PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

TELECOMMUNICATIONS (SECURITY) BILL

Sixth Sitting

Thursday 21 January 2021

(Afternoon)

CONTENTS

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

not later than

Monday 25 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

Thursday 21 January 2021

(Afternoon)

[Steve McCabe *in the Chair*]

Telecommunications (Security) Bill

2 pm

The Chair: Before we resume, I have been asked by Mr Speaker to remind people that, when they are not speaking, they should wear a mask. I know this is extremely inconvenient for lots of people, not least me—my glasses steam up. I do not want to be taking names or issuing yellow cards, but may I ask you to try to be mindful of Mr Speaker's concerns and do the best you can? Hopefully we will all be okay.

Clause 1

Duty to take security measures

Amendment proposed (this day): 21, in clause 1, page 3, line 26, at end insert—

'(2A) The Secretary of State must make regulations under subsection (1) requiring providers of public electronic communications networks and public electronic communications services to carry out an audit of the goods, services and facilities supplied, provided or made available for the purposes of the provision of their network or service to ascertain whether they present a risk to the security of that network or service.'.—*(Chi Onwurah.)*

This amendment is a probing amendment designed to learn how the Government plans to ensure network operators have a comprehensive audit of hardware of interest because, for example, it is manufactured by a designated or high-risk vendor.

Question again proposed, That the amendment be made.

Mr Kevan Jones (North Durham) (Lab): I am demasked. Welcome to the Chair, Mr McCabe. It is a pleasure to serve under your chairmanship. The amendment's intention is similar to that of new clause 7, which we spoke about earlier. My hon. Friend the Member for Newcastle upon Tyne Central is trying to probe, like I was, how we get operators to ensure that there is a full audit of their telecoms networks. This is not an easy situation. I accept what the Minister said about trying to strike a balance between prosperity—not wanting to put undue burdens on operators—and ensuring security. As my hon. Friend said, with her huge expertise in the field, these networks are not static entities; they develop over time. The example that she cited was that some of the kit in networks is many years old, which may now create security issues that were not evident when the equipment was introduced.

We are not talking about too onerous a burden on the network operators, because they are large companies. I accept that they will be resistant to anything that adds cost because, at our insistence of wanting cheaper phone calls and mobile technology, prices are competitive between the various operators. My hon. Friend therefore makes a good point that there must be a clear level playing field between the operators.

The Bill will ensure that existing Huawei kit is taken out by 2027, even though the networks did nothing wrong by putting in that kit in the first place. Without wanting to carry on my campaign against the Cabinet Office, the Intelligence and Security Committee's 2013 report "Foreign involvement in the Critical National Infrastructure" shows that the Cabinet Office was made aware of BT's contract with the Chinese company Huawei in 2003. That the Cabinet Office felt it was not important enough to tell Ministers so until 2006 reinforces my point about its role. That brings me to Ofcom and its capacity, which I will come to later. If we want the most robust system, we will need a system by which we know what is in the network.

There are two issues. I think it is possibly easier for future deployments, because we know what we are putting in. In the debate around Huawei and the security risks, I think it has been very clear. Let us be honest: an operator would be very silly to put in a piece of equipment that was deemed to be high risk for any future roll-out. However, as my hon. Friend says, it is what is already in the network. We accept that some of that will be taken out as a result of the Huawei issue, but a huge amount of equipment will still be in there.

That is before we look at software. What saddens me about the entire debate around Huawei and the telecoms sector is that it has been very hardware-centric. We know that the risks to our network from software are greater in some respects; we have seen examples of where network compromise is easier, too. Again, how do we get a robust framework in terms of the audit around software—not just what has already been used, but what will be used in the future?

Chi Onwurah (Newcastle upon Tyne Central) (Lab): My right hon. Friend is making some excellent comments. He has raised another issue, which I perhaps did not highlight in my speech, which is that there might be existing equipment that is not necessarily seen as having a security implication but that, as the network evolves, will pose a security threat in the future. I gave an example in the evidence sessions. Say Amazon Web Services was to be bought by a Chinese company. As our networks move the functionality into the software, that will be running in the cloud over the Amazon Web Services infrastructure, which would have a huge potential security impact. An effective audit of where that equipment is now would be critical to knowing the level of that threat.

Mr Jones: I do not disagree with my hon. Friend. That is why we need to get into the idea of the audit. As I said earlier, we basically need a level playing field for operators; we do not want one to have an advantage over another. We also need a clear picture of what we are asking in terms of the audit. On the point she makes regarding web services and the cloud, there is an issue there that I think is worth referring to. It links today's Bill with the National Security and Investment Bill, which we were discussing yesterday. There was a lot of discussion around what we define as critical—a point she has already raised.

For yesterday's Bill, the question was what is critical to national infrastructure—for example, a company that is developing software that is then acquired by a state that we deem is a security risk to us. If that equipment or software is being used in our telecommunications

network, does that mean that the network is compromised, and how do we guard against that? There are provisions in the National Security and Investment Bill that enable the Government to stop the acquisition of companies that we consider vital to our national security, but unless we know that in advance, how will we make that decision?

If we have a situation where a small company is providing software for part of our critical national infrastructure for telecoms, how will that be joined up? How will we be able to use the provisions in the National Security and Investment Bill, so that the Business Secretary can block the sale? Likewise, how do we get that connection? We can do that only by the Minister and Ofcom having a very clear indication from day one—I do not think it will be possible from day one, but from some time into it—what is in our network, not just now, but into the future. That will be important.

That brings us to the role of Ofcom. We have seen a development of regulators in this country. I am not a great fan of regulators, because I think it is a way for Ministers to palm off their responsibilities to third parties and then stand back and saying, "If it all goes wrong, it is nothing to do with me, guv—it is these independent organisations." A long time ago—perhaps it is a bit old-fashioned—the General Post Office used to be responsible for this type of thing, and I am currently reading the excellent new history of GCHQ that has come out, which I recommend to everyone. It is fascinating to read about some of the challenges—things that apply to this Bill—such as, in the first world war, what was conceived as national security and who was responsible for it. Was it the GPO, the military or someone else?

How will Ofcom be able to look at a network and say, "Yes, we are satisfied that there is nothing in there that is a matter of national security"? They do not know. I do not think for one minute that we are going to have a situation whereby this Government or any future Government will suddenly throw so much money at Ofcom that a huge army of inspectors will be climbing up poles and going into operators' offices to check source codes and so on. That is not going to happen.

From a practical point of view, the operators will have to be responsible for providing that information to Ofcom. Whether it is in the Bill or in the guidance, it must be clear what is expected of operators. It is no good looking back in hindsight and saying, "We should have done that," when something happens. The operators will just say, "You did not tell us we had to do that," or, "We didn't know about that." It has to be very clear, to prevent a competitive advantage between different companies, that there is one standard. They also have to know what we are asking for. Then, taking the telecoms hat off and putting the national security hat on, from the Government's point of view, that needs to be very clear as well, because we need to be reassured that the components and software in those networks, now and in the future, are not a national security risk.

That brings us to an issue that I have already raised. I am not someone who thinks that every time we go to bed at night, we should look under the bed to see whether the Chinese are there, unlike some members of the China Research Group, but there is an issue about the way in which China will look at supply chains as a way of getting access, for two reasons. The first is national security. The second is commercial reasons—dominating the market, which is what China has done with Huawei. How will we identify that, without having some type of audit process? I do not think that everything to do with China is bad, but a huge number of the components in all our mobile phones in our pockets today will have come from China, including Ericsson and Nokia hardware.

James Sunderland (Bracknell) (Con): I am enjoying the right hon. Gentleman's logic. He talks a lot of sense, which is great. I am really intrigued by his insistence that the Government place these obligations on the National Cyber Security Centre and Ofcom. In my humble view, and knowing how those organisations work, it is likely to be the case that the Joint Forces Intelligence Group, GCHQ or the National Cyber Security Centre inform Government where there have been transgressions of security and breaches. I am intrigued by the counter-logic with where I think we need to be.

2.15 pm

Mr Jones: This is a remarkable day. This morning I was told that my contribution to the debate was inspiring, and now I am being told that I am talking sense—I thank the hon. Gentleman for making my day.

The hon. Gentleman is right, but he is also wrong. He is right in the sense that there are threats that will come through GCHQ and others—they will say to operators, "You've got to be careful of these things." Where he is wrong, though, is with the idea that somehow GCHQ can take a guess at what is in the network. It does not have that capability. Going forward—the emphasis in this country, in the Bill, in terms of looking at telecoms security—yes, the bar has been raised substantially.

There will be occasions when GCHQ—it does it already—contacts operators and others to say, "Beware of this software or this thing." I accept that as a proactive approach, but handling backwards will also be important. How do we have a gold-plated system, whereby we have GCHQ doing what the hon. Member for Bracknell suggested they are already doing, but one that also matches up with operators taking responsibility to say, "We have spotted something and are doing something about it"? It is pulling the two things together.

Chi Onwurah: Part of the challenge is that the operators do not know themselves and, as we have discussed, there are no incentives for them to find out. To give an example, Virgin Media took over from NTL, which I think took over from the 13 different cable providers in the franchises of the '80s, and the BT mobile network was bought partially from EE—so there are takeovers and acquisitions, and partners may not know, and do not necessarily have an incentive to find out unless we put in a requirement.

Mr Jones: My hon. Friend makes the point precisely: the way in which telecoms have developed in this country has been piecemeal, only developing now into the four main operators. I hope we will try to get others into the market.

We are to blame for that, as consumers, because we have demanded ever lower prices for our mobile services. Does that suggest that the operators have taken shortcuts? No, I am not suggesting that, but consumer preferences

[Mr Kevan Jones]

have driven down price, and therefore the costs of what those operators provide in delivering the services that we all take for granted. Let us be honest: the Chinese saw the opening door for Huawei—that is why they bought into and flooded the market, putting Government loans behind it. Can we blame the operators for saying, "Well, actually, this is a good deal—we can get good deals"? But they cannot.

