirements on their use of goods, services or facilities supplied by a specified designated vendor. Proposed new section 105Z2 provides further details on the types of requirements that may be imposed in a designated vendor direction. Proposed new section 105Z3 sets out the consultation requirements and expectations for public communications providers. Proposed new section 105Z4 sets out a requirement for the Secretary of State to provide a copy of a direction to the designated vendor or vendors, specified in a direction and, hence, affected by it. Proposed new sections 105Z5 and 105Z6 set out when and how the Secretary of State may vary or revoke a direction. Lastly, 105Z7 enables the Secretary of State to require a public communications provider to provide a plan setting out the steps that it intends to take to comply with any requirements set out in a direction and the timings of those steps.

Although the Government have made specific announcements on Huawei, the high-risk vendor policy has not been designed around one company, country or threat. The designated vendor direction power, as set out in these provisions, is intended to be an enduring and flexible power, enabling the Government to manage the risks posed to telecoms networks both now and in the future.

Clause 16 includes a non-exhaustive list of matters to which the Secretary of State may have regard when considering whether to issue a designation notice. Amendment 18 seeks to amend that clause by adding a person's control of data flows to the list of matters to which the Secretary of State may have regard. However, nothing in the clause prevents the Secretary of State from considering control of data flows before issuing a designation notice already, if the matter were deemed relevant to the assessment of national security. It is already covered and so is not required as a stand-alone measure.

The clause creates a power for the Secretary of State to issue a designation notice, which designates a vendor for the purposes of issuing a designated vendor direction. Proposed new section 105Z8 is the principal measure of the clause, and sets out the power for the Secretary of State to designate specific vendors where necessary in the interests of national security. A designation notice must specify the reasons for designation unless the Secretary of State considers that doing so would be contrary to the interests of national security. The proposed new section also lists the primary factors that may be taken into account by the Secretary of State when considering whether to designate a vendor on national security grounds.

Finally in this group, amendment 19 would require the Secretary of State, when laying a designation noticed before Parliament, also to lay before Parliament a report detailing the impact that the designation notice might have on the diversity of the UK's telecoms supply chain. The effect of the amendment would be to require the Secretary of State to lay a report purely on the impact of the designation notice, but a designation notice simply notifies vendors that the Government consider them a risk to national security.

Only when the designation notice is issued alongside a designated vendor direction are controls placed on the use of a designated vendor's goods, services and facilities by public communication providers, so it is those controls that might have an impact on the diversity of the supply chain. I can reassure the Committee that the Government will consider the diversity of the supply chain before issuing designation notices and designated vendor directions. A lack of diversity is in itself a risk to the security of a network. I hope that answers the question that the hon. Member for Newcastle upon Tyne Central asked in regard to an earlier amendment. It is right that the Government consider that risk before deciding whether to issue designation notices and designated vendor directions.

To conclude, clauses 15 and 16 provide us with the ability to improve the security of our telecommunications networks and to manage the risks relating to high-risk vendors, both now and in the future.

Mr Jones: I thank the Minister for his reply. I do not question his commitment to ensuring that we have security at the heart of the Bill, and I do not intend to press my amendments to a vote.

Chi Onwurah: I will speak to amendments 18 and 19, standing in my name and those of my hon. Friends, and to clauses 15 to 17. As the Minister set out, the clauses are about key powers in the Bill that seek to secure our networks and to regularise requirements already in place, albeit informally or not legally, to remove Huawei as a specific high-risk vendor from our networks. The clauses give Government the powers to do what they have said they will do.

On the clauses, I will not repeat what the Minister said, and I congratulate him on clearly setting out their powers, which the Opposition believe are necessary. I also join the Minister and my right hon. Friend the Member for North Durham in paying tribute to our security services, which do such great work to keep us secure across a wide range of threats and challenges—both present and evolving—and on whose continued work and effectiveness the Bill is highly dependent. As my right hon. Friend set out, we want to ensure that national security is absolutely at the heart of the Bill.

10.30 am

As the Minister set out, the clauses are rightly not specific to Huawei or any vendor or country of origin. It is also important, as the Minister clarified to me in a letter, that they sit in addition to the current process for identifying and designating high-risk vendors and then issuing designated vendor directions, which set out how a designated vendor is to be treated and are critical to ensuring that we do not again find ourselves in a position where we have a high-risk vendor dominant in our telecommunications networks.

