PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

TELECOMMUNICATIONS (SECURITY) BILL

Third Sitting

Tuesday 19 January 2021

(Morning)

CONTENTS

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

not later than

Saturday 23 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, Yohanna Sallberg, *Committee Clerks*

† attended the Committee

Witnesses

Professor William Webb, CEO, Webb Search

Emily Taylor, Chief Executive, Oxford Information Labs

Dr Alexi Drew, Research Associate at the Centre for Science and Security Studies, Kings College, London

Simon Saunders, Director of Emerging Technology, Ofcom

Linsey Fussell, Group Director for Networks and Communications

Public Bill Committee

Tuesday 19 January 2021

(Morning)

[Mr Philip Hollobone *in the Chair*]

Telecommunications (Security) Bill

9.25 am

The Committee deliberated in private.

Examination of Witnesses

Professor William Webb and Emily Taylor gave evidence.

9.26 am

The Chair: We now resume the public sitting. Welcome to our third session of oral evidence on the Bill. All our witnesses today will be giving evidence by video link.

Before calling the first panel of witnesses, I remind all Members that questions should be limited to matters within the scope of the Bill, and that we must stick to the timings in the programme motion that the Committee has agreed. For the first panel, we have until 10 minutes past 10 o'clock.

I now call the first panel of witnesses: Professor William Webb, CEO of Webb Search, and Emily Taylor, chief executive of Oxford Information Labs. Would you please be kind enough to introduce yourselves for the record and make a brief opening statement? We will start—ladies first—with Emily Taylor.

Emily Taylor: Thank you, Mr Hollobone. Good morning. My name is Emily Taylor. I am a lawyer by training. I have worked in the internet environment for more than 20 years. I am CEO of Oxford Information Labs, a cyber-intelligence consultancy. We are actively involved in standards organisations such as the International Telecommunication Union. I have authored papers on 5G and geopolitics, and on China's efforts to standardise a new internet. I am an associate fellow at Chatham House, editor of the *Journal of Cyber Policy* and a research associate at the Oxford Internet Institute.

I have listened to the evidence that you have heard so far, and in three areas I think I can bring new information or offer alternative perspectives to the Committee. Those are: why standards matter and what China is doing in standards; the need for a holistic approach to minimising cyber-security risks across critical national infrastructure and especially supply chains; and the China containment strategy and whether there might be more positive alternatives. I have several drafting points to make about the Bill itself, which I am happy to explore with you if time allows. I am of course happy to answer any other questions that you would like to put to me, within my capabilities.

The Chair: Thank you very much. Professor William Webb?

Professor Webb: My name is William Webb. I am an engineer by background. I have worked as a telecoms consultant for many years, and that is what I do now, advising regulators, operators and manufacturers around the globe. Most relevant to this Committee is perhaps that I spent seven years at Ofcom, helping it with radio spectrum and technology strategy. I spent 18 months at the Department for Digital, Culture, Media and Sport, helping it with its 5G programme. I have also co-founded a start-up in the telecoms space, so I understand that area.

Potentially, I can help the Committee on the security side by looking at whether we can be sure that we are being proportionate in our response to security issues. I can certainly help on the diversification side by talking a little about the strategies of operators, the potential role of open radio access networks and other such diversification strategies, and perhaps some of the better ways to deliver diversification in the future.

The Chair: Thank you very much indeed. I am now in Members' hands. Who would like to be first out of the blocks? Kevan Jones.

Q82 Mr Kevan Jones (North Durham) (Lab): Thank you both very much for agreeing to come before us this morning. Emily, will you expand on standards issues and how important that will be to how the telecoms sector develops in the future? Who are the leading players in setting standards? You clearly made reference to China trying to get a set of regulations to suit itself. Where are we on what has been described in many documents as the D10—trying to get the democratic nations to influence that agenda? How do you see the way forward?

Emily Taylor: Thank you very much for those questions. The first aspect is why standards are important. Standards development can be very long, drawn-out and not the most interesting thing to participate in, but they are vital both for our security going forward and as part of the diversification strategy. Dominance or over-reliance on a small number of players is bad for innovation, security and procurement. It is great to see the importance of standards coming through in the diversification strategy that has been published. Although standards can take many years to be created, they also hang around for many years, so if we miss the boat with a particular standard when it is critical to a new industry or technology, that can have a lasting effect on our domestic and international industries.

Many scholars, such as Laura DeNardis, have pointed out that technology is not neutral, and this really applies in standards. By accident or design, standards embed the attitudes, values and world view of the engineers who create them. That has not really been a problem for western countries to date, because the US and European participants have tended to dominate, but going forward we need to find a new way of coping and co-existing with a technological superpower that does not share our values and that has invested heavily, with a strategic approach to standards, for several years.

You asked who the leading players are in standards, and in particular you alluded to the role of China. It is quite telling to reflect on the number of leadership positions across the standards organisations environment currently held by Chinese nationals. Of course there are many standards organisations, including the Internet Engineering Task Force, the International Telecommunication Union, which sits within the UN, and bodies such as 3GPP—the 3rd Generation Partnership Project—and

the European Telecommunication Standards Institute. The Chinese players we see, not just from the Government but industry, include Huawei, Futurewei, ZTE, China Mobile, China Academy of Telecommunications Technology, and Tencent. All of them are active in standards.

The ITU is headed by a Chinese national, and of 11 working groups within the ITU's Telecommunication Standardisation Sector, or ITU-T, China has a chair or vice-chair in 10, and a total of 25 positions at chair or vice-chair; 135 so-called "questions", which are sort of agenda items across those working groups; and 87 rapporteurs. I could go on, but I think the point is made.

On where we are with a D10, as you know, the Defence Committee has quite majored on the idea of a D10—indeed, the idea has been going around for several years. The key element as I understand it is a recognition that this country needs to act with others to have a chance of having the coverage and investment that China has had, and that there are like-minded countries that we can partner with across standards, and also to reinvest in domestic or shared capability for manufacturing. Manufacturing has been leaving western countries for more than 30 years and we are now seeing the effect of that. It is all very well to worry about the rise of China, but if at the same time you are asking China to make absolutely everything, it is inevitable that there will be some technology transfer.