I am interested to know from the Minister how, looking forward, we are going to do that. I accept that something will be done under the regulations that the Government will put out, but how will we look backwards as well? As my hon. Friend the Member for Newcastle upon Tyne Central said, there is a lot of legacy equipment there, and it is important for Ofcom to have a clear understanding of what is in the networks.

The Parliamentary Under-Secretary of State for Digital, Culture, Media and Sport (Matt Warman): It is a pleasure to serve under your chairmanship, Mr McCabe.

We are redefining UK telecoms security, but I worry that we are also redefining the aspiration of the hon. Member for Newcastle upon Tyne Central to crack on, so I will try to be brief. The good news that I can deliver, briefly, is how the aspirations of both the hon. Lady and the right hon. Member for North Durham are met in the legislation, and how we envisage those aspirations' being implemented.As the Committee is aware, the Government have published an early draft of the security regulations. Certain draft requirements are relevant to the aims that we have talked about today. If hon. Members look at regulation 3(3)(a), with which they will be familiar if they are insomniacs, they will see a duty for network providers

"to identify, record and reduce the risks of security compromises to which the entire network and each particular function… of the network may be exposed".

That is already there and key to the issues that hon. Members have been talking about.

Chi Onwurah: I had looked at those requirements. I appreciate that they are drafts, but they talk about identifying issues. They do not say "audit".

Matt Warman: I think this would be impossible to identify without carrying out some kind of audit. There is a danger of a semantic argument, but I understand the point the hon. Lady is making. We want people to be in the position to make the kind of identifications that we are requiring. I do not see how they could do that without the records to which she refers, in terms of both the existing kit and future kit that they might put into their network.

Christian Matheson (City of Chester) (Lab): This is an important point. The criticism that I will articulate later is that too much of the Bill is based on an assumption that the players in the sector will automatically do the right thing. For example, there is an assumption of a dialogue between Ofcom and the major players. Will the Minister think about whether he is satisfied that an assumption goes far enough in something as important as this?

Matt Warman: The regulation that I cited is an example of the Government not relying on assumptions. It is an example of us publishing, in advance, exactly the sort of material that demonstrates that this is not assumptions, and that it is there in black and white. That is an important distinction and it demonstrates the cross-party consensus that we have had thus far. We continue to be on the same page in terms of the level of detail required.

The evidence sessions with industry demonstrated that national providers already maintain some asset registers. Witnesses were clear that those registers are maintained and updated as technologies are updated. That is an important part of the existing landscape, but our regulations will ensure this kind of best practice is extended across public telecoms providers.

In addition, the Bill contains measures with regard to the use of particular vendors' equipment. Inspection notices under clause 19 enable Ofcom to carry out surveys of a specific network or service where Ofcom receives a monitoring direction from the Secretary of State to gather information on a provider's compliance with a designated vendor direction. Alongside that, clause 23 enables the Secretary of State to require the provision of information about the use of goods, services or facilities supplied, provided or made available by a particular person. That could be used to require information about a provider's use of a particular vendor's equipment.

Taken together, the issues that have been raised are not only entirely legitimate, in the view of the Government, but are addressed in black and white already, both in the Bill itself and in the drafts that we have published. We are ensuring that "hardware of interest," whatever that might be, is subject to proper oversight and monitoring. That objective does not need the approach that might come as a consequence of this amendment, because it is already there. For that reason, I welcome the probing nature of the amendment. I hope that my answer has satisfied some of the concerns, and I look forward to doing so further in future answers.

Chi Onwurah: It is a pleasure to serve under your chairmanship, Mr McCabe, and I thank the Minister for his comments. I also thank my right hon. Friend the Member for North Durham and my hon. Friend the Member for City of Chester for their comments. This amendment is probing, so we will not push it to a Division. I would like to say two things to the Minister. Although it is true that the providers were confident that they had an asset anywhere their equipment was, other experts who gave testimony in the evidence sessions were not. My experience of networks is that there are multiple systems and this information is not easily accessible or searchable.

I am reassured by the Minister saying that his view is that these requirements could not be met without there having been some kind of audit, to have that information ready. I ask him to write to me, if possible, stating which provisions in the requirements set that out. I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

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

Matt Warman: It is good to reach this landmark point. I do not propose to go over all the ground we have covered, because we have already covered a large chunk of this in discussing the amendments.

As I mentioned, proposed new section 105A means that telecoms providers will need to take appropriate action to ensure adequate security standards and limit the damage caused by any breaches. To support that duty, the proposed new section will create a new definition of "security compromise". The definition is purposely broad. It includes anything that compromises the availability, performance or functionality of a network or service, or that compromises the confidentiality of the signals conveyed by it. That addresses some of the points made by the right hon. Member for North Durham a moment ago. This is a comprehensive approach that will help to ensure providers protect their networks and services properly in the future.

Earlier, I mentioned law enforcement and national security. This part of the Bill excludes certain conduct that is required or authorised under national security legislation or for law enforcement from the definition of "security compromise" in subsections (3) and (4). Those subsections also clarify the fact that, for example, disruption of the use of unauthorised mobile phones in prisons would not be a security compromise.

Proposed new section 105B will give powers to the Secretary of State to make regulations imposing duties to take specific security measures. The power will enable more detailed requirements to be imposed on providers, further to the overarching duty set out in proposed new section 105A(1). This will give greater clarity to providers about the measures that they must take. It will also allow the legal framework to be adapted as new threats arise and technology changes.

These security requirements deliver on our commitment in the telecoms supply chain review to place targeted, actionable and proportionate requirements on a statutory footing. Taken together, the new overarching security duty and requirements will, in secondary legislation, make clear what the Government expect of public telecoms providers. The provisions in the clause are crucial for improving the security of our telecoms infrastructure.

Chi Onwurah: As the Minister says, reaching the end of consideration of clause 1 is a landmark. We are cracking on at a slower pace than anticipated, but it is important that we have rehearsed a number of the arguments that you will hear, Mr McCabe, throughout our detailed scrutiny of the Bill.

Those arguments relate to our concerns with regard to national security, which Labour prioritises, yet we do not see that priority recognised consistently in the Bill; the effective plan to diversify supply chains on which it depends, but which it does not mention; and the scrutiny of the sweeping powers that the Bill will give to the Secretary of State and Ofcom. Those issues all arise in the clause, although we welcome the Bill and the increased duties. Will the Minister clarify the relationship between proposed new section 105A and proposed new section 105B? If he cannot do so now, perhaps he will write to me.

2.30 pm

On the specific duties that the Secretary of State will have the power to require, are they considered updates to the powers in proposed new section 105A—the general duties for all providers—or will they be specific to a certain network provider, and perhaps to a change in its security situation? I do not quite understand why the Secretary of State will have the power to make regulations for specified security measures when he already has the power to require providers to take steps to identify and reduce the risks of security compromises, and there will already be the telecoms security requirements set out in a framework, as he has published in draft.

The Minister looks slightly puzzled, so perhaps he does not see the point that I am making. I am trying to understand what the specific security measures might be. Presumably, they will not already be in the telecoms security requirements, which will have been published, so are they specific to the provider or to some issue that arises—a Russian attack or a SolarWinds attack—or are they simply there as a backstop, in which case why would not the telecoms security requirement be updated regularly, as I think he said it would be, to deal with and address that?

Notwithstanding that outstanding question, we are happy to support the clause.

Matt Warman: I am happy to write to the hon. Lady on the matter she has discussed. We anticipate draft directions in due course that will be network specific, because each network is different, but the overall tenor will be in the same direction. This is probably a matter that we can talk about outside the Committee in a bit more detail to make sure she gets the answers she wants.

Question put and agreed to.

Clause 1 accordingly ordered to stand part of the Bill.

Clause 2

DUTY TO TAKE MEASURES IN RESPONSE TO SECURITY COMPROMISES

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

Matt Warman: We are one thirtieth of the way there. The clause will place a duty on providers to take measures in response to security compromises through proposed new section 105C. When managing security, providers should seek to reduce the risk of security compromises occurring under their duty in proposed new section 105A. As security threats and attacks evolve, it will never be possible for providers to reduce that risk to zero. Therefore, should a security compromise occur, it is crucial that providers take swift and effective action to mitigate its effects. Taking action quickly will also help to mitigate the risk of any further incidents.

Mirroring the approach taken in clause 1, the new duty in proposed new section 105C is overarching and sets out a general duty on providers. It is supported by proposed new section 105D, which will provide the Secretary of State with powers to make regulations requiring providers to take specific measures in response to security compromises of a description specified in regulations. Although it will clearly not be possible to anticipate every security compromise that might occur and to set out how providers should respond, this will enable more detailed provision to be made in appropriate cases. Measures can be specified in the regulations only where the Secretary of State considers those measures appropriate and proportionate.

[Matt Warman]

In practice, the first set of requirements will be contained in a single set of regulations made under the powers of proposed new sections 105B and 105D. A draft of the regulations has already been made available to members of the Committee, and published on gov.uk. Regulations made using this power will give providers clarity about the measures that they need to take, and having those measures set out in secondary legislation has the benefit of allowing the regulations to be reviewed as technology and security threats change over time.

In summary, this duty on providers is an integral part of the new framework, which will ensure providers take control of the security of their networks and services at a time when the UK stands on the cusp of a 5G and full fibre revolution. We must keep those technologies secure to enjoy their full benefit, and the clause is essential to doing that.

Chi Onwurah: We are cracking on: clause 2 is taking but a few minutes. The Opposition recognise the critical importance of our network providers taking responsibility for the security of their networks, and that there can never be a zero-risk network. Given that network communications are ever present in almost every aspect of our life and of our nation's economy and security, it is right and appropriate that the Bill should put requirements in place, both on the operators and in response to specific security compromises.

I should like to have better understood how we would expect network operators to respond to a compromise such as the SolarWinds one, for example, but I expect that the clause will at least place the right duties on network operators, and I am content that it should stand part of the Bill.