Although I accept that the clauses were not designed for Huawei, as is right, the Minister and the Committee must recognise that their impact will be different for Huawei and for future vendors. Parliament and the sector have spent some years considering the level of risk posed by Huawei specifically, and we have spent some time in this Committee discussing the impact of removing Huawei on the diversity of our supply chain. We have agreement from the Secretary of State, the sector and experts that that leaves us in a position where we have only two vendors, effectively, which is not, as the Minister set out, an acceptable position.

Any further designated vendor notices after the one to deal with Huawei will have a considerable impact and will require considerable consultation. We are in a position now where our telecommunications networks supply chains are not diverse or resilient; that is the general consensus. A further designated vendor notice will therefore have a significant impact on the progress of the diversification of our supply chains, which I do not feel is adequately reflected in the Bill or the debate around it. That is partially what our amendments seek to probe.

We are quite focused on Huawei and the process that got us into the mess that we are in at the moment, having to rip a vendor out of our existing networks. I am not sure that we are sufficiently focused on what will happen in the future should there be a need to designate another vendor, perhaps from a hostile state or perhaps not, because of the impact on security. Our amendments probe whether there is sufficient understanding there.

Amendment 18 amends the list of concerns in clause 16 to which the Secretary of State must pay attention when issuing a designation notice, by adding,

"the person's control of data flows."

The list is already quite long, at about 40 lines, and includes,

"the nature of the goods… the reliability of the supply of those goods… the extent to which and the manner in which goods, services or facilities supplied, provided or made available by the person are or might be used in the United Kingdom".

Our concern, which we are highlighting, is whether those are sufficiently forward-looking, whether we are—as was suggested in evidence sessions—fixated on Huawei, the current architecture and current major security threats, and whether we are looking forward to the evolving security threats. That is because—as we have said and I will repeat—the Labour party puts national security at the heart of our scrutiny of this Bill, as the party of national security, a priority which is above the economic considerations that have too often been prioritised above our national security.

Our concern is that failings in the Bill show that the Government may take risks with the security critical network infrastructure and, as part of that, with our long-term economic security. Data is absolutely central to the information economy, which is the economy. Almost all digital services gather personal data and use it for commercial purposes. Data is often described as the new oil. I prefer to call it the engine of our economy. The international and national flows of data are critical to our security, as well as to our economy. We would like the Minister to explain that the protection for UK data flows is recognised as a threat, which is taken into account by the Secretary of State when considering designation notices.

One reason behind the amendment is what we heard from the Committee's expert witnesses. In response to my question about different aspects of network security that might not be fully addressed by the Bill as it stands, Dr Louise Bennett, the director of the Digital Policy Alliance, said:

"I think most people would agree that the diversity of end points, of interfaces and of applications running over complex networks all pose security problem areas. The more of those you have, the more resilient your network might be on the one hand, because there are multiple parts, but on the other hand, the harder it is to maintain them adequately."—[*Official Report, Telecommunications (Security) Public Bill Committee,* 14 January 2021; c. 52, Q68.]

Dr Bennett suggested that control of data flows was a threat that needed to be specifically addressed by the Bill. Howard Watson, the chief technology officer of BT Group, also said:

"We also faced logical threats, such as malware implants, DDoS attacks and what are called advanced persistent threats, which is an actor embedding themself into parts of the environment, staying hidden for a while and potentially collecting credentials—think of the SolarWinds hack that is in the news at the moment."—[*Official Report, Telecommunications (Security) Public Bill Committee,* 14 January 2021; c. 17, Q16.]

Emily Taylor, chief executive of Oxford Information Labs, said

"It is also the case that consolidation of infrastructure providers, like the cloud providers, is a security risk, because they become too big to fail. There was a brief outage of Google just before Christmas, and people just cannot work. When Cloudflare or Dyn go down, they introduce massive outages, particularly at a

point where we are all so reliant on technology to do our work. These are security risks, and that highlights the need for a flexible approach. You have to be looking across all sectors."—[*Official Report, Telecommunications (Security) Public Bill Committee,* 19 January 2021; c. 74, Q88.]