Of course, the D10 does not exist. The idea of a Five Eyes type of thing that would also morph into an economic and legal type of partnership also does not exist. Five Eyes is an intelligence-sharing network, not an economic bloc or a trading bloc. So there are challenges, but there are also opportunities for partnerships.

Q83 Mr Jones: It is quite clear from what you have said that China has been active in this sector. That is not unusual; China has done similar types of things in other international bodies. Have we in the west taken our eye off the ball in terms of representation on these bodies, and what will it take to step up to the plate and be involved in these standards settings?

Emily Taylor: It is a bit like waking up halfway through a chess game and realising that you are about three moves away from checkmate. I think we have taken the eye off the ball, although the UK has been strong on standards and has invested in them, but we cannot match China, where we see the fruits of a patient long-term strategy. It is all laid out in the "China Standards 2035" document, but some people in working groups say that they get more than 100 papers to deal with just before a meeting.

There is a sense that we are losing a grip. Part of that is that we did not realise how far standards embed our values until we started to see the alternatives. New IP is something that we have been writing about and studying over the last year. That is China's efforts to standardise effectively an alternative architecture for the internet, which would not be compatible with what we have today. That is at quite an advanced state across numerous working groups within the ITU.

The Chair: Professor Webb, would you like to respond?

Professor Webb: I certainly agree with all that. I have written standards myself and even run a standards body, so I know how they work. The important point is that it is not possible for a Government just to say, "We are going to influence that standard." Standards are influenced by the working papers written by the companies that attend the standards body. The UK Government themselves could not really have an influence, and nor could a university or any other organisation like that, not unless they spent inordinate amounts of money and hired a lot of people to write a lot of papers. There needs to be a concerted global or western European effort, or some kind of larger scale activity that can help the larger companies with the resources and expertise and the standards bodies to step up their efforts.

Q84 Sara Britcliffe (Hyndburn) (Con): Good morning, William. You alluded to this in your introduction, but what are the main risks to the Bill achieving the Government's aims for the security of the telecoms network? Can you expand on how you believe these could be mitigated?

Professor Webb: I think the Bill is fine when it comes to potentially delivering the security desires. It seems to be a very flexible Bill and has the capability to do all those kinds of things. My key worry is more one of proportionality. The Bill essentially says everything must be done to make sure that networks are completely secure. Of course, security is extremely important, but we could have a situation where there is a very tiny risk of some security breach but the mitigation is inordinately expensive, and that might result in higher consumer costs for mobile phones.

Ofcom will need to weigh up that proportionality and make sure its response is correctly balanced, but I do not see that in the Bill. I worry that the risk aversion that I think will happen automatically with the regulator may result in excessive security measures that penalise consumers when they are not particularly necessary. That is my biggest concern looking at the current structure.

Emily Taylor: I agree with William's overview of the Bill. It is great to see that the industry welcomes it. We heard from Ciaran Martin yesterday in his evidence to the National Security Strategy Committee that industry asked for this, because it had reached the limit of what it could do on a voluntary basis. It is great that it will lead to substantial investments and security. The telecoms security requirements are almost a recipe book—a very clear set of instructions on how to build more secure networks, which is great, particularly the focus on securing the management plane.

However, as William has described, in certain scenarios, there are almost unlimited liabilities for providers, not just to their customers, but to every person who could be affected by a contravention under clause 8. The inspection notices give very wide powers, including entry to premises, and the provider pays for that, so there is not much incentive for Ofcom as the regulator to think about whether this is justified value-for-money-wise and how to target interventions. I could go on, but the other question I have is about Ofcom's capacity in this sector, because it will have to acquire a very specific set of skills and capabilitie,s and that will require substantial investment and learning as an organisation as well.

Q85 Sara Britcliffe: Can I just quickly follow up with both witnesses? Were you consulted on the Bill prior to this?

Professor Webb: No, I was not.

Emily Taylor: No.

Q86 Chi Onwurah (Newcastle upon Tyne Central) (Lab): It is a pleasure to serve under your chairmanship again, Mr Hollobone, and thanks very much to the witnesses for joining us this morning. I should declare that William and I worked at side-by-side desks at Ofcom for some years, so I am well aware of his expertise in this area.

I have a couple of questions, starting with you, William. We heard from Mavenir on Thursday that open RAN could provide 2G, 3G, 4G and 5G networks now, but the operators were not looking to purchase networks from it. What is your view on the accuracy of that statement and the maturity of open RAN? What challenges does that pose with regard to the diversification strategy set out by the diversification taskforce?

Professor Webb: Thank you, Chi. I am sure Mavenir is correct that it can sell equipment that can do 2G, 3G, 4G and 5G, but that is not sufficient for an existing operator. If an operator wants to put this equipment into its network, it needs to work with its network diagnostic systems; it needs to handle all of the various features that it might deliver to customers, businesses or whatever, or that it might use for optimising its network or the various software systems that it has. It has built these up over 20 or 30 years, so adding in the equipment is a lot more than simply ticking the box and saying that it can transmit 2G or 3G. That takes quite some time, particularly with the more complex base stations that we find in city centres. The ones in rural areas are typically much simpler and less problematic if they go wrong. That is why we see people like Vodafone trialling open RAN in those places.

Although Mavenir has all the ticks in the boxes, it does not yet have work-through with the operators to deliver something that really works for all of its network. As we have heard from the operators, that is a long, slow process. The operators are rightly risk averse—they do not want to rush out a whole load of equipment and for their networks to fail after a few months, with all the problems that that would have for consumers. So it seems to me that we are still some time away—I think the operators have said five, six or maybe seven years—from any significant deployment of open RAN. That sounds very plausible to me as a strategy for evolving a network. Of course, by the time you get to that point, they will have deployed most of their 5G network already, so it feels as though open RAN will be too little too late to have a significant impact on diversifying the 5G networks that we have in this country and that we will have for the next few years.

Q87 Chi Onwurah: What would your recommendations be in terms of an effective diversification strategy? Where is the capability strong?

Professor Webb: If I wanted to diversify, I would instruct the telecoms operators to diversify. I would not try and pull the levers one step removed. I would say to the telecoms operators, either with a carrot or a stick, "You must diversify. If you have x number of vendors in your network, I will give you £x million as a carrot." The stick might be some kind of licence condition that said, "In order to meet your licence, you have to have at least x number of vendors in your network." That seems to me to be the way to pull through, and then the operators can decide whether they want ORAN, something like NEC or Samsung or someone like that. They can make that choice and that will pull through the decisions to them, rather than the Government trying to decide on their behalf what the best technology for them to use might be.