Question put and agreed to.

Clause 2 accordingly ordered to stand part of the Bill.

The Chair: This must be down to that productivity seminar they sent me on. Still, nothing lasts forever.

Clause 3

CODES OF PRACTICE ABOUT SECURITY MEASURES ETC

Mr Kevan Jones: I beg to move amendment 6, in clause 3, page 5, line 4, at end insert—

"(ia) the National Cyber Security Centre;"

This amendment would require the Secretary of State to consult the National Cyber Security Centre on any draft code of practice about security measures under new section 105E.

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

Amendment 10, in clause 3, page 5, line 8, at end insert—

"(iiia) the National Cyber Security Centre;"

This amendment requires the Secretary of State to consult the National Cyber Security Centre before issuing a code of practice about security measures.

Amendment 5, in clause 4, page 7, line 41, after "OFCOM", insert—

"and the National Cyber Security Centre".

This amendment would require providers to inform the National Cyber Security Centre, as well as OFCOM, of any security compromise.

Mr Jones: We are romping through the Bill, aren't we? Two clauses in less than 15 minutes.

Again, these amendments are probing. I might sound like a broken record, but my aim with them is to ensure that national security and those who deal with national security decision making are at the centre of the decisions that are taken. Amendment 6 would require the Secretary of State to

"consult the National Cyber Security Centre on any draft code of practice about security measures under new section 105E."

The Minister will say, "Well, it is self-evident that they will do that," but going back to my Robin Day analogy from this morning, legislation needs to survive him, me and everyone else. The guidance will change over time, and we have to ensure that whoever is sitting in the Minister's seat in 10 years' time—hopefully, it will not be the current Minister, not for any unfair reason, but because he has gone on to higher and better things—the onus is on the Secretary of State to consult. Having that on the face of the Bill, or at least some discussion about it, would reinforce that, because the Secretary of State will move on, and there will be new civil servants, who might not have as clear an indication as the Minister will give today, or perhaps a Minister who thinks that this is the key part.

It might be a bit anorak-ish, but the problem with the national security world, which I inhabit occasionally, is that people can see everything through the national security prism—although I am not sure that that is the case for everyone. It will be important to ensure that the individuals at the National Cyber Security Centre have a real input, and not just to say that they will be consulted. The NCSC, which was introduced at the tail end of the coalition Government, is the only positive thing I can think of that that Government did. We now have a world-beating centre that protects our national security and also does a very strange thing: it looks to the secret world, but also looks outwards, engaging with the industry and individual citizens, too.

That is now being replicated around the world. I chair the science and technology committee of the NATO Parliamentary Assembly. On our visit to the UK the year before last, we visited the centre, and most of my parliamentary colleagues from across the world, including the US, were quite impressed with how it balanced complete secrecy about things that need to be kept secret and having that outward-looking approach. I am really just trying to see how we can ensure that going forward.

Amendment 5 seeks to ensure that the NCSC, as well as Ofcom, is informed of compromises and breaches. I am sure the Minister will tell me that Ofcom and the NCSC have such a symbiotic relationship that that information will automatically be transferred, but again we are assuming a lot about what will be done. It is important that this Committee at least discusses how we ensure that that continues. I will come to Ofcom personnel, but various comments have been made. I asked the head of Ofcom about Ofcom's expertise in dealing with these issues, and this comes back to the point I made to that witness. This is about mindset. Whether we like it or not, people in the security world think differently from the rest of us in how they approach things. Ofcom will have a learning curve, not only in recruiting the individuals with the capability to do this work, but in ensuring the culture to react to these issues. My two amendments seek to ensure not only that

national security is at the heart of the Bill, but that practitioners have a clear focus on national security risk.

2.45 pm

Chi Onwurah: I rise to support my right hon. Friend's excellent comments and to add a couple of points on amendment 10, which would require the Secretary of State to consult the National Cyber Security Centre before issuing a code of practice about security matters. My right hon. Friend spoke ably about the amendment's intent to ensure security input on national security measures. That sounds basic, so I hope the Minister will explain why he feels it is unnecessary to make that explicit in the Bill. My right hon. Friend suggested that perhaps it should go without saying, but as we heard in the evidence sessions and have already discussed, the evolving security landscape and the change that the Bill represents, through the new powers for the Secretary of State and Ofcom, make it particularly important to set that out expressly.

The Bill looks at many issues to ensure the security of our networks from supply chains to requirements on network providers as well as raising technical issues, and Ofcom will need to do a lot specifically, so it is important to have a specific reference to the security function of the National Cyber Security Centre.

It came across clearly in the evidence sessions that Ofcom will not be making national security judgments. Lindsey Fussell said:

> "It is important to say that, across the scope of the whole Bill, it is not Ofcom's role to make national security judgments. That is really important. Clearly, that is the Government's and the Secretary of State's role, taking advice from the NCSC and the intelligence agencies."—[*Official Report, Telecommunications (Security) Public Bill Committee,* 19 January 2021; c. 89, Q113.]

In introducing the code of practice, it is essential to ensure that security input and expertise. I do not see why the Minister would object to including such a requirement in the Bill. Unfortunately, we are not always as joined up as we would like to be. There are numerous examples of issues that could have been prevented, had agencies of Government done what might have been expected of them and talked to teach other. As the Bill involves network operations and deep technical and security issues, a requirement to consult the NCSC is particularly important, and that is what the amendment would achieve.

Matt Warman: I apologise in advance, having said that we should crack on, for detaining the Committee for a few minutes on this group of amendments. They relate to clauses 3 and 4, which deal with the codes of practice for security measures and informing others of security compromises. Ultimately, the new telecoms framework comprises three layers. There are strengthened overarching security duties set out in the Bill, there are specific security requirements in secondary legislation, and there are detailed technical security measures in codes of practice. Clause 3 deals with the final layer of the new security framework. Specifically, it provides the Secretary of State with the power to issue and revise the codes of practice and sets out the legal effects of any published codes of practice.

Clause 4 addresses what would happen should there be a security compromise. It puts in place a process for users to be informed of significant risks of a security compromise. The clause also places a duty on public telecoms providers to inform Ofcom of any security compromises with significant impacts, and it creates the power for Ofcom to inform other persons in turn, including users.

I turn now to amendment 5, which seeks to ensure that the NCSC is also informed of security compromises. From a drafting point of view, the NCSC is part of GCHQ, and I take the amendment to refer to GCHQ in that sense. Within the new telecoms framework, the Department for Digital, Culture, Media, and Sport will set the policy direction, Ofcom will regulate and the NCSC will provide technical and security advice. As the UK is an world-leading national authority on cyber-security, we expect the NSCS to share its expertise with Ofcom in order to support the implementation of a new telecoms security framework.

For that reason, the Government absolutely agree that it is crucial that the NCSC receives information about telecoms providers' security. That is why such information-sharing provisions already exist. Under section 19 of the Counter-Terrorism Act 2008, Ofcom or the Secretary of State is able to share with the NCSC any information that would support the NCSC in carrying out its functions. That would of course include the passing on of details of security incidents. Under new section 105L of the Communications Act 2003, which this Bill inserts, Ofcom must report all serious security incidents to the Secretary and State and can pass on information about less serious incidents as well. On receiving such information, the Secretary of State can then share the information with the NCSC, as I have set out. Although these probing amendments are well-intentioned, it is obvious that the provisions are already there.

Chi Onwurah: I thank the Minister for his response to the amendments. He is focusing on the fact that it is possible for information to be shared, but it is not required. I understand that the Bill as drafted, and preceding best practice, means that it is possible for information to be shared. My concern is that it is not required.

Matt Warman: I understand the hon. Lady's point, and I will come to something that I think will address it in a moment. Before I do, I will speak to amendments 6 and 10, as they would be functionally identical amendments to new section 105F in clause 3.

New section 105F sets out the process for issuing a code of practice. It requires a statutory consultation on a draft code of practice with the providers to whom the code would apply, Ofcom and other persons such as the Secretary of State considers appropriate. The amendments would apply an additional requirement to formally consult the NCSC when publishing a draft code of practice. I can reassure the Committee that we will continue to work closely with technical experts at the NCSC, as we have done over a number of years.

The telecoms supply chain review demonstrated the Department's capability to work with our intelligence and security experts to produce sound recommendations, backed by the extensive and detailed security analysis that I know Members of all parties would like to see. That initiated the next phase of the collaborative work that culminated in the introduction of the Bill, and the codes of practice continue that theme. The purpose of such codes is to provide technical security guidance on the detailed measures that certain public telecoms providers should take to meet their legal obligations.

[Matt Warman]

We have already been clear that NCSC guidance will form the basis of an initial DCMS-issued code of practice. The NCSC has already developed a set of technical measures that is in the process of being tested with the industry, and those technical measures have been refined and improved over the last two years. The NCSC will continue to update the measures to reflect any changes in the landscape of threats, as the right hon. Member for North Durham described, and the relationship between the work of the DCMS and that of the NCSC means that such changes would be reflected in the code of practice. Alongside the DCMS and Ofcom, the NCSC will play a key role in advising public telecoms providers on how to implement detailed codes of practice.

Mr Jones: I agree with the Minister, in the sense that I think he and the Secretary of State at the DCMS are committed to there being very close working, but as I said, he ain't gonna last forever. An issue will come up —in fact, it came up last night on the National Security and Investment Bill—when operators and others say, "Actually, from a commercial point of view, this is more paramount," or, "This is what we should be doing." The Secretary of State will come under a lot of pressure to perhaps look at prosperity issues rather than security issues. I just wonder whether, without the relevant provision in this Bill, a future Secretary of State could say, "Well, I'm going to ignore that issue, because I want to pander to"—well, not pander to—"accept the commercial and prosperity arguments."

Matt Warman: The right hon. Gentleman keeps going on about ministerial impermanence, but I will not take it personally.

Mr Jones: I talked about promotion.