The witness evidence testimonies show that this is not only about the ability to control our signalling systems and protocols in the 5G network as it stands, but as the network evolves more and more of the network control will be both in the centre and on different infrastructure, such as Amazon Web Services in the cloud.

What I particularly want the Minister to respond to the question of how he anticipates the threat from consolidation as the network evolves—this consolidation at cloud level—will be addressed by designation notices? He said that the amendment talks about having regard to designation notices rather than the directions, which would specify the steps that operators have to take. When it comes to making decisions when issuing a designation notice, this requirement fits in with paragraphs (a) to (l), which are already included.

Amendment 19 to clause 17 requires the Secretary of State to lay before Parliament a report on the impact a designation notice will have on telecoms market supply chain diversity to enable parliamentary scrutiny. The amendment seeks to provide greater scrutiny of the diversification of the telecoms market supply chain, which, as we have all agreed, is a prerequisite for the Bill to be effective. It follows amendments 13 and 14, which we have already discussed, in addressing supply chain diversity.

I have mentioned a number of times that the Bill does not refer to the diversification strategy. We heard during the evidence sessions that it was a strategy and not yet a plan. The security of our networks depends on an effective plan to diversify the supply chain, which should also include support for UK capability. The amendment would require that a report be laid before Parliament to set out the impact that the designation notice will have on supply chain diversity. The Minister commented on whether it should be the designation notice or the direction. The objective of the amendment is to ensure discussion and understanding of the impact on the diversification strategy. It is particularly important because, as I have said, any future designation notice will be in the context of a telecoms supply chain that has been significantly reduced as a consequence of Huawei's removal. It is important that the further impact be understood.

10.45 am

To be clear, we recognise that a designation notice is an appropriate response where there are risks to our national security and to the security of our telecommunication networks, regardless of the impact on diversification. However, we feel strongly that it is important to understand the impact, because of the reduced state of diversification in our supply chain. We cannot have a robust and secure network with only two vendors, and the Government's emphasis on open RAN technology is yet to be shown to be sufficient to ensure the diversification of our networks in a reasonable timeframe.

I want us to imagine that the Government chose, for whatever reason, to issue a designation notice against one of the remaining vendors—Ericsson or Nokia. It would be critical for the impact on the progress of the diversification strategy to be set out, as well as for discussions to be had with industry and so on. A designated vendor notice could remove a vendor from the supply chain, further reducing resilience and security. I am sure the Minister will agree that it would be important to fully understand the implications, even as we put in place a designation notice. I think we all agree that we are aiming to have a rich diversity of suppliers, but it is also essential to understand the impact of designation notices on that.

We want to encourage the network operators to diversify their supply chains, as we discussed in the evidence sessions. The Bill contains a lot of stick and not very much carrot. A designation notice is absolutely a stick. A requirement to report on the impact on supply chain diversity would encourage the Government to put in place appropriate carrots to increase the incentives for diversification with one hand, as they take away potential vendor diversity in the supply chain with the other.

I support the clauses standing part of the Bill.

The Chair: Order. The hon. Lady has done really well, but we are not debating clause 17 stand part. She can refer to the other clause if she wishes.

Chi Onwurah: Thank you for the clarification, Mr Hollobone. I see that we are discussing whether clauses 15 and 16 stand part. I support those clauses and look forward to the Minister's response to the amendment.

Matt Warman: I pre-emptively covered a lot of the hon. Lady's questions, but I will say two brief things. She talked about consolidation in the cloud sector. While the Bill is very much a national security Bill, the National Security and Investment Bill would cover consolidation in that sort of sector, rather than this one. Obviously they do work together.

Chi Onwurah: The point I am making—clearly, I did not make it effectively—is that that sector is becoming this sector. The cloud sector is becoming the telecoms sector. The reason we need this Bill in addition to the National Security and Investment Bill is to address the security concerns of the telecoms sector specifically. The cloud sector is becoming part of the telecoms sector, yet the Bill does not address those concerns.

Matt Warman: The hon. Lady is not wrong, obviously, in the sense that there is a potential conversation to be had about when a cloud provider is a telecoms provider and vice versa, if I can put it like that, although it is not the most elegant way of doing so. However, the point is that the reason we have comprehensive coverage of the landscape is because we have both the National Security and Investment Bill, which she debated recently, and this Bill. The broad powers that she described are intended to provide precisely that sort of coverage.