Q88 Chi Onwurah: Emily, what other security threats are not fully addressed by the Bill? How can we ensure that our networks are resilient to future security threats? I am thinking of the consolidation in cloud services, for example. As we move to more software-based networks, more and more of the value is in the cloud services. Say, for example, Amazon Web Services was bought by a Chinese company. Would you consider that a threat to the security of our networks?

Emily Taylor: Thank you very much for those questions. As a general point about the cyber-security of critical national infrastructure, I feel a little like we have been fetishising 5G and a single company for the last two years, perhaps at the expense of a more holistic awareness of systemic cyber-security risks. Ciaran Martin spoke eloquently yesterday about the need for flexibility in what critical national infrastructure is. The last year has shown us that what is critical very much depends on what you are going through at the time. Healthcare systems probably would not have been top of the list two years ago, but now they are. The SolarWinds attack shows that the identity of the vendor is not always the key risk point. SolarWinds is a very trusted vendor from a like-minded, close ally country, and yet it turns out to be a critical single point of failure across key, very sensitive Government Departments, both in the US and the UK.

Thank you for talking about consolidation across cloud services, Chi. One of my reflections on open RAN is that, although, of course, I am excited at the idea of open, interoperable standards, which would prevent vendor blocking, most of my experience has been in the internet environment rather than the mobile environment, and we are replete with open, interoperable standards, but we have a major competition problem. That in itself is not going to be enough of a lever to secure diversification.

On the point about acquisitions, particularly where you have cutting-edge technologies coming through, this country is really good at R&D—we have wonderful universities full of very brainy people who are creating things—but there does not seem to be the follow-through to create world-beating companies that can compete across the world stage. Why is that? It is because they either get sold to the US or to China. Of course, the foreign investment security strategies are all part of this as well, but you make a key point. If Amazon Web Services was sold to a frenemy country, that would potentially introduce the same kind of, at least theoretical, security risks that we have been troubled by over Huawei and 5G.

It is also the case that consolidation of infrastructure providers, like the cloud providers, is a security risk, because they become too big to fail. There was a brief outage of Google just before Christmas, and people just cannot work. When Cloudflare or Dyn go down, they introduce massive outages, particularly at a point where we are all so reliant on technology to do our work. These are security risks, and that highlights the need for a flexible approach. You have to be looking across all sectors.

Q89 Chi Onwurah: I see that William wants to come in. I just want to say that we have also been told that there was a major difference between fixed and mobile architecture when it came to security issues. You seem to be saying that there may be differences, but there are security issues within fixed networks as well as within our mobile networks.

Emily Taylor: Generally, our standard of security across the board is not as high as it should be.

Professor Webb: I realise that Chi had also asked me how the UK can strengthen its ability to provide diversified supply chains, and I did not address that.

I want to pick up on something Emily said as well. I think she is absolutely right—the UK has a great number of really excellent engineers, both in universities and in leading consultancy-type organisations. Here in Cambridge there is a plethora of wonderful consultancies and start-up companies. In my experience, the biggest problem is actually finance. To try to raise the finance to get a start-up company off the ground, particularly one that sells to operators who have huge purchasing power and tend to squeeze all their vendors—quite naturally—is very difficult in the UK. It is much easier in the US. Addressing the ability to provide finance for those kinds of entities and, to Emily's point, allowing them to exist for many years rather than to be bought as part of that financial process would help more than anything else, for the UK to grow its own major players in this space.

Q90 The Parliamentary Under-Secretary of State for Digital, Culture, Media and Sport (Matt Warman): Thank you for your comments so far. You will have seen in the diversification strategy that we completely agree with the points you have made around standards and the importance of international co-operation, so I will not go further into that. But it is interesting that a lot of what you have talked about is the diversification strategy rather than the Bill itself. In terms of where we have put increased duties on Ofcom, for instance, where do you feel that there should be more in legislation, rather than in the diversification strategy itself? It seems that tying our hands is not what you are asking us to do, but there is obviously a balance there, isn't there?

Professor Webb: Yes, I think there is a balance. I do not have strong views on that. The legislation appears to be sufficient and flexible in this space. I think the issue is the way it is implemented, and particularly the downstream actions of the Government and of Ofcom might need a bit more care.

Emily Taylor: The legislation is creating a framework, and a lot of that will be filled out through statutory instrument and the codes of practice that are envisioned. I imagine the codes of practice will reflect the TSRs to a large degree. Thinking particularly about how the legislation might impact on the wish and the essential need to diversify, it imposes very high levels of liability for providers, and almost unlimited duties on everybody for the smallest infractions. That is William Webb's point about proportionality.

As the measures come to life through secondary legislation, codes of practice and the actions of Ofcom, it is going to be very important that there are checks and balances. I am not sure whether the Committee is hearing from any civil society groups, but I am sure they would be worried about the very wide discretion for the Secretary of State. There is a lot of concentration of power in the Secretary of State and, perhaps, insufficient safeguards, as things are currently drafted.

Also, on the provisions that relate to the identity of the supplier—the nationality—rather than the qualities of security, which I think are the more relevant points, of course identity and nationality can be relevant, but there may need to be more of a look there to ensure that we are on the right side of potential risks of discrimination.

Q91 Matt Warman: In response to that, it is worth saying that there will never be such a one-dimensional approach as the one you have described, and I do not think you are suggesting that there is. However, I think we agree that there is a balance to be struck, and, inevitably, that comes in a whole series of advice from agencies and other entities. I was interested in something that Professor Webb said about the carrot and the stick. How would you propose that Governments or, I suspect, Ofcom incentivise operators to provide the greater security that you have been talking about?

The Chair: Emily Taylor?

Emily Taylor: I think that was a question to Professor Webb.

Matt Warman: It was to both of you, to be fair, but I did mention Professor Webb.

The Chair: You will both get a chance. We will go to Professor Webb.