Matt Warman: Too kind! The key part to this is that, obviously, Ofcom remains an independent regulator and will be working closely with others. The right hon. Gentleman makes a fair point about the inevitable balance between national security and a whole host of other issues, but ultimately that independence is absolutely essential. In the light of our long-standing and established working relationships across the DCMS, NCSC and Ofcom, it seems reasonable to say that there is a track record demonstrating what he has asked for. But given the Committee's interest in the role of the NCSC in this regime, I will just make one last point. Its role is not explicitly described in the Bill, as the NCSC already has a statutory remit, as part of GCHQ, to provide technical security advice and to receive information on telecoms security for the purpose of exercising that function.

The NCSC and Ofcom will very soon publish a statement setting out how they will work together. I think that addresses some of what the hon. Member for Newcastle upon Tyne Central mentioned; I believe she has some familiarity with Ofcom. I think it is right, because they are independent, that that statement comes from them, as well as the Government expressing a view on this. The statement will include information on their respective roles and their approach to sharing information on telecoms security, and it should provide greater clarity, which hon. Members are entirely legitimately asking for, about the NCSC's role, including how it will support Ofcom's monitoring, assessment and enforcement of the new security framework.

I hope that the sorts of matters that I have talked about provide the kind of reassurance that Members have asked for.

Mr Jones: A statement is a welcome step forward, but—the Minister can write to me on this; he need not respond to me today—what is its legal weight? Again, I am not wanting to consider the Minister's demise, but I would like to know that future Secretaries of State and Ministers will use it as the template and will not be able to say, "Well, we are going to ignore that statement." That would be very welcome, because it would bind the two organisations together, which is important, and ensure that the security aspects were taken into consideration, but will the Minister just write to me, saying what weight the statement would have? I have to say that I sympathise; I do not like Christmas tree Bills that start having things added on. If it could be done in a complete way, I would be quite happy with that. The only thing that I want to know is, basically, what its status will be in future. I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

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

3 pm

Matt Warman: The Committee has already heard me talk about some of this, but I think it important to provide a little more detail. The code of practice, which we have discussed, is a fundamental building block of the regime and will contain more specific information on how telecoms providers can meet their legal duties. It will provide guidance on how, and to what timescale, certain public telecoms providers should comply with their legal obligations, and will be based on technical analysis by the NCSC. Individual measures will therefore reflect the best protections against the most pressing threats to network security. The code will, for example, set out the detailed technical measures that should be taken to segregate and control access to the areas of networks that process and manage customers' data.

We recognise of course that different companies have different ways of setting up and running their networks, and because our telecoms market is dynamic and competitive, providers range in scale from multinational giants such as Vodafone down to innovative local start-ups. We want therefore to ensure that the code of practice is proportionate, and that public telecoms providers take appropriate security measures.

I will touch as briefly as I can on how we intend to achieve that proportionality through a tiered system. Tier 1 will contain the largest national-scale public telecoms providers. Should any of those providers have a significant security incident, it could bring down services to people and business across the UK. Those operators will have the greatest level of oversight and monitoring from Ofcom. Tier 2 will contain medium-sized public telecoms providers. Those providers may not be as large, but in many cases they are critical to regions and to business connectivity. They are expected to have more time to implement the security measures set out in the code of practice.

Tier 3 will contain the smallest public telecoms providers, including small businesses and micro-enterprises, which, of course, must also comply with the law. They are not anticipated to be subject to the measures in the code of practice, but will need to comply with their legal duties as set out in new sections 105A and 105C, and in any regulations. Our expectation is that Ofcom would regulate those providers more reactively.

New section 105F describes the process for issuing a code of practice. When the Government publish a draft code of practice, we will consult with industry, Ofcom and any other appropriate persons. Specifically, publishing the first code of practice will include consulting on the thresholds of each of the tiers that I have described and on the timings for their implementation. Following the consultation period, and once the code is finalised, it will be published and a copy will be laid before Parliament.

New section 105G gives the Secretary of State the power to withdraw a code of practice. Again, that will follow consultation with industry and Ofcom. A notice of withdrawal will be laid before Parliament. The legal effects of the code of practice are described in new section 105H. To be clear, the code of practice is guidance only; it is an important tool that operators should use to comply with their legal duties.

Mr Jones: Is the Minister saying that the code of practice is the standard that providers are expected to meet? Is it the legal bare minimum or do we expect them to do more than what is set out in the code of practice? What is the direction of travel?

Matt Warman: The legislation places a duty on providers. Meeting the strictures of the code of practice would be the way of demonstrating that they were meeting that duty as an initial step, but of course, we see individual companies making decisions, for a host of reasons, to exceed codes of practice in every area of regulated life,

and I would expect that to continue in the area in question as well.

Where relevant, provisions in a code could be taken into account in legal proceedings before courts or tribunals, which I think gives some sense of their status. That would include any appeals against Ofcom's regulatory decisions heard by the Competition Appeal Tribunal. Ofcom will take account of the code of practice when carrying out its functions as required in new section 105H(3) in relation to telecoms security, as I have just described.

Under new section 105I, if Ofcom has reasonable grounds for suspecting that a telecoms provider is failing, or has failed, to act in accordance with a code, it can ask public telecoms providers to explain either how they meet the code of practice or, if they do not meet it, why. For example, if the network set-up of a particular telecoms provider meant that it could achieve a level of security equivalent to that in the code by other means, it could explain that in its statement responding to Ofcom. In such a case Ofcom might be satisfied that the provider was complying with its security details, but hon. Members will see that we are again trying to ensure a proportionate approach to the relevant part of the framework.

We believe that the code of practice will provide an appropriately flexible framework, which will be able to change as new security threats evolve, providing clarity for telecoms operators on what is required of them by this new telecoms security framework.

Chi Onwurah: I will not detain the Committee very long either, as we agree about the importance of codes of practice. I will not say that I am entirely reassured to hear of the statement being issued by Ofcom and the NCSC on how they will work together, but I certainly think that it is a positive development, and I hope we will be able to see it before the Bill progresses to the House.

On the codes of practice, as my right hon. Friend the Member for North Durham set out, it is important that the sector should understand the standard to which it will be held. I have some concerns about the tiering system, because, as was made clear by a number of witnesses during the evidence sittings, all networks are joined up and we are only as secure as the weakest link. At the same time, it is important to have a proportional burden on new entrants as we indeed hope to diversify the supply chain.

I understand, although perhaps the Minister can clarify the point, that the codes of practice will not refer to the diversification of the supply chain, despite the fact that having a secure network—we shall debate this in more detail—is dependent on having a diverse supply chain. I have made the point a number of times, and will make it repeatedly, that the lack of linkage between the diversification strategy, implementation and the security of our networks is an ongoing cause for concern. However, having made those comments, I do not object to the clause.

Question put and agreed to.

Clause 3 accordingly ordered to stand part of the Bill.

Clause 4

INFORMING OTHERS OF SECURITY COMPROMISES

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

Matt Warman: As with clause 3, I have already spoken to clause 4, addressing an amendment on this issue. It will be crucial that we ensure that the Government, Ofcom, public telecoms providers and their customers have the information that they need to understand when security compromises have occurred, and then use the knowledge to prevent compromises in the future. New section 105J requires that providers inform their users of significant risks of security compromises and actions that they can take to avoid or mitigate any adverse consequences.

We want to ensure that this is done in a transparent and open way, so the clause specifies that telecoms users should be notified in clear and plain language, and given a named contact they can get in touch with if they have any further questions. Giving users that information will help to ensure that, where possible, they can take swift action to protect themselves and raise broader awareness.

New section 105K requires security compromises to be reported to Ofcom. That information will provide Ofcom with insight into the security of individual telecoms providers and security risks across the landscape, enabling us to target its regulatory action more effectively. The Bill also requires that providers report pre-positioning attacks on the network. These are attacks that do not affect the network or service at the time but allow access

[Matt Warman]

that could result in further security compromises. These attacks pose real risks but too often remain invisible to a regulator.

Finally, under new section 105L, Ofcom is required to share information about serious security compromises with the Government. It may also share information on less serious compromises if, for example, it would help the Government with developing telecoms policy and future regulation.

The clause explains how Ofcom can share information about security compromise with other groups and organisations, and the Bill allows information sharing at Ofcom's discretion with overseas regulators, other providers, telecoms users and, where appropriate, the wider public. It allows Ofcom to advise network and service users of the measures that they should take to prevent, remedy or mitigate the effects of the security compromises, to direct providers to give such advice themselves.

The clause ensures that the regulator has access to the information that it needs, and will help to ensure that the entire industry is aware of new and evolving risks and can respond accordingly—be that a customer changing their password or an operator tightening its defences against a new attacker.

Chi Onwurah *rose—*

Matt Warman: I will pretend I have not finished, and give way to the hon. Lady.

Chi Onwurah: I thank the Minister, as always, for graciously giving way. I will make this point later, but I want to give the Minister the opportunity to consider how the requirement for Ofcom to notify users might work with the Information Commissioner's requirement on data controllers to also notify users when there is a data hack.

Matt Warman: Obviously, there could be an overlap in those notification requirements, but our expectation would not be that anyone would receive multiple notifications. That is why there is an emphasis on the nature of communications being clear and obvious to laypeople.

Mr Jones: Speaking gives me an opportunity to take my face mask off. I will make a few points about clause 4, which is broadly welcome because it clarifies for operators what their responsibilities are, not just from a national security point of view but from a consumer point of view. I think there is an issue, though, which my hon. Friend the Member for Newcastle upon Tyne Central raised.

Again, I do not want the Minister to respond now, but I think the crossover with the Information Commissioner might be one area that we need some clarity on. Is there an example of this? Yes—the TalkTalk case. People might look at this Bill and think national security is about the Russians or the Chinese hacking, but that was a criminal act that led to a lot of people's data being compromised. From a constituency point of view, as any Member of the House at that time will know, trying to get TalkTalk to do anything about that, in terms of the losses that people incurred, was virtually impossible. That is why these clauses are so important.