Similarly, the hon. Lady referred to the length of the list in clause 16 of matters that can be taken into consideration. That relates to the point I made previously, namely that the sorts of issues that she is talking about, such as data flows, are already covered in the long list. The list is as long as it is because it is intended to look to the future. Therefore, being prescriptive in the way that she describes is fundamentally unnecessary. We are not excluding what she wants to be on the list. A matter is

[Matt Warman]

already very much there if it is pertinent to national security. For that reason, I do not think there is a compelling case to add that single topic to the list, both because it is already there and because if we start going down that route, we could make the case for adding a host of other things that are already covered but that people might want to be mentioned specifically.

As I said earlier on the convergence of the two sectors, the point is that we have comprehensive coverage through both Bills. It will be for the NCSC, Ofcom and the Government to make a judgment as to whether any consolidation in a sector poses a national security risk.

Mr Jones: I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Clause 15 ordered to stand part of the Bill.

Clause 16 ordered to stand part of the Bill.

Clause 17

Laying before Parliament

The Chair: We now come to amendment 20 to clause 17. This is Christian Matheson's big moment. I call him to move the amendment.

Christian Matheson (City of Chester) (Lab): I beg to move amendment 20, in clause 17, page 29, line 31, at end insert—

"(4) Where the Secretary of State considers that laying a copy of the direction or notice (as the case may be) before Parliament would, under subsection (2), be contrary to the interests of national security, a copy of the direction or notice must be provided to the Intelligence and Security Committee of Parliament as soon as reasonably practicable.

(5) Any information excluded from what is laid before Parliament under the provision in subsection (3)(b) must be provided to the Intelligence and Security Committee of Parliament as soon as reasonably practicable."

This amendment would ensure that the Intelligence and Security Committee of Parliament is provided with any information relating to a designated vendor direction or designation notice which on grounds of national security is not laid before Parliament, thereby enabling Parliamentary oversight of all directions and notices.

The Chair: With this, it will be convenient to discuss the following: amendment 22, in clause 20, page 35, line 30, at end insert—

"(9) The Secretary of State must provide the Intelligence and Security Committee of Parliament with a copy of any notification under this section relating to a designated vendor direction, designation notice, a notice of a variation or revocation of a designated vendor direction or a notice of a variation or revocation of a designation notice to which subsection (2) or (3)(b) of section 105Z11 applies."

This amendment would require the Secretary of State to provide the Intelligence and Security Committee of Parliament with a copy of any notification under this section which relates to a direction or notice that has not been laid before Parliament on grounds of national security.

Amendment 23, in clause 20, page 37, line 41, at end insert—

"(10) The Secretary of State must provide the Intelligence and Security Committee of Parliament with a copy of any confirmation decision relating to a designated vendor direction, designation notice, a notice of a variation or revocation of a designated vendor direction or a notice of a variation or revocation of a designation notice to which subsection (2) or (3)(b) of section 105Z11 applies."

This amendment would require the Secretary of State to provide the Intelligence and Security Committee of Parliament with a copy of any confirmation decision which relates to a direction or notice that has not been laid before Parliament on grounds of national security.

Amendment 24, in clause 21, page 39, line 9, at end insert—

"(6) The Secretary of State must provide the Intelligence and Security Committee of Parliament with a copy of any urgent enforcement direction relating to a designated vendor direction to which subsection (2) or (3)(b) of section 105Z11 applies."

This amendment would require the Secretary of State to provide the Intelligence and Security Committee of Parliament with a copy of any urgent enforcement direction which relates to a direction that has not been laid before Parliament on grounds of national security.

Amendment 25, in clause 21, page 40, line 6, at end insert—

"(8) The Secretary of State must provide the Intelligence and Security Committee of Parliament with a copy of any confirmation of an urgent enforcement notification relating to a designated vendor direction to which subsection (2) or (3)(b) of section 105Z11 applies."

This amendment would require the Secretary of State to provide the Intelligence and Security Committee of Parliament with a copy of any confirmation of an urgent enforcement notification which relates to a direction that has not been laid before Parliament on grounds of national security.