Professor Webb: I am certainly all in favour of placing the requirements on those best placed to deliver them. For diversification, that is certainly the operators. I talked a bit about how you could, for example, offer them some financial incentive to have a more diversified supplier base. That would make some kind of sense, given that this would add costs to their management of the network.

In terms of security, I think it is a bit more difficult to see how that one might follow. I can imagine that there might be certain security issues where, for example, the decision might be made that a replacement is needed for a certain component in the network, or that they need to purchase some additional elements, and then you might imagine that it might help to have some sort of financial incentive to do that. But I think that would be on more of a case-by-case basis—I cannot see a clear, catch-all type of approach that would enable that.

Emily Taylor: I very much agree with what Professor Webb has said. Indeed, one of my reflections on the draft Bill is that it is very much at the stick end rather than the carrot end. Maybe we will start to see a bit more of the incentives coming through as the detail is filled out. But I think that thinking about incentives would very much reflect the close working relationship that there has historically been between the industry and Government. That is not the case in every country; it is actually a benefit in this case.

Security is expensive, and it is also long term. The telecoms supply chain review last year put it very accurately: the market does not reward investment in security—quite the opposite—so I would hope that there would be some recognition from Government about what is needed. I do not think that the investment in the diversification strategy is nearly going to match the investment that is required by the mobile providers who—yes, they are very successful large companies—have not had the great

decade that, say, the Googles of the world have had in terms of their margins. So you are asking an already squeezed sector to make substantial investments, and I think that is the place where you could be looking at incentives.

Q92 Christian Matheson (City of Chester) (Lab): Ms Taylor almost answered this question, but I just want to press both witnesses on this. The Minister referred to Professor Webb's comment on "carrot and stick", and obviously we are very keen to see diversification of suppliers increase in domestic capability as far as possible.

There is one way of looking at this legislation, which is that it can provide a market-led opening for suppliers, in a market that is no longer, in the long term, going to be distorted by, for example, Huawei, with its state backing. Is there any evidence, therefore, that other suppliers—first tier and lower suppliers—are looking at this and thinking, "There is a chance here to get back into the game"?

Ms Taylor, you talked about security being quite a difficult and expensive barrier to overcome, but are there any discussions in the wider sector about there being an opportunity to be had here, or about whether, actually, a stronger diversification strategy is necessary?

Emily Taylor: The initiative is welcome—the diversification strategy is welcome—but, as Professor Webb has described, there are many barriers to entry for new suppliers. To build out an entire country's network requires substantial scale, and, very understandably, the operators are risk-averse. You cannot just turn up and build out a network; open RAN is exciting, but, as you have heard from witnesses—and this morning, from Professor Webb—it is not ready, yet, to build out an entire country.

Also, the market distortions can still happen despite a diversification strategy. You can well imagine that the companies that decide it is attractive to enter this market are not, perhaps, the cheeky start-ups that you would want to encourage; they would be already dominant in other sectors. Imagine if we were sitting here, in five or 10 years' time, lamenting the fact that the equipment market is now dominated by Microsoft and Google. I am just making that up as a hypothetical example—I have no knowledge to back that up—but those are the companies that have the sufficient scale and skills, and as Chi Onwurah said in her question we are moving to a more hybrid network, where skills in cloud computing and software are going to define the success of the player.

Professor Webb: If you want to encourage a new entrant—be that a company that has some skills in this space but is upping its game to develop a complete system, or a brand-new company—they have got to develop the equipment, and that involves developing a lot of software and hardware, and an awful lot of effort and investment. If you add yet more requirements on them—for example, security requirements—that makes their effort even harder; it makes it even harder for new entrants to compete with existing players, who have already made much of that investment, to have the scale and capability to add on that extra. Adding security is the right thing to do—I am not criticising that—but the implication is that it will make it harder to diversify the supply chain. What you want to do is make it as easy as possible for new entrants, with the minimum requirements on equipment, if you want to bring a larger number in.

Q93 Christian Matheson: It would level the playing field, would it not? Everybody is having to work to the same level of security standards, rather than others thinking they can jump in there and cut in.

Professor Webb: I am not sure it would quite work like that. I think the operators would always want to procure to a certain security standard, whether there is legislation or not, so everyone would have to get to that standard. Raising the standards bar would essentially require everyone to move up higher above that bar.

Emily Taylor: If I may, just to support Professor Webb's point, the security standards do not level the playing field, although they are the right thing to do. In just the same way as we have seen some of the perverse consequences of, say, GDPR, the companies that have the scale and capacity to absorb the cost of compliance fare better than the smaller companies, who really do not have the scale and capability. The disincentive to enter the market, or perhaps the incentive to exit the market, as a result of these requirements, hits precisely the type of companies that you want to encourage, although it is welcome to see some recognition of that in the factsheets, with the tiering system. The third tier would probably let the smaller independent ISPs and providers off the hook. It is not quite correct to view it as the security requirements levelling the playing field. They are definitely required, and the market is not delivering that, but it will require close monitoring, I think, to ensure that there is still a competitive market.

Q94 Christian Matheson: If I have got it completely wrong, feel free to say, by the way, that I have got it completely wrong, because you are the experts here, not me.

Finally, could you sum up the chat around the sector at the moment? I get the impression that you are suggesting there is still a way to go to bring confidence that we can diversify across the broad range of the sector, as a result of this proposed legislation, and that there is still more reassurance and consultation required.

Professor Webb: Certainly, as I look at the information that I get back on ORAN, there is a lot more scepticism than optimism throughout the sector about its ability to do anything in the short term. We have talked a bit about why that is the case.

There is potentially more promise from the vendors that are somewhat established—the Samsungs and the NECs—and there is generally better comment about their ability to do something. If I had to look at what I am seeing around the industry and bring some advice, it would be focused on those vendors, rather than ORAN, as the most likely source of diversification over the next few years.

Emily Taylor: I can talk about the feedback that I have been getting. I come from a segment of the internet environment that has not historically been highly regulated at all. I would reflect that, if this Bill were brought forward to cover that sector, you would hear the screams. One thing that has really surprised me, and reassured me to a certain extent—it came through in the evidence you have heard—is that there is a degree of comfort with the direction of travel, and I think that speaks to the strong relationship that the industry has with Government on that.