Chi Onwurah: Is my right hon. Friend aware that the hack used by the young person had been around for longer than that young person had been alive? That is an indication of the low level of security TalkTalk had in their network; they had not been able to address a known hack that had existed for at least 16 years. The Bill aims, in part, to address that and the consequences of that lack of security for our constituents.

3.15 pm

Mr Jones: My hon. Friend is correct. A lot of the debate has been about hardware, but the biggest threat to our national security, in terms of telecoms, is from hacking and cyber-attacks. The changing nature of the threat is interesting. There are state actors and there is organised crime, acting on of behalf of states, but there is also, as referred to by my hon. Friend, some poor teenager who thought it was a good idea. The TalkTalk case showed the emphasis they put on the security of their network. Not just clause 4, but the whole Bill, puts the onus on the operators, which is why it is so welcome. Never again could they be accused of not knowing their responsibilities.

New section 105J requires providers to take "reasonable" steps to inform users about the risk, the nature of the security compromise, the steps the user could take in response, and the name and details of the person to contact. That is fine, but how to respond might be a matter for Ofcom. That is important, because people might then quickly take steps to stop compromises to their security.

The Bill lays out penalties for telecoms operators, but what about the consumer and people who have lost money because of data breaches? Do I assume that the Bill does not change that? It beefs it up, but I assume that any mitigation or compensation that should be paid to individuals who have been compromised would be an issue for Ofcom. When we had the TalkTalk compromise, getting TalkTalk to do anything was like trying to get blood out of a stone. That is important from the point of view of consumers.

It is important that the Secretary of State is informed, but how will that be done? I presume GCHQ and others would do that. Would that lead to lessons learned or to a notice being given to other operators that that has happened? Would that be done by Ofcom, the National Cyber Security Centre or GCHQ, or would it be a combination of all of them? It comes back to the point made by my hon. Friend the Member for Newcastle upon Tyne Central: this is a risk and this clause puts the onus initially with the operators, where it should be.

Chi Onwurah: We are cracking on at such a pace that I lost my place somewhat. I had forgotten that we are now discussing clause 4. My apologies, Mr McCabe.

My right hon. Friend the Member for North Durham has already addressed some of the points that I wanted to make, but let me say that we welcome the duty being placed on providers to report security incidents. I have long campaigned, in relation to cases such as the TalkTalk incident, to make that duty clearer and more comprehensive regarding the information that needs to be shared with users and those who are affected, and for them to have some kind of right of redress, which is effectively part of the Bill.

I welcome the requirement in clause 4 to inform others of security compromises, but will the Minister provide more clarity? There is some indication of the range of actors that the providers and Ofcom must inform, but I do not feel that there is an understanding of the level of information that will be shared with different actors. For example, if the public are to be informed of a security breach, compared with the requirement from the Information Commissioner's Office, which, as I said, actually goes far enough, what level of information might be shared with other actors, such as other networks? My right hon. Friend talked about who else might be informed. It is also clear that the sharing of information will probably need to evolve over time, as the nature of compromises and their potential reach changes. I wonder how these requirements might be adapted to reflect that.

I will just say a little about the sharing of information with overseas regulators. If that is clearly set out in the Bill, I am unable to find it. Presumably, such data sharing will still have to conform with the requirements of our data protection legislation. Will it also reflect international data-sharing gateways for criminal prosecution purposes?

Those are just some general comments. We welcome the clause.

Matt Warman: I will reply briefly. On the point about compensation, essentially new section 105W of the Communications Act 2003, which is inserted by clause 8, covers the civil liability point, which I think opens the door that the right hon. Member for North Durham seeks to open. Then there are the notifications to industry of what is essentially best practice and recent threats. Of course, as he implied, there is a balance to be struck with the existing work of all those involved, but ultimately it would feed into the codes of practice, so there is both an informal and a formal mechanism, if I can put it like that.

On the hon. Lady's final point about the international sharing of information, it would depend on the nature of the information, as she implied. Some of it would pertain to national security, and some of it would pertain to the kind of criminality that she has spoken about about, where there are existing provisions as well. In that sense, of course, it is all covered by our own data protection regime, which has the sorts of carve-outs I have just described but operates in that holistic framework.

Mr Jones: Will the Minister write to us on the issue of data and the link to the Information Commissioner?

Matt Warman: I am not sure I fully understand the right hon. Gentleman's point.

Mr Jones: I raised the point, as did my hon. Friend the Member for Newcastle upon Tyne Central, that we are asking operators to inform individuals about data compromises. That is welcome, but as my hon. Friend said, there might also be a breach of the Information Commissioner's regulations, and we just wanted to get some idea of how the two would mesh together. I do not expect the Minister to know now, but could he write to us to say how the two would interact?

Matt Warman: As I said in response to the hon. Lady, there is obviously a potential overlap. The focus of this Bill is on clarity of communication to the consumer, but I am very happy to write to the right hon. Gentleman or the Committee with further details of that potential overlap.

Chi Onwurah: The Minister is being incredibly generous with his time. To clarify what we are hoping to receive, as he has indicated, we would not want the ICO to be sending out notifications to 2 million people who had been affected by a hack, and Ofcom to be doing that as well. We would expect there to be co-ordination in that regard, and we would just like to see that set out.

Matt Warman: I am very happy to do so. I think it is obvious that clarity of communication would be incompatible with duplication.

Question put and agreed to.

Clause 4 accordingly ordered to stand part of the Bill.

Clause 5

General duty of OFCOM to ensure compliance with security duties

Christian Matheson: I beg to move amendment 11, in clause 5, page 9, line 41, at end insert—

"(2) Providers of public electronic communications networks and public electronic communications services must notify Ofcom of any planned or actual changes to their network or service which might compromise their ability to comply with the duties imposed on them by or under sections 105A to 105D, 105J and 105K."

This amendment would require providers of public electronic communications networks or services to notify Ofcom of any changes to their network or service which might compromise their ability to comply with their security duties.

It is a great pleasure to serve under your chairmanship, Mr McCabe. Since this is my first substantive contribution to the Committee, I pay tribute to the Front Benchers. It is nice to have a Minister who, I believe, was formerly a tech journalist specialising in telecoms, and who knows the subject well. Of course, the shadow Minister, my hon. Friend the Member for Newcastle upon Tyne Central, was a telecoms engineer and an Ofcom regulator for many years, and I pay tribute to her and her staff. The Committee should know that in addition to running this Bill Committee from the Opposition's side, she has also been working in the main Chamber this week on the National Security and Infrastructure Bill Committee. Juggling two Bills at once is no mean feat.

I have also greatly enjoyed the interplay between my right hon. Friend the Member for North Durham and the hon. and gallant Member for Bracknell, both of whom have considerable national security experience. I was intrigued by my right hon. Friend's estimation of the hon. and gallant Gentleman's intervention as Schrodinger's intervention—one that managed to be simultaneously right and wrong. He has set a new standard there.

From listening to the debates on previous clauses, it is clear that a common thread passes through the Bill, which we in the Opposition have been hoping to link up. Partly, it is to do with the question we raised earlier about the assumption that everybody understands exactly what the intention in the Bill is, and that everything will be all right in the long term. My right hon. Friend the Member for North Durham has talked about the importance of making things as clear as possible when it comes to responsibilities, because a future Minister

[Christian Matheson]

might not be as adept in this subject as the hon. Member for Boston and Skegness, who currently occupies that position. In a sense, that is the heart of amendment 11.

3.30 pm

Clause 5 asserts a general duty on Ofcom to assure compliance with security details. Much of the detail required under this clause is specified in the next one, clause 6. Obviously, we welcome the clause, which lies at the heart of the purpose of the Bill and underpins the powers and responsibilities given to the regulator. The amendment shares some responsibility with the network providers, which must surely also have a duty to maintain a running assessment of security—something that I am sure that they must try to do already, but which still requires scrutiny. The historical context is clear because, as my hon. Friend the shadow Minister and my right hon. Friend the Member for North Durham have talked about, BT sold off a chunk of its network to Huawei and did not formally inform the regulator or the Government of its intention to do so until a couple of years after the event.

In the evidence sessions, we heard varying views on the ability of network providers to assess their networks, equipment and software for compliance with the proposals before the Committee today. All the main network operators gave confident answers regarding the integrity and reliability of their asset registers when it comes to equipment and presumably—but only presumably—the software that drives it. The impression was clear that, at the top level, work had already been undertaken on making an assessment of what assets would need to be replaced before the 2027 deadline, and where the operators were on that. We welcome that.

Some later witnesses, however, while not entirely contradicting that certainty, suggested that the task would not be so easy. We heard about overlapping 2G, 3G, 4G and 5G networks, with different equipment of different ages. My hon. Friend the shadow Minister gave a shocking statistic in relation to the age of the equipment that was responsible for the insecurity that led to the TalkTalk hack. I describe that overlapping network as sounding to non-experts—such as me, I hasten to add—like a bowl of spaghetti.

We therefore accept that any assessment is a complicated task, and we recognise the work that providers have undertaken and will continue to undertake to make good the security of the networks, but several problems remain. First and foremost, any audit or asset register is simply a snapshot at the moment. When national security is at stake, an accurate, up-to-date and rolling picture and assessment must be available. It is better to know in advance where problems might occur.

Any business faces commercial pressures, and although I have confidence that no British provider will ever take risks with our nation's security, the obligations outlined in the amendment will provide clarity and certainty as to which side of the line they should fall in any situation where doubt occurs about whether they ought to discuss potential issues with Ofcom. I think my right hon. Friend the Member for North Durham was hinting at some of those pressures when in the previous clause he mentioned the TalkTalk hack and some of the commercial pressures that companies are under.

Another issue is the relationship between Ofcom and the companies that are being regulated —the network and service providers—because Ofcom it at once a regulator, necessarily with a stick in hand, and a partner agency that is hoping to support the service providers to meet their obligations. We hope that the amendment will provide a little bit of clarity in order to make that partnership more even.