Christian Matheson: I am sure the Committee has been waiting with bated breath for my big moment all morning, Mr Hollobone. May I say what a great pleasure it is to serve under your chairmanship?

I had prepared some notes to help me present the amendments, but I need not have bothered; I could simply have taken the *Hansard* report from last week and quoted my right hon. Friend the Member for North Durham. He talked about being a stuck record, but he is not; he is being consistent. I like to think that Labour has been consistent throughout the detailed consideration of the Bill. My hon. Friend the Member for Newcastle upon Tyne Central talked about the three areas that we consistently think would improve the Bill, and the amendment falls into one of those areas: scrutiny and the role of the Intelligence and Security Committee.

I refer to my right hon. Friend's speech last week on amendment 9, when he talked about the desire to help the Bill. He also laid down a challenge. He commented on the fact that I thought that some parts of his speech were inspirational. They were, because they made me think quite a lot. There was one lightbulb moment when he used his experience of, I believe, 20 years in the House this year—on which I congratulate him—and said that the chances are that a similar amendment will be proposed in their lordships' House and the Government may well agree to it.

My right hon. Friend also said that it is not necessarily a good thing for the Minister—not in this case, mind you—to be a tough guy who wants to get through the Bill without any amendments, when there is a genuine desire among the Opposition to get the Bill through. I remind the Minister and Government Members that we support the Bill. There have been occasions when an Opposition have tried to scupper, delay or make mischief with a Bill. I assure Government Members—I hope it is obvious to them—that there is no such skulduggery on this side of the House, not with this Bill and not ever, and certainly not when my hon. Friend the Member for Newcastle upon Tyne Central, my right hon. Friend the Member for North Durham and I on the Bill Committee. We are genuinely keen to improve the Bill during its passage.

The amendment again falls into one of the three areas my hon. Friend the Member for Newcastle upon Tyne Central has identified as necessary. As the Minister may have guessed, the chances are that we will not put it to the vote, but we do ask that he gives it careful consideration. I refer the Committee to the speech by my right hon. Friend the Member for North Durham last week about the role of the Intelligence and Security Committee. Amendments 20 to 25 relate to different clauses, but have the common aim of ensuring that there is correct parliamentary oversight of the process outlined in the Bill, specifically by referring all orders made under proposed new section 105Z11 of the Communications Act 2003 to the Intelligence and Security Committee.

It would normally be the Digital, Culture, Media and Sport Committee that would take on telecommunications matters. Additionally, the Secretary of State may lay orders before Parliament for general consideration and scrutiny. However, the Bill has our national security at its heart, and as a proud former member of the Culture, Media and Sport Committee, I am the first to admit that it would not be at all an appropriate forum for the consideration of such reporting to take place, nor would it be the normal procedure for laying orders before this House or the other place, either in general or on the specifics of the order.

As we touched on last week, the temptation is therefore the default position that no reporting at all would take place, which is clearly not desirable. I hope the Minister will confirm that that is not the Government's intention. To be fair, I think he touched on that point last week, but it would be helpful if he could touch on it again.

The use of the ISC is therefore an elegant and obvious solution. The Committee, of which my right hon. Friend the Member for North Durham is such a distinguished member, has worked well and has the confidence of the House. It provides a secure and trusted forum for decisions of the Secretary of State that may have far-reaching commercial and technical implications, as well as security implications, to be scrutinised and considered by hon. Members who are able to receive the full facts and make a judgement based on them, while giving nothing away to those who wish us ill and would exploit our open democracy in doing so. I see no reason why our determination to protect our communications infrastructure should be used against us by our adversaries, but nor should that determination be traded off with a reduction in parliamentary scrutiny of the Executive and agencies that act on behalf of us all.

The ISC is there for a reason: it is precisely to cover situations such as this. If the Minister can propose an alternative solution that balances security with scrutiny, we would be pleased to hear it. I suspect this solution would also make commercial UK businesses more open to scrutiny themselves by offering a level of confidentiality, although I accept that that is not the primary role of the ISC.

It should also not be option for the Secretary of State to report. Such a chaotic patchwork would undermine the integrity of the Bill and the processes that we are setting up. Failing any alternative being proposed, we believe that these amendments, which involve the ISC acting on behalf of the whole House—indeed, the whole of Parliament—would fill a glaring hole and enhance the Bill. I commend them to the Committee.