The Chair: We have five minutes left; I am afraid there is a hard stop at 10 minutes past 10 o'clock. Two Members are seeking to ask questions, so would our witnesses treat this as a quickfire round, with punchy, pithy responses?

Q95 Mr Jones: Can I ask for your thoughts about Ofcom being the regulator of security? Has it got the capacity or culture to ensure the security of the network, particularly in light of the ISC's 2013 report on critical national infrastructure? That suggested that civil servants did not even tell Ministers about security threats. Would it not be better to place security with an agency that is responsible for security, rather than with a regulator that has a wide range of responsibilities?

Professor Webb: I think that has already been mooted. I doubt Ofcom has that capability at the moment. In principle, it could acquire it and hire people who have that expertise, but the need for secrecy in many of these areas is always going to mean that we are better off with one centre of excellence, where the threats are analysed, assessed and understood. We have that, of course, in NCSC.

NCSC would advise Ofcom, perhaps at a high level. Perhaps they would not need to detail exactly what the issue was, but they could talk to Ofcom about the mitigation, and Ofcom could be the entity that performs the proportionality of understanding whether a threat needs to be addressed and to what extent, in the midst of all the other things. That is how I would arrange these organisations.

Emily Taylor: Thank you for this question, which goes to both the capabilities and the culture. With the capabilities, as I have said in earlier remarks, Ofcom is going to need to upskill. In reality, as Professor Webb has said, they are going to be reliant on expert advice from NCSC, at least in the medium term, until there is a significant transfer of skills and technology, and in terms of the need for secrecy and a broader view.

Ofcom's historical role has been much less interventionist than is foreseen in this piece of legislation. Those cultural changes go deep into the organisation and into the character of the people who work there. Cultural change is always difficult and takes time, so I would not underestimate the challenge.

Q96 James Sunderland (Bracknell) (Con): This is a very explicit question to finish with, but could I ask both of you whether, from a security perspective, you agree with the decision to kick out high-risk vendors from the network? If so, why?

The Chair: You have about 30 seconds each, I am afraid.

Emily Taylor: I think it was inevitable after the US sanctions on semiconductor chips. It is something I regret, because the more difficult part is what we had being trying to do for 17 years, which is to treat all the networks as potentially vulnerable and adopt an evidence-based approach.

I do not think there is a going back from there. Unfortunately, the effect of the US sanctions has not just been on our domestic market. It will have hardened the resolve of China to have an entirely indigenous supply chain, and therefore will hasten exactly the outcomes that it is intended to avoid. We need a much more positive approach, investing in innovation and research, matching the capability and advocating for the benefits for a single, open and free internet.

Professor Webb: I do not have strong views. I think it depends, but clearly if it is high risk then it is probably appropriate to exclude them. The worry I have is that you end up focusing predominantly on vendors that you think are high risk, rather than on the overall security challenge, which will be across all vendors.

The Chair: May I thank both our witnesses very much indeed for your informative evidence this morning, and for giving us the benefit of your wisdom and expertise? We are very grateful to you. That brings us to the end of the time allotted for the Committee to ask questions in the first session.

Examination of Witness

Dr Alexi Drew gave evidence.

10.9 am

The Chair: We now move on to our next panel, which is a solo performance from Dr Alexi Drew, research associate at the Centre for Science and Security Studies at King's College London. Good morning, Dr Drew. Would you be kind enough to introduce yourself and make a brief introductory statement?

Dr Drew: Good morning, and thank you for inviting me to present and give evidence as part of this Committee. My name is, as stated, Dr Alexi Drew. I have actually recently changed my position. I currently work at the Policy Institute at King's College London, and my area of research is emerging technologies and their security and geopolitical implications. I have done a few pieces on Huawei in particular and the implications of supply chain security issues and risks, with publications in the *Financial Times* and so on, and that is why I find myself in your company today, I believe.

The Chair: Thank you very much indeed. I am in the hands of Members. Who would like to ask the first question?

Q97 Mr Jones: Thank youfor appearing before us today, Dr Drew. I would like your opinion on what the strategy is behind Huawei, possibly in terms of linking Huawei with the Chinese Government's strategy in the telecoms sector. What is the bigger picture or vision they have for this sector?

Dr Drew: I think the bigger picture is bigger than purely telecoms when it comes to China. China treats all its emerging technologies and its advancement of technologies—including telecoms, artificial intelligence and quantum research—as part of a broader means of advancing its influence, its economic strength and its geopolitical power on a global, regional and domestic stage.

Telecoms is a large component of that predominantly because, as I am sure you are all aware, the future of telecoms is essentially the provision of what will be the backbone of most of those other technologies; you require a good, advanced telecoms network to gain the full benefits of applications of artificial intelligence or quantum networking, for example. I think China and the CCP have essentially seen that telecoms is a key component of that and have thus done as much as they

can both to strengthen the sector within China, and to export that to gain further routes for the future stages of implementing more technological growth and economic and political growth through the next stages of their emerging technology portfolio.

Q98 Mr Jones: So the strategy is about market domination in certain areas?

Dr Drew: I would say that is definitely the case. It is market domination primarily for domestic, good use: it is a mistake to think of all that China generally does as primarily internationally orientated. The primary interest is domestic strength, security and stability. The fact that that can be achieved through gaining dominance in markets outside China is an added benefit.

Q99 Mr Jones: Clearly there is Huawei's domination in Europe, but what is the strategy when it comes to belt and road? We have seen investments in certain strategic areas such as the ports in Pakistan, Sri Lanka and other places. What is its strategy for telecoms? Is it a similar type of initiative?

Dr Drew: It is very similar. That is a great point to make. Pretty much wherever you see belt and road initiatives in, say, a port or supply chain of a physical good, you will see simultaneous investment and market input in a telecoms sense. There is a digital silk road as much as there is a belt and road initiative in the physical goods and supply chain sense.

They are becoming increasingly entwined fields; 10, maybe 15 years ago you could easily have seen a distinct separation between the physical supply chain and the digital supply chain. That differentiation is fading as we progress through time, and I think the Chinese have worked that out perhaps faster than we have and they are rapidly making inroads in order to amplify that effect and gain the benefits of it.