The amendment encourages a rolling conversation with Ofcom, with those matters at the forefront. I assume and hope that that will be happening anyway but, as I have said already, assumption is no basis on which to proceed in legislation. The amendment therefore provides clarity on a sense of obligation. It would also help providers to address problems at the outset and to have the knowledge, as far as possible, but they are likely to be complying on security under the regulations, rather than finding themselves in a situation where they have to comply with the duty under the sections mentioned in the amendment only after the fact and only after work has been done.

Finally, clause 5 puts an obligation on Ofcom, but Ofcom cannot be blamed for not knowing something that it does not know and so failing in its duties under clause 5. The amendment, by sharing the responsibility with the network providers, would assist Ofcom in its duties of overseeing the networks and, I hope, foster more of a partnership when addressing the problems, in the interests of the nation.

We have to avoid providers doing first and telling Ofcom later, because the avoidance of problems is greatly to be preferred to enforcement action further down the line. We have to make things easy for Ofcom. The regulator is growing in scope and complexity, as my hon. Friend the shadow Minister has said, and national security responsibilities are still fairly novel for Ofcom. That load has to be shared, and the amendment provides a focus for providers to assist.

I was a little concerned by suggestions during the evidence sessions that it gets harder to verify security and compliance the further we go down the supply chain. The focus on national security has to be baked in. With a chip here or a piece of software code there which might have been carried forward from a previous or separate piece of equipment, as my right hon. Friend the Member for North Durham has said, it has to be the responsibility of the suppliers and ultimately the network providers not to make any assumptions, but to query every aspect of their asset register and propose changes to it to maintain their duty of security and compliance under sections mentioned in this amendment.

We heard expert testimony during the evidence sessions. Dr Drew said:

"On having providers be more proactively involved, I think it would make complete sense for these actors to be made to inform Ofcom, or whichever regulator is chosen, of significant changes to their supply chains."—[*Official Report, Telecommunications (Security) Public Bill Committee,* 19 January 2021; c. 83, Q101.]

Andrea Donà said:

"We need a clear understanding between Ofcom and us as providers before the legislation is enforced, so that we understand exactly the boundaries and the scope, and we all work together, having done the audits, to close any vulnerabilities that we might have. That is a clear aspect of our working together: ensuring that the assets in the telecoms network infrastructure that are in scope are very well defined."—[*Official Report, Telecommunications (Security) Public Bill Committee,* 14 January 2021; c. 16, Q14.]

The amendment is simple and straightforward, sharing the obligation on security and allowing for a forward-looking assessment by Ofcom and network providers to give the assurance that we need and to head off problems before they arise. It is about being forward-looking and not always being reactive. I commend it to the Committee.

Chi Onwurah: I rise simply to support the excellent speech made by my hon. Friend the Member for City of Chester. I thank him for his very kind words. In the amendment, he makes an important contribution in ensuring that Ofcom knows what it needs to know and in putting the onus more firmly on the network providers. I simply ask the Minister to respond to the points that my hon. Friend made in his concluding remarks about being forward-looking.

A challenge for us as a nation in securing our networks during such fast-paced technological change is looking backwards to the problems we have had rather than forwards to the evolving and new threats. During the evidence sessions, we were accused of fetishising 5G as if that was the only security challenge, because of the visible problem with Huawei, and that we were not looking more broadly. I admired Ofcom during my time there because it was set up to be a forward-looking regulator. To achieve that aim, when it comes to the sweeping new requirements around security that are placed on it under the Bill, it needs to be able to see what changes are happening and are likely to influence future evolving threats. To do that effectively, amendment 11 requires the network providers to notify Ofcom of planned or actual changes.

It is worth remembering that—I made this point earlier—if BT had been required to notify Ofcom or another body of changes to its network as Huawei moved to a greater and more dominant position in its network, that might have rung alarm bells more generally. We have also already mentioned the shift that we are seeing on the importance of software and software configuration and services in controlling the network. Requiring providers to notify Ofcom of planned or actual changes to the network would make that evolution more easily visible and therefore provide Ofcom with greater visibility of how all our networks are evolving and what new threats may arise as a consequence.

Matt Warman: The amendment would add to the general duty in clause 5 that places on Ofcom the duty to ensure that providers comply with their security duties. The duty as written in the Bill makes clear Ofcom's increasing role. The duties imposed on public telecoms providers in the Bill are legally binding, so as the Bill is written providers should not be taking decisions that would prevent them from complying with those duties in the future. If they were not to comply, they would be in breach of their legal duties and liable for enforcement action, including the imposition of the significant penalties set out in the Bill.

The underlying purpose of the amendment—that Ofcom should take a proactive role in regulating the regime—is already core to what is in the Bill and the Government absolutely agree with the principle that the hon. Member for City of Chester set out. We need to ensure that Ofcom has the tools to be forward-looking so that, in a world of fast-changing technologies and threats, it can understand where operators are taking their networks and how that will affect their security. That is an absolutely essential part of the Bill.

James Sunderland: Does the Minister agree that the Bill in its current form is prescriptive enough already?

Matt Warman: I think the Bill is perfectly drafted down to every comma and punctuation mark. To be slightly more serious, what we have sought to do in the drafting is to strike the balance between proportionate regulations and the overarching requirements for national security. That is the balance that we have struck and it is exactly for that reason that we already do in the Bill what the hon. Member for City of Chester and the shadow Minister seek with the amendment.

In section 135 of the Communications Act 2003, as amended by clause 12, Ofcom is already allowed to require information from providers about the future development of networks and services that could have an impact on the security of the network or service they are providing. That would enable Ofcom, for instance, to assess the security risks arising from the deployment of a new technology or from the proposed deployment of a new technology. For those reasons, I hope that the hon. Members are reassured not just that the Bill does what they seek, but that previous drafts of the Communications Act already did so.

Chi Onwurah: I thank the Minister for giving way; in doing so, he shortens what I will say later. I think the Minister is saying that Ofcom has the power to require information, which is true, but the amendment is about providers proactively giving that information. Ofcom cannot request information about a change to the networks that it does not know is happening. I am hoping that perhaps what the Minister is implying is that he would expect Ofcom regularly to review what was changing in the networks and therefore make those requests for further information. Could he clarify that point?

Matt Warman: The sort of horizon scanning that the hon. Lady describes is core to all essential regulation, and the relationship that Ofcom has with those whom it regulates promotes the ability to have such conversations. But as I said, the key point is that an operator that proposes knowingly to introduce a risk into its network would clearly not be complying with the statutory provisions of the Bill. That is the essential nub of the issue.

3.45 pm

Christian Matheson: I am most grateful for the debate on the amendment. My hon. Friend the shadow Minister made the key point that Ofcom cannot be blamed for not enforcing something that it does not know anything about. The amendment's intent was to encourage a sense of shared responsibility in what my right hon. Friend the Member for North Durham reminded us is still a competitive industry in which businesses might want to maintain a level of confidentiality about technological changes or the deals they are doing with suppliers. However, if the Minister is satisfied that that is covered in other parts of the legislation, I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Clause 5 ordered to stand part of the Bill.

Clause 6

POWERS OF OFCOM TO ASSESS COMPLIANCE WITH SECURITY DUTIES

Christian Matheson: I beg to move amendment 12, in clause 6, page 10, line 12, at end insert—

"(3) In this section "another person" means a UK government agency or a person from a UK government agency.

(4) OFCOM may not incur costs exceeding £50,000 in carrying out, or arranging or another person to carry out, an assessment under this section.".

This amendment restricts those who Ofcom may arrange to carry out an assessment under this section to a UK government agency or person from such an agency. It also caps the cost of an individual security assessment at £50,000 for Ofcom.

The desire of the Committee is to crack on, so I will not detain us for too long. The clause, which covers more than three pages of the Bill, is extensive in outlining the powers of Ofcom to assess compliance with security duties and will amend sections of the Communications Act 2003 to that end. The Opposition's probing amendment intends to bring clarity in two areas in particular.

The clause will insert proposed new section 105N into the Communications Act to give authority to Ofcom or "another person" to undertake an assessment of whether a network or service provider is carrying out its duties—an inspection, spot check or audit, whatever you will, Mr McCabe. That is all fine, but the appointment of "another person" is far too vague and needs clarity. Since this is a matter of national security, we believe such an authority can be vested only in an agency or arm of the UK Government. It would be wholly inappropriate to outsource it to a telecoms, IT or other consultancy in part because of the need for full co-operation from the business being audited, which must have absolute confidence to be open and transparent and, therefore, must have confidence in the inspector. Ofcom therefore cannot appoint any Tom, Dick or Harry to do the job but only someone who rides above the industry and will not give the inspected business any reason to think that its commercial confidentiality is at stake.

My hon. Friend the Member for Newcastle upon Tyne Central, with her extensive experience of the telecoms sector, has told me that it is a tight-knit industry in which everyone has worked for everyone else at some point. We got that impression from the oral evidence as a lot of the experts had worked with or knew one another. Perhaps it is an exaggeration to say that everyone has worked for everyone else, but it is illustrative of the nature of the sector, so there will be limits on who could be appointed. Does the Minister agree that the current suggestion of "another person" is too wide?

Chi Onwurah: Will my hon. Friend give way?

Christian Matheson: Always.

Chi Onwurah: The impression that I have given my hon. Friend about the telecoms sector being tight-knit is absolutely right. One concern that that brings is that there will therefore be conflicts of interest. Ofcom, as a public servant with the status of a quango, has rules and regulations for declaring interests that mean previous conflicts of interest will not weigh into its work. The concern that I have articulated to my hon. Friend in the past is that that would not apply to "other persons", so broadly defined.

Christian Matheson: I am really grateful for that intervention—not just for the context that my hon. Friend gave, but for prompting me to think that having such a tight-knit sector, and the character of the sector, works both ways. Ofcom might appoint as an inspector to undertake one of the audits somebody who is on very good terms with the business or the provider. They will perhaps take their foot off the pedal and not do quite as thorough an investigation, because they know the business and trust them. As a result, the inspection would not be as thorough.