11 am

Mr Jones: My hon. Friend the Member for City of Chester said that we were going over old ground, and to a certain extent we are because some of the amendments reflect those that I moved last week.

May I say at the outset, Mr Hollobone, that the Minister has been an exemplar in engaging with and briefing the ISC? He has set something of a precedent; usually we have only Cabinet Ministers or Prime Ministers before us to give evidence. He is one of the few junior Ministers to have appeared before us, so I congratulate him. He did it because he wanted to engage with the issues. He must therefore be commended on his commitment to ensure that there is scrutiny. However—this is not to wish his demise, but to argue for his promotion—he will not be there forever. I think he does not quite understand why the Government are not at least moving on this.

The ISC's remit is defined in the Justice and Security Act 2013. It sets out which Departments we cover, and the Department for Digital, Culture, Media and Sport is not one of them. However, as I said last week, security is increasingly being covered by other Departments, and this Bill is a good example. The National Security and Investment Bill is another one, where security decisions will be taken by the Secretary of State for Business, Energy and Industrial Strategy. Parliament must be able to scrutinise that.

If a high-risk vendor is designated as banned from the network by the Secretary of State for Digital, Culture, Media and Sport, there are perfectly good reasons why the intelligence behind that cannot be put into the public domain. The methods by which such information is acquired are of a highly sensitive nature, so it would not only expose our security services' techniques, but in some cases would make vulnerable the individuals who have been the source of that information. I think most people would accept that that is a very good reason.

This sort of thing is happening increasingly. We have the two Bills that I have referred to, but we also have the Covert Human Intelligence Sources (Criminal Conduct) Bill, which will come back to the House tomorrow. Covert human intelligence and the ability to collect intelligence on behalf of our security services is very important. Most of that is covered by the Home Office, and covert human intelligence sources are covered by the ISC's remit and can be scrutinised. However, there is a long list of other organisations that will be covered by tomorrow's Bill, including—we never quite got to the bottom of this—the Food Standards Agency, for example. Again, how do we ensure that there is scrutiny of the decisions?

We also have—this has come out of the pandemic—the new biosecurity unit in the Department of Health. Again, there is no parliamentary scrutiny, because the Health and Social Care Committee will not be able to look at the intelligence that supports so much of that. An easy way out of this is in the Justice and Security Act 2013: the memorandum of understanding, which just means that, were our remit extended to look at this and other matters, the ISC could oversee and ask for the intelligence.

Having spoken to the Business Secretary and the Minister, who sympathises with us, I am not sure where the logjam is in Government. The point is that an amendment will be tabled in the Lords. Whether the

[Mr Kevan Jones]

provision is in the Bill or just in the memorandum of understanding between the Prime Minister and the ISC, it is easily done and would give confidence that the process at least had parliamentary oversight.

On many of these decisions, frankly, the oversight would not be onerous; we are asking only that we are informed of them. On some occasions, we might not even want to look at the intelligence. It might be so straightforward that, frankly, it is not necessary, so I do not think that it is an administrative burden. I cannot understand what the problem is. To reiterate what I said last week in Committee, it is not about the ISC wanting to have a veto or block over such things. It is, rightly, for the Government and the Secretary of State to make and defend those decisions.

It is also not about the ISC embarrassing the Government, because we cannot talk in public about a lot of the information that we receive. It is not as though we would publish a publicly available report, because of the highly classified nature of the information. However, the ISC can scrutinise decisions and, if it has concerns, write to the Prime Minister or produce a report for the Prime Minister raising them. That gives parliamentary scrutiny of the Executive's decisions.

As I say, the report might not be made public. People might ask, "Would that be a new thing?" No—it happens all the time. For example, on the well-publicised Russia report this year, there was a public report with redactions in it and quite an extensive annex, which raised some issues that we were concerned about. That annex was seen only by individuals in Government, including the Prime Minister.

There is already a mechanism, so I fail to understand why the Government want to oppose this. From talking to Ministers privately, I think that there is a lot of sympathy with the position and I think that we will get there eventually. How we get there and in what format, I am not sure—whether the method is to put it in the Bill or to do it through the mechanism in the 2013 Act. That might be a way forward.