Q100 Chi Onwurah: Thank you for providing your expertise, Dr Drew. We heard from one of our previous witnesses that the security aspects here might be part of, if you like, a battle for the heart of the internet when it comes to embedding values into the standards that drive it. You seem to be saying that that is a part of China's requirements to monitor and surveil its domestic population, so I wondered what your thoughts were on that expressly.

Also, you have great experience in evolving security threats. In your view, does the Bill address major telecommunications threats to national security—future and evolving threats? For example, do you think this Bill would have helped to mitigate the impact of the recent SolarWinds Orion network monitoring hack, which was also mentioned by a previous witness?

Dr Drew: I will start with the question of values. I am a great believer that technology and values and norms of behaviour are implicitly connected: you cannot separate them. It should be explicitly understood that it is an implicit truth. I believe—and I have stated this before to some of your colleagues and civil servants in various Departments—that the CCP has realised that the great firewall of China, which tries to police content within China, has holes in it and is not going to last, or was not going to last, given the direction that the internet, freedom of communication and transfer of information is going.

The next logical step, and what I believe is happening, is that if you cannot control the internet within the great firewall, it is better to be able to shape the internet everywhere, both outside and inside it. I would argue that a lot of the technological standard-setting that you see take place in the ITU and elsewhere is essentially that taking place, as is the use of social media platforms to harvest data, which is then used to aid in the censorship of domestic content within China.

With regard to evolving threats and the Bill specifically, I think that the Bill goes a very long way towards pre-emptively meeting threats that are likely to come in the future. My biggest issue echoes what I caught of the previous witness statements: the fact that it is a matter of capacity for the institutions that are given this responsibility—that is, Ofcom—and the ability to change their culture to actively engage within that framework and take action to ensure these standards are met and kept to. Those are my biggest queries about the ability of this Bill to be as forward-looking as we would like it to be.

Finally, with regard to SolarWinds, I think this Bill is aptly timed in a way, given the context of this particular threat. SolarWinds was a perfect example of a supply chain security risk, and a vector of attack that went through a diverse supply chain to meet what should have been some of the most secure systems that the United States had.

Telecoms will, as I have already said, be the backbone of all the UK's future advancements of technology in all the things we are seeking to develop within our borders. The hardest thing to do as an attacker is to gain access. We should be making it as hard as possible to gain access; we should be making sure that there is as much oversight and understanding as is possible of where our supply chains go, the standards that they should meet, and whether those standards are being met, and I think this Bill goes some way towards that. I would argue that it needs to be continually updated, checked and maintained. This is not a one-off: times change, and the internet changes faster. Those would pretty much be my recommendations.

Q101 Chi Onwurah: Thank you very much for that. The Bill does not create any incentives for network operators to diversify their supply chain, or place any requirements on them to make notifications of changes to their supply chains or their networks that could have security implications. There is no proactive requirement on network operators to do that, or to actively participate in standards development—and we have heard about the importance of standards development and the huge presence of China in that space. Do you have any thoughts about how we could address those incentives, and also the power of standards development?

Dr Drew: The two essentially go together. If you look at the membership and those who take part in ITU standard setting committees and groups, you will see a predominance of not only state representation from China, but also representation of Chinese companies.

I think it needs to be made clear to our providers the benefits to them of being able to set standards; I believe this has been overlooked. The easiest way to do that is to simply look at some of the technical standards that have been set or lobbied for in this group by companies such as Huawei and ZTE, which are essentially entrenching

their technical standards into a global standards body—that obviously gives them an advantage in producing that output. I think our companies could benefit in exactly the same way, and they would certainly benefit from taking part.

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. It would be akin to having a black box where we go, "Okay, this black box must output something secure, but we don't need to know how it gets there." I think we should know, as much as is possible, who is involved in the supply chains to reach our eventual telecoms network.

Q102 Sara Britcliffe: Good morning and thank you for joining us, Dr Drew. In July last year, the Secretary of State made it very clear that the ban on procurement by the end of last year would have an effect on the roll-out. My question is: what will be the impact of the Bill on telecoms providers and infrastructure roll-out, as well as the 2027 deadline?

Dr Drew: It is undeniable, as the previous witness stated, that this Bill will increase costs and potentially slow down the pace at which development of these technologies, to the standards that are now being asked for, can be done. I have been asked similar questions before about what is the cost of us not getting to 5G roll-out as soon as possible. My general response has been to point out that although 5G is a backbone technology that provides access, we have very few practical applications of the speeds and connectivity that this network will provide us with.

It is something that you might see on your phone, but the increase in speed from having a 5G connection will be almost so fast as to be unnoticeable to the normal user. We have not got to the point where we have large city-wide technologies that will draw on this infrastructure, such as traffic management, health systems and economic production systems.

Although there might be a delay and an increase in cost—which again, I think we should try to meet in a way that incentivises more players to come into this market—I think this delay is not crippling. That is because, at the moment, although the 5G technology itself is maturing, the uses of that technology are still immature and I do not think we are losing out too much if we have a slight delay, with the benefit of reaching greater security.

Q103 Sara Britcliffe: Can I just quickly follow up on that? I think you have answered it. Were the Government right not to quantify the impact of any delay in roll-out of 5G and full-fibre networks in their impact assessment?

Dr Drew: I believe they were. I have seen a lot of attempts to quantify the damage or impact of limiting our vendor net, as it were. With the removal of Huawei, I have seen multiple attempts to put a value to that—of the slowdown and having to go to different vendors. I am uncertain as to the accuracy of any of those, and I think that it would be very difficult to put a number on that in any useful sense.

My impression is that there is nothing that should stop us from being able to enact the goals of this Bill and the incentives to diversify the market, while also being able to develop and invest in the next stage of 5G use, which is its actual application, and to marry those two up together in a manner that provides us with both security and financial and economic benefit from putting these systems in place.

Q104 Matt Warman: Thank you for what you have said thus far. Some of it has touched on the National Security and Investment Bill, which I think is a complementary part of this. A lot of what you talked about regarding any reservations you might have was around, essentially, the resources for Ofcom—something that I think we will be talking about quite a lot in Committee. I am looking forward to saying that Ofcom will have all of the resources that it needs. I wonder how you think the Government could best demonstrate, beyond that short statement, that Ofcom is getting the resources that it needs.