Mr Jones: My concern is also that the Government do not have a good track record on applying the standards that have been developed over many years to ensure proprieties in public appointments. No doubt somebody who would fit the bill for the role would be Dido Harding, who was responsible for TalkTalk and is now having huge success, as we have been told by the Prime Minister, with Test and Trace. She seems to have a common thread, but success does not seem to be part of that.

Christian Matheson: Who am I to disagree with my right hon. Friend and his years of experience? So far, we have been fairly consensual in this Committee, because we want the Bill to pass. My right hon. Friend is absolutely right: we have seen a certain level of—

Mr Jones: Chumocracy.

Christian Matheson: I was going to say cronyism, but chumocracy is a far nicer way to put it, and we have seen it in the way consultancy contracts have been dished out during the current crisis. My right hon. Friend is absolutely right to say that there can be as little scope as possible for people who are perhaps not quite as qualified as they should be to be given such jobs.

Chi Onwurah: My right hon. Friend the Member for North Durham raised the Test and Trace programme. I do not want to dwell on that, as it is not within the scope of the Bill, but it is important to understand the extent to which the programme has been used as a vehicle to privatise parts of the NHS by building up private sector skills as opposed to public sector skills. There must be some concern that the huge new powers for and requirements on Ofcom might effectively be used to privatise some of its duties.

Christian Matheson: My hon. Friend says that it is not in the scope of the Bill, but so wide is the definition of "another person" that, quite frankly, anything or anyone could be in the scope of the Bill. Again, the possibility is there, and it would not be down to the Minister. I know him—he is a friend and a man of integrity. As my right hon. Friend the Member for North Durham said, however, the next Minister to come along, in this Government, at least, might not be. Who knows? In four years' time, we might not have that problem.

This is an important aspect of national security, so I ask the Minister for clarity. It goes to the heart of the question of accountability—where responsibilities for inspections should lie. Similarly, in the second part of the amendment, we are seeking clarity on a limit on the amount that can be spent on inspection. We certainly

do not want Ofcom to be swayed into decisions about whether inspections can go ahead based solely on fears that it might wrack up big costs. Nor can those costs be allowed to spiral if the first part of the amendment is not adopted and private contractors are brought in but abuse the system. I refer the Committee to the comments made by my right hon. Friend the Member for North Durham a while ago—such abuse does happen.

It is often not helpful to put a financial cost limit on the face of the Bill, if only because it can become outdated over time. To be honest with you, Mr McCabe, the truth is that the £50,000 limit specified in the amendment is arbitrary. We plucked it out of thin air to illustrate a point.

Mr Jones: I thought that was the case was when I looked at it. Frankly, for anyone to do that job in telecoms for £50,000 would be very unusual.

Christian Matheson: Fortunately, we will not push the amendment to a vote, so we will not have to put that point to the test. It is an arbitrary figure and I hope the Minister will not fixate on it. It simply illustrates the point that there is a question of open-ended costs. We will not push the amendment to a vote, but we think there is a vagueness and a lack of clarity that needs addressing. I urge the Minister to consider these issues and whether Ofcom would be assisted by the greater clarity that these probing amendments would bring.

Chi Onwurah: Again, I rise mainly to support the excellent contributions made by my hon. Friend the Member for City of Chester in moving this amendment. I will raise a couple of points from my experience in this area.

As I said to my hon. Friend, having worked in telecoms for 20 years, when I joined Ofcom in 2004, I had worked with, or worked with someone who had worked with, just about every operator and network provider in the business. Those personal relationships can be helpful in ensuring quick, effective collaboration, but they can also bring about conflicts of interest. Ofcom, as a public body, has processes and procedures to address those conflicts of interest. However, the Bill makes no provision for that to be applied to whoever is "another person".

It is also the case that, unfortunately, as a regulator, one can be subject to regulatory capture by those who are regulated. The large operators often have tens or, in some cases, hundreds of lawyers and public affairs spokespeople. However, the smaller operators, unfortunately, cannot afford to dedicate so much time and resource to engaging with the regulator. It is critical that this huge increase in new powers and work for Ofcom is carried out in the right way.

As my hon. Friend said, the £50,000 figure has not been calculated on the basis of the likely costs to Ofcom, because the impact assessment does not indicate what they could be. However, it is merely the cost of five consultants at £1,000 a day for 10 days. We know that hundreds of consultants have been hired as part of the Test and Trace programme at those sorts of prices. That likely cost is within scope of any programme that is to be carried out by bringing in large private sector organisations. I hope the Minister will reassure us that he is taking these considerations into account.

Finally—I think we will discuss this point in more detail—this is a huge additional requirement on Ofcom. In the evidence session, Ofcom said that it thought it would need to hire 50 or 60 people to address the requirements of the Bill. There is always going to be an inclination to reduce internal resources, especially if they are in short supply, such as those to do with network engineering resources and the current skill set. So it is really important that the Bill should have a better definition than it currently does of who may carry out the work.

4 pm

Matt Warman: I enjoyed the semantic gymnastics by the hon. Member for City of Chester as he tried to expand the scope of the Bill, but I shall try to stick to what is in it. There is a lot of consensus across parties, so I shall resist the temptation of saying that £50,000 is a demonstration that Labour is willing to put a price on national security, which this party will never do, but I understand the points that he makes on both fronts.

The clause provides Ofcom with strengthened powers, including powers to give assessment notices to a provider, that are vital to enable it to fulfil its expanded and more active role. Assessment notices are an important new power in the regime that will give Ofcom tools to assess fully a provider's security and the extent to which it complies with its security duties. It is Ofcom's intention that when assessing a provider's compliance, its first port of call would be to use its information-gathering powers under section 135 of the Communications Act 2003. Ofcom would then use its power to give an assessment notice if it wanted to check the veracity of the information or to follow up a security concern. While Ofcom will therefore use its powers in a targeted and proportionate way, it is also the case that a provider with good security practices would expect to be subject to a lighter-touch assessment. Providers' duty to bear the costs of assessments will therefore have an incentivising effect.

The amendment would insert a new subsection into new section 105N, limiting the costs that Ofcom could incur in carrying out an assessment. Fundamentally, a hard cap of any sort will always be an arbitrary number which will potentially put an additional hurdle in place. It might be necessary for some of those tests to require genuinely extensive assessment—penetration testing, or red teaming, as exercises are sometimes called, where penetration tests mimic the action that an attacker might take to access the network. Those attacking actions may of course be from sophisticated sources, and the costs of mimicking them in an entirely legitimate way could be substantial; but it is right, in the interest of national security, that Ofcom does not reduce the quality of its testing. We would not seek to limit that either, notwithstanding its independence.

I can offer the Committee some reassurance, however, that Ofcom's assessment costs will not be excessive. It has a general duty to act proportionately and to follow other principles representing regulatory best practice. Finally, a provider's duty is to pay only such costs as are reasonably incurred by Ofcom in an assessment, so there is a balance there.

As to the proposed new subsection that would limit those able to carry out assessments to Ofcom or a UK Government agency, the assessments, as the hon. Member for City of Chester knows, may be complex and need

[Matt Warman]

specialist skills. Methods such as penetration testing might need specific technical skills and we should not limit Ofcom in that way. However, we should also bear in mind, as the hon. Member for Newcastle upon Tyne Central mentioned, that the independence and expertise of Ofcom is the greatest bulwark against such entirely unfounded but legitimate concerns as those raised by the hon. Member for City of Chester, about who might be appointed by this or any Government to carry out a task in the national interest. None of us would want—and I do not suggest that the hon. Gentleman is doing this—to get into the business of questioning Ofcom's independence in performing the tasks in question.

Chi Onwurah: I am somewhat concerned at the implication of what the Minister says. We cannot put a price on national security, and Ofcom has a role. In an evidence session, Ofcom's representatives said that although its role excludes any question of its making security decisions, it would ensure compliance, yet now the Minister seems to be saying that Ofcom will not have the skills to ensure compliance. I agree that there are specialised skills. Penetration testing, for example, is a specialised skill, but I would argue that it is a skill that Ofcom should take on as part of this new remit. I say again to the Minister that the skills needed to ensure compliance should be within Ofcom's remit, or should be better defined.

Matt Warman: Ofcom itself is best placed to exercise discretion as to whether it should carry out those assessments in-house, or whether it should have the flexible capacity to have the capability brought in as necessary. Ultimately, I do not think that anyone would wish to prevent Ofcom from having the ability to do what it thinks necessary by forcing it to use in-house staff only, because we cannot predict the future, as Members on both sides of the Committee have highlighted. Although the cause that the hon. Member for City of Chester is pursuing is a noble one, its unintended consequence would be to constrain Ofcom in both the expertise that it has at its fingertips and the costs that it might incur. We would not want to limit Ofcom's discretion to make those decisions as an independent organisation.

Chi Onwurah: Actually, the amendment would not limit Ofcom's discretion to bring in additional resources or skills. It would limit Ofcom's discretion to Government agencies or organisations within the public sector, which, on matters of national security, we should be able to do.

Matt Warman: If the hon. Lady were right, the only people from whom we would have heard evidence over the last few days would have been public sector employees. She knows just as well as I do that the cyber-security sector is a vast mesh of public and private expertise, which is inevitable given that we have private networks offering communications services. Although I understand her point, and I am all for Ofcom having as much expertise as it needs to do its job properly in-house, I simply do not think that we should constrain what it can access in the way that the amendment would.

On this, I think we probably agree on far more than we would perhaps like to admit, but the reason that this is a probing amendment, as the hon. Member for City of Chester said, is because imposing artificial constraints would not be beneficial to Ofcom's work. We understand what he said, however, and in broad terms, the Government agree.