Chi Onwurah: I rise to support the excellent comments made by my hon. Friend the Member for City of Chester and my right hon. Friend the Member for North Durham. I did well to delay my remarks till after my right hon. Friend had spoken, because he has set out very effectively, based on his considerable experience as a long-standing member of the Intelligence and Security Committee, both why it is important that that Committee should be consulted and receive the reports, and why it is hard to understand the Minister's reluctance both in this Bill and in the National Security and Investment Bill to involve a source of such credible security expertise and, importantly, security clearance in key issues of national security.

I want to add two points to those made by my right hon. and hon. Friends. The first is to reiterate a point made previously: our security threats are changing, evolving and, unfortunately, diversifying. We see that in changes to our defence spending, in changes in the national review of our defence capabilities, and in changes in the evolution of the geopolitical landscape—the potential source of threats. However, the Minister does not seem able to support reflecting that by ensuring that, rather than keeping to our existing modes of parliamentary scrutiny, we enable parliamentary scrutiny of issues of national security by those who are best placed to carry out such scrutiny—undoubtedly members of the Intelligence and Security Committee.

I want to point briefly to a discussion in the evidence sessions. Ofcom made it clear that it does not consider itself in a position to make national security decisions, which is understandable, and that some of the decisions and considerations about national security with regards to telecommunications networks would require people who have STRAP clearance. Ofcom's group director for networks and communications pointed to the fact that she had had STRAP clearance previously, and she said that if the NCSC

"feels that that is needed for the type of information that we may need to handle, we would make sure that happened."—[*Official Report, Telecommunications (Security) Public Bill Committee,* 14 January 2021; c. 90, Q115.]

To my knowledge, Digital, Culture, Media and Sport Committee members do not have STRAP clearance. I would like the Minister to comment specifically on the level of security clearance required for members of the Committee that he has identified as being the location for scrutiny of important issues of national security. What level of security clearance do its members have? Would that enable the scrutiny that we all agree is in the best interests of the Bill?

I would like the Minister to respond to a specific example. Amendments 20, 22, 23, 24 and 25 are designed to require that the Intelligence and Security Committee has access to the appropriate information. There is a requirement for the Secretary of State to lay before Parliament a copy of a designated vendor direction, as set out in clause 15, which inserts new section 105Z11 into the Communications Act 2003. The new section states:

"The Secretary of State must lay before Parliament a copy of—

(a) a designated vendor direction;

(b) a designation notice;

(c) a notice of a variation or revocation of a designated vendor direction; and

(d) a notice of a variation or revocation of a designation notice."

So far, so good—we have that scrutiny. However, the new section also says:

"The requirement in subsection (1) does not apply if the Secretary of State considers that laying a copy of the direction or notice (as the case may be) before Parliament would be contrary to the interests of national security."

11.15 am

My right hon. Friend the Member for North Durham alluded to occasions when, we can see, that would be the case. I should like the Minister to respond specifically. Imagine, for example, that through the work of our excellent security services we became aware that a telecoms start-up in this country or abroad was under the undue influence of someone hostile to our national interest, and its integrity was compromised, and that those who had come by the information did not want to share with the wider world how they had done so. Indeed, as my right hon. Friend said, sharing that information might compromise the means by which it was acquired. It might also have a significant impact on the stock market price of the company, and perhaps of other companies

or British institutions that were invested in it. That information could not be shared publicly. Yet there could not be an understanding of the reason for the designation notice or effective scrutiny of it by Parliament unless the information was shared in some secure way. Surely that secure way would be sharing it with the ISC.

To take another example, what would happen if the security services became aware that the billionaire owner of one of our major suppliers for, say, cloud services was compromised in some way or that it was going to be bought by a hostile actor? I have previously suggested that I want to understand how the Bill would address the potential for, say, Amazon Web Services to be bought by a hostile actor, and the influence that that would have on our security.

That information would be incredibly security-sensitive, but it would also be market-sensitive. My hon. Friend the Member for City of Chester said that market sensitivity is not the primary reason for the amendments. We prioritise national security. However, let us recognise that questions of national security have a huge impact on our markets as well, and our markets are influential on national security.