Dr Drew: I think what needs to be considered in that question is the type of resources that will be the hardest for Ofcom to acquire. I frankly believe it is not necessarily technology; I believe it is actually personnel. The edge that is given to companies that have already been mentioned in your hearings today—Google, Microsoft, Facebook et al—is not necessarily in the technology, but in those who design the technology. Those people are hard to come by at the level that we require them at. They are also very hard to keep, because once they reach that level of acumen and they have Google, Facebook or Amazon on their CV, they can pretty much choose where they go and, often, how much they ask for in the process.

I think the biggest issue that Government face—not only in Ofcom, but in regards to future technology policy—is attracting and keeping those individuals who can provide the services and understanding, as well as develop the tools, that a future Government will need. If you can demonstrate a way to capture that talent and retain it, I think that would go a long way to soothing any potential questions about whether Ofcom will be capable of meeting the requirements of this and other Bills. This goes across all Departments, I feel.

Q105 Matt Warman: Although is it fair to say that the best way that we demonstrate that capability currently is in the capabilities that we see clearly demonstrated at NCSC and GCHQ?

Dr Drew: Yes. I believe that this is potentially one thing where, as much as possible, greater co-operation between these Departments should be encouraged, to the extent that it is possible to do, given how the security dynamics of the different Departments work. Quite frankly, Government do not have enough of this kind of personnel and expertise. What you do have, you must ensure is used as effectively as possible. That means that you cannot let them languish in one silo or Department, when their expertise would be highly useful in another where suddenly they find themselves dealing with types of issues that are far beyond their normal remit.

Matt Warman: I am, of course, talking about co-operation between NCSC and Ofcom.

Q106 Mr Jones: Can I just come back on that? I agree with you that GCHQ has difficulty in retaining staff, as you quite rightly say, Dr Drew, when they get to a certain senior level. I think it is about more than that; it is about culture, as well. Ofcom has a wide number of

[Mr Kevan Jones]

responsibilities in this sector. Would it not be better, for the security element of this, to give that to the National Cyber Security Centre and GCHQ, rather than leaving it to an organisation, which—we have been told—even if it got the culture right, would take a long time to get there?

I think the Minister is relying on good co-operation between the two organisations, but it is clear from the 2013 ISC report on critical national infrastructure and Huawei that civil servants with a bent for looking at economic development did not have their eye on the ball in terms of security, and they did not even tell Ministers about security concerns that were clear then.

Dr Drew: That is a fantastic question. The best way for me to phrase this is that I believe there is an imbalance that is natural to those who have a particular role within Government or the civil service. Those with responsibility for economic advancement will have a different take on the same issue from those of their colleagues with a security bent to their work.

I find this is a complex topic that needs to be balanced across those different interests. That is why I would generally lean towards co-operation between these groups as opposed to others. I also suspect—although, due to the nature of their work, I cannot be certain—that GCHQ and the NCSC have significant work already, which is only likely to increase. Although they might have the technical capability that Ofcom lacks, I am not sure they have the capacity to take on the sheer volume of work that this is likely to create. I would argue that, actually, more resourcing in general is required for whatever co-operative body is created to carry out the actions of this Bill and other Bills attached to it. That is needed.

Q107 Mr Jones: I do not disagree with you about the balancing act between security and economic development, which will be important. This Bill leaves it with the Secretary of State for Digital, Culture, Media and Sport, who is not a natural fit for security, and there will clearly be tension between the two. Do you therefore think that these key decisions—not the actual work on them—should not be vested with the Secretary of State, but should perhaps have the sign-off of the Cabinet and the NSC?

Dr Drew: I would agree with you. I believe that the decision needs to be taken on a security level first, because insecurity and the risk of a poorly made decision would have negative impacts on the economic outputs as well. I am not certain that where it is currently vested in this Bill is the best place for it, but I also believe that transparency is the other balancing component here. I have had some conversations with one of the companies mentioned quite predominantly in this literature, and their biggest press is that they feel that decisions are being made with a lack of transparency and a lack of technical justification, and that it is all politics. The best way to solve that is through transparency.

Q108 James Sunderland: Dr Drew, as a graduate of King's College, it is great to have you with us. The Bill as currently written provides the Government with unprecedented new security powers. Might this in some way perhaps disincentivise new entries to the market?

Dr Drew: It potentially could, depending on the type of company that you are attempting to incentivise. It would have a different effect on those potentially two or more categories. If you take one category to be pre-existing companies that previously have not operated within the UK, such as NEC from Japan, they are likely not to be put off to such a great extent—they have already had to deal with some level of security commitment within their normal markets. However, I suggest that it could be more of a barrier to entry for the smaller companies that we are attempting to encourage to get into this market. Emerging companies would find a culture of components and cultural risk to how they view their work, as well as the technical and financial cost of meeting the new standards. Yes, I believe there would be an impact, but it would be different between types of vendors that you are seeking to encourage.

Q109 Chi Onwurah: We have talked a lot about 5G—indeed, we have been accused of fetishising 5G. The Government are currently consulting on security issues and fixed networks. Do you see major architectural differences or market differences in the security threats for fixed networks? Are they similar, and should a similar approach be taken to the removal of high-risk vendors? With regards to Ofcom, its principal duties are set out in the Communications Act 2003—I know this very well, having worked for it. They are

"to further the interests of citizens in relation to communications matters; and to further the interests of consumers in relevant markets, where appropriate by promoting competition."

Do you think there is an argument to add a further security duty, if that is going to take such a large portion of Ofcom's capacity?

Dr Drew: As to the second question first, I believe that security should be a component here. In fact, I believe it fits with what Ofcom is likely to be responsible for, and with the Online Harms White Paper as well. Security is fundamentally and inexorably linked with technology, culture and communications in the modern sense, so I believe that it would be important for that to be included as a key provision for DCMS.

With regard to the differences between fixed networks and 5G and the implications of this Bill, in the efficacy of its methodology towards the other, there are technical differences in how 5G operates right now and how we perceive the next generation of telecommunications to operate, but those differences will change over time, I believe. They will become less distinct. It is likely that fixed networks will move towards the concept of computing on the edge, and this is indeed already happening in some senses.