Christian Matheson: I am grateful for the debate and for the Minister's response, but I do not intend to press the amendment any further. I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Chi Onwurah: I beg to move amendment 13, in clause 6, page 10, line 20, at end insert—

"(aa) provide a report on the diversity of their network's supply chains;"

This amendment gives Ofcom the power to request a report from a network provider on the diversity of their supply chains for the purpose of assessing whether they are complying with the security duties placed on them by earlier sections of the Act.

It is a great pleasure to speak to this amendment, which goes to the absolute heart of one of our key concerns about the Bill—the lack of any reference to the diversification of our supply chain. That is absolutely critical and should be integral to our national security. Our amendment 13 affects clause 6, which we have already discussed. The objective of the amendment is to give Ofcom the power to

"request a report from a network provider on the diversity of their supply chains for the purpose of assessing whether they are complying with the security duties placed on them by earlier sections of the Act."

As we have heard, clause 6 amends the Communications Act 2003 to insert section 105N, which gives Ofcom powers to assess compliance with the security duties set out in earlier sections, and section 105O, which gives Ofcom the power to impose on providers the duty to do any of a significant list of things, from (a) to (k)—to

"carry out specified tests or tests of a specified description…make arrangements of a specified description…direct an authorised person to documents on the premises…"

or

"assist an authorised person to view information".

As I have said, this is an integral part of the Bill and requires some considerable debate, so it may detain the Committee for some time, but this debate can be continued at a later time if necessary. There is a long list of requirements that Ofcom might place on network providers, but nowhere is there a requirement for those providers to give a report on the diversity of their supply chains, yet the diversity of a network provider's supply chains is absolutely integral to the security and resilience of that network provider.

We heard that very clearly during our evidence sessions. In particular, I asked Dr Drew:

"Is it possible for the UK to have secure networks without a diverse supply chain for them?"

Her answer was:

"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—in secure 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.]

The reason I have highlighted that particular quote—there were a number of quotations supporting the diversification of supply chains—is that it sets out really well what might happen if a network provider has only one possible supplier. If every aspect of its network is supplied by, let us say, Ericsson, and Ericsson then has supply issues itself or is bought or acquired by another operator from a different country that we might not be so close to, or—I do not mean to imply that this is a possibility—should fail in some way, that network provider no longer has any support for their network and no longer has the ability to maintain it securely.

The dependence of our telecoms security on diversifying the supply chain was set out in the 2019 telecoms supply chain report; yet the Bill fails to mention it at all. The objective of the clause is really for Ofcom to assess how successful a network provider is in meeting our nation's security requirements. My argument is that it is not possible to do that without understanding the diversity of that network provider's supply chain; yet the clause as it stands makes no reference to that.

4.15 pm

Our clause would enable Ofcom to request a report on the diversity of the network's supply chain. Alongside network provider diversity more generally, that provides a double layer of network diversification measurements because it enables Ofcom to see what each network provider is doing, as well as generally how our network supply chain is being diversified. During the evidence sessions, we heard a lot about open RAN. Indeed, the telecoms diversification taskforce and the telecoms diversification strategy put a lot of emphasis on open RAN. Open RAN is a development in standards, and so on, which will enable interfaces in networks to be open so that there can be a multiplicity of suppliers at different points in the network.

The evidence that we heard suggested that open RAN was at least six to eight years' away from maturity and from playing a significant role in our networks. What we seem unable to do in the Bill as it stands is collect the information to enable us to see how different operators are diversifying their supply chain, through the use of open RAN for example. We heard from Vodafone that it is undertaking trials of open RAN, particularly in rural areas, and we would expect, over time, that similar trials may be taken up by other network providers in the UK. How will we see that flowing through network providers' supply chains if we do not have a requirement or amendment of this type?

In Committee, we heard from Julius Robson, who said:

"Security is about resilience, and it is not a question of whether something will go wrong; it is a question of when. When we realise that one of our vendors is high-risk, will it take seven years to fix that problem? That is not a healthy place for our industry to be in. We want a rich diversity of suppliers working together, so that when we identify a suspect component or part in our network, there is something sitting there, warmed up and already integrated, ready to be swapped over. That is where we want to get to."—[*Official Report, Telecommunications (Security) Public Bill Committee,* Thursday 14 January 2021; c. 48, Q60.]

My question for the Minister is: how will we know that we are getting there? How will we know how diverse network providers' supply chains are? How will we know how resilient they are, and what the impact and security threat of a vendor being acquired by a hostile actor will be, for example?

We also heard from Doug Brake about the problems of regarding open RAN as a silver bullet that we can make a quick transition to.

He said to us:

"I honestly worry that it is too late for open RAN to be incorporated into 5G, at least on a broad scale. For greenfield networks, it is a different story and it might make sense to go with these open and modular systems from the get-go."—[*Official Report, Telecommunications (Security) Public Bill Committee,* 19 January 2021; c. 125, Q166.]

My question to the Minister is this: how will we know the extent to which particular vendors are taking up more diverse solutions and more resilient solutions without an amendment to the Bill of this type?

When it comes to understanding the diversity of vendors' supply chains, we have heard—I have spoken about this a few times, so I apologise for repeating myself—that there is an evolution of the network, from hardware into software services. We also heard during the evidence sessions that more and more of those software services and controls would be on cloud services.

However, in terms of understanding how resilient the new network architectures are, currently the Bill does not make any requirement for reporting on the evolution of network providers' networks with regard to who their different suppliers are and how many of them there are. So I have real concerns that the Bill is short-changing us on our network security, with the lack of any requirement on network providers to share with Ofcom information about the diversity of their supply chains. We have discussed the importance of supply chains and, to a certain extent, the complexity of supply chains, but we have not seen anything that will enable us to follow how the diversity of particular network operators' supply chains evolves over time.

I will finish on this point. We have seen significant consolidation in this industry, including in the number of network vendors, over the years. With the removal of Huawei, we are down to two equipment vendors, Ericsson and Nokia. However, we have also had a significant consolidation in terms of the management of networks and particularly in the underlying network architectures, so that many different network operators are effectively operating by perhaps using the same radio access network, or they may have very similar management layers.

The amendment is also designed to enable Ofcom to see how those technological changes are bringing new threats into our telecoms networks by bringing in new areas of potential consolidation. A number of times, I have used the example of Amazon Web Services. The future of networks that was suggested in our evidence sessions would ideally be a radio access network, manufactured by a number of different manufacturers but with quite simple boxes and antennae. And then the control, the services—everything—would be in a layer that would be running over equipment, or servers, from Amazon Web Services or any cloud computing service. That in itself is a different form of potential monopoly consolidation and potentially a different single point of failure, yet I see no requirement on Ofcom to assess how each vendor, each network provider, is evolving in terms of its network architectures and the threat to diversification of the supply chain that comes as a consequence of that.

When it comes to understanding the supply chains of the network providers as they are today, understanding how successfully they are evolving to become more

diverse, which is a hope that we all have—a shared desire—and understanding how technological changes may be bringing in new potential areas of consolidation, monopoly provision, and single points of failure, this amendment is designed to ensure that we have greater understanding of how things are today and advance warning of the implications of changes, and I do hope that the Minister will be able to accept it.

Matt Warman: I will go very briefly over the diversification strategy, which is essentially a £250-million initial tranche of investment to diversify the UK network, with a focus, to a certain extent, on open RAN, as the hon. Lady said. On the information that she would require, I agree with her so comprehensively that the provision is already in the Bill. Section 135 of the Communications Act 2003, as amended by clause 12—she is right that the provision is not in this clause—provides Ofcom with the power to gather information on diversification where Ofcom considers the information necessary for the purpose of carrying out its functions. Clause 12 specifically provides that such information can include information concerning future developments of a public electronic communications network or public electronic communications service that could impact on security. As I said, I agree with her so comprehensively that we had already foreseen the issue and the provision is already in clause 12. The addition of it to this clause would not change that fact. I hope that that provides—

Chi Onwurah: I thank the Minister for those comments. He says that the provision is already in clause 12. This is obviously down to my lack of studying, and I thought that I had studied every line of the Bill, but where specifically does clause 12 refer to diversification of supply chains?

Matt Warman: The approach that we have adopted across the Bill is that powers such as those in clause 12 are more than wide enough to cover exactly what is needed. What I am essentially saying, I suppose, is that the legal interpretation of clause 12 absolutely does what the hon. Lady seeks, because it is an absolutely essential part of one of the purposes of the Bill. That is why I hope she can take the necessary comfort to withdraw her amendment.

Chi Onwurah: I thank the Minister for that, but I am still puzzled as to where clause 12 says that Ofcom will collect data with regard to diversification of the networks. Ofcom is given the power to collect data with regard to the duties under the Bill, but there is not a duty under the Bill to diversify networks. I am trying to speed-read clauses and subsections; perhaps the Minister can direct me to a part of the clause that specifically requires information concerning. Clause 12 mentions

"information concerning future developments of a public electronic communications network or public electronic communications service that could have an impact on the security of the network or service."

I agree that that could be liable to an interpretation that included diversification of the network, but given that the Bill does not anywhere mention diversification of the supply chain as being part of the security of the network, I am afraid I do not feel reassured.

4.30 pm

Matt Warman: I am very happy to write to the hon. Lady to clarify why it is our belief that the Bill does that. What I would say is that the kind of specificity that she seeks would have the unintended consequence of narrowing what we do, rather than retaining the broad powers that we have in the Bill. As has been the case so often today, we do not disagree on the intent that she is seeking to obtain, and that is why the Bill is drafted as it is. As I say, I am very happy to write to her to try to clarify some of that.

Chi Onwurah: We all agree that the Minister is someone whom we like and who has the best intentions. On that basis, and on the basis that we can table further amendments at this stage or on Report if his letter of reassurance should not be sufficiently reassuring, I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Ordered, That further consideration be now adjourned. *—(Maria Caulfield.)*

4.32 pm

Adjourned till Tuesday 26 January at twenty-five minutes past Nine o'clock.

Written evidence reported to the House

TSB 09 Heba Bevan OBE, CEO and Founder, Utterberry Ltd.

TSB 10 Photonics Leadership Group and UK optical communication community