Under the clause the Secretary of State would not need to lay a copy of the direction or notice before Parliament if it would be contrary to the interests of national security. Revealing the way we obtain security information through our excellent security services would clearly be contrary to the interests of national security. How would the Minister ensure that there would be an appropriate level of scrutiny for a notice of that kind, which would not be laid before Parliament for reasons of national security? How would scrutiny be maintained?

I look forward to the Minister's response. I emphasise that we support clause 18—*[Interruption.]* I am sorry. We are discussing clause 17.

The Chair: We are.

Chi Onwurah: We support clause 17 and our amendments are intended to make it more accountable to Parliament and therefore more successful and effective in securing our national security.

The Chair: Order. I misled the hon. Lady. We are now discussing amendments 20 and 22 to 25. When we finish the debate on those amendments, we will debate clause 17 stand part. The hon. Lady may want to save this part of her remarks until the next debate.

Chi Onwurah: Thank you, Mr Hollobone. It is sometimes confusing to know exactly what is being discussed at what point. With that, I ask the Minister to respond to our concerns about the scrutiny of the powers in the clause.

Matt Warman: I welcome the second salvo in the campaign to address this matter by the right hon. Member for North Durham. He said it would be an ongoing campaign.

This group of amendments would require the Secretary of State to provide information relating to a designated vendor direction or designation notice to the ISC. The amendments would require the Secretary of State to do this only where directions and designation notices had not been laid before Parliament, whether in full or in part, as a result of the national security exemptions in clause 17. It will not surprise the right hon. Member for North Durham or other Opposition Members that some of these short remarks will overlap with the conversation that we had earlier on a similar matter.

Amendment 20 would require designated vendor directions or designation notices to be provided to the ISC. Amendments 22 to 25 would require the Secretary of State also to provide the ISC with copies of any notifications of contraventions, confirmation decisions and so on. Although I recognise some Members' desire for the ISC to play a greater role in the oversight of national security decision making across government, including in relation to this Bill, the amendments would, as the right hon. Member for North Durham knows, extend the ISC's role in an unprecedented way. None the less, I thank his welcome for my unprecedented appearance.

As I said in the debate on amendment 9, the ISC's primary focus is to oversee the work of the security and intelligence agencies. Its remit is clearly defined in the Justice and Security Act 2013, and the accompanying statutory memorandum of understanding, to which the right hon. Gentleman referred. I do not think he thinks it is my place to take a view on that role, and I do not think this Bill is the place to have that debate.

Mr Jones: Yes, but I would ask the Minister's civil servants to read the Act before they write this stuff for him. The Act refers to "intelligence". Our remit is not fixed by a Department. I know the Minister sympathises with this and that we will get there eventually, but I say to his civil servants, please read the Act.

Matt Warman: I will come on to that. Accepting any of these unilateral amendments to this Bill is not the appropriate place to achieve an overall enhanced role for the ISC—

Mr Jones: I am sorry to say to the Minister that it is not looking for an enhanced role at all. It is actually doing what it says in the Justice and Security Act 2013. It is about scrutinising intelligence. A lot of the information, which will be used by him and others in these orders, will be derived from the same decisions that we oversee .

Matt Warman: Absolutely. Members of the Committee should note that in exercising the powers created by this Bill, the Secretary of State will be advised by the NCSC on relevant technical and national security matters. The NCSC's work already falls within the Intelligence and Security Committee's remit, so the right hon. Gentleman has found his own salvation.

In that context, the amendment seems to duplicate that existing power, while also seeking to do something that is better done in reform of a different Act, if that is what the right hon. Gentleman seeks. I am sorry to disappoint him again. I think he knew already that I would do that, but I look forward to his third, fourth and fifth salvos in his ongoing campaign.

Christian Matheson: I hear the Minister's explanation, which we have been over before when considering other amendments. He talks about other salvos by my right hon. Friend the Member for North Durham. I go back to the statement that my right hon. Friend made last week, which is that he expects that at some point something will happen and we will move forward.

The Chair: Order. If the hon. Gentleman would like to chair this afternoon's sitting, I am sure we could arrange for him to do that. I know Members will be disappointed, but I am instructed to say that as it is 11.25 am, the Committee is now adjourned.

11.25 am

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

Adjourned till this day at Two o'clock.