As for the actual efforts to control security risk, I do not see any major differences between telecommunications suppliers and fixed network suppliers. There is the same potential risk. You mentioned the SolarWinds hack earlier. That was a fixed network supplier in a way—it was not telecommunications—but there was the same risk involved and the same means of access, through a diversified chain with limited oversight at Government level, because it is a private sector actor with limited responsibilities. That is as true in that case as it would be for a fixed network with Cisco, and as it would be with a telecoms provider by ZTE, Huawei, Ericsson or any other. I do not think there is a significant technical difference to mean that the goals and direction of this Bill could not, and perhaps should not, be applied to others.

Q110 Chi Onwurah: I have just one quick follow-up question. Thank you very much for your evidence. The Bill separates out the diversification strategy, and in fact

it does not refer to the diversification strategy. Is it possible for the UK to have secure networks without a diverse supply chain for them?

Dr Drew: 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.

The same is true in this sense if you transfer these issues to telecommunications or fixed networks. If you have only a single supplier, all it takes is that supplier to be compromised for your whole network to be compromised. As I said earlier, with any form of cyber-attack, the access is always the hardest part if you are the attacker, so if you have an easy target or if the target is just one point, they can throw all their resources at it and it is easier. I would argue that diversification is one of the most basic and probably most effective means of limiting the damage that could be caused in any attack against one of those vectors.

Chi Onwurah: Thank you very much.

The Chair: Dr Drew, there are no further questions from Members, so I thank you very much indeed for your time this morning and for sharing your expertise with the Committee.

Dr Drew: It was a pleasure. Thank you.

Examination of Witnesses

Simon Saunders and Lindsey Fussell gave evidence.

10.38 am

The Chair: We now move to the next panel, which consists of Simon Saunders, director of emerging technology at Ofcom, and Lindsey Fussell—I hope I pronounced that correctly—group director for networks and communications, also from Ofcom. In the previous two sessions we have been talking about you quite a lot, and now is your chance to respond. Could I ask you to introduce yourself and give a brief opening statement, starting with Lindsey?

Lindsey Fussell: Thank you, Chair; that was the correct pronunciation of my name. I am Lindsey Fussell, I am the group director for networks and communication at Ofcom. My group oversees all of our telecoms regulation, including the new responsibilities for network security that we will be talking about today. I am sure we will have a lot of conversation about the nature of our responsibilities, but I think by way of opening I would say that we very much welcome the Bill. The National Cyber Security Centre found in carrying out its telecoms supply chain review that our existing responsibilities and the existing approach that operators took to telecoms security—and our powers as a regulator alongside that—really needed substantial strengthening, so it is great to see that happening in the Bill, giving operators the certainty of what they need to do to promote telecoms security.

Simon Saunders: Good morning, I am Simon Saunders, Ofcom's director of emerging and online technology. I have worked on mobile network technology since 1991, before there was 1G, all the way through to current work on today's and future implementations of 5G. Last week we published a round-up of technologies that could form the basis of future 6G networks. I have worked for mobile equipment vendors, operators, large end users and software companies. I founded and chaired an industry association, the Small Cell Forum, where I led a previous initiative on interoperability and open standards—in that case, in 3G—and I have invented a number of mobile technologies.

Today, I lead Ofcom's technical work on diversification, including Open RAN. I provide technical advice on behalf of Ofcom to the telecoms diversification taskforce. I hope I can help the Committee with issues on diversification, Open RAN and Ofcom's potential role in that area.

The Chair: Thank you both very much. James Wild will start the questions, followed by Sara Britcliffe.

Q111 James Wild (North West Norfolk) (Con): Clearly, these are new substantial duties on network providers and on you as the regulator to enforce them. What assessment have you made of the resourcing and additional expertise that Ofcom will require to take on these new duties?

The Chair: Simon Saunders?

Lindsey Fussell: I think I will lead on that one, if that is all right. Thank you for the question. I will start by clarifying Ofcom's role in the two parts of the Bill—I am sure we will talk about both. We have a significant role in relation to the telecoms security requirements, where we will have the obligation of monitoring and enforcing operators' compliance against them. In relation to high-risk vendors, our involvement is rather more limited. The Secretary of State will have the power to direct us to collect factual information from the operators, but the question of monitoring, compliance and enforcement then rests with the Secretary of State. I thought it might be helpful to clarify the two different roles before we got going.

In relation to telecoms security, as you say, these are important new responsibilities. We have existing responsibilities for network security—and have had since 2011, albeit in a more limited way—so we have a network security team in place. We are also very familiar with monitoring clients and enforcement, and with working with precisely the same set of operators that we will hear about on the remit of other responsibilities, so we have a base to start from. That absolutely does not underplay the difficulty, importance and challenge of building up our resources to deal with this. We anticipate that the cost will be around £6 million to £7 million in steady state, and we will build up a team of probably 40 to 50 new people and new resources to cope with those responsibilities.

The Chair: Simon, do you have anything to add?

Simon Saunders: On our capabilities relevant to the expectations end of things, we are building on our existing capability, working with mobile operators and network providers on the equipment and the software. That is spread across Ofcom, in the leading networks group that Lindsey leads, the spectrum group, and indeed in our technology group, which I look after. In

the relevant teams, we have been adding capabilities in with recent experience, with the mobile operators and mobile networks applying the formal diversification.

Q112 James Wild: You refer to needing 40 to 50 new additional staff. Have you begun recruiting those people yet and how confident are you that you will be able to get them? The security world is a competitive space and these are highly sought skills. How confident are you that you will be able to get those people in place in order to monitor and enforce the powers in the Bill?

Lindsey Fussell: We have indeed already started to build up our team, and have had some success in recruiting people with experience of network security—from the operators, for example. We do not underplay the difficulty of doing that; I completely agree that those are sought-after resources. Frankly, it is unlikely that we will be able to compete on salary. The type of people we attract are those who are interested in looking at these questions from that broader perspective—looking across the industry—rather than in their previous roles in companies.

We have found that we can have some success in that, but we will also have to be creative in the way that we approach this. We are thinking about how we can build up a pipeline, for example. The NCSC has accredited a number of university courses, and we are looking at how we, alongside the NCSC, can pick graduates up from those courses, for example, to build up a future pipeline of staff, as well as bringing in people with more direct experience.

The Chair: Simon, do you have anything to add?

Simon Saunders: No, not in that area. It might be relevant to mention, just to make the point that it can be done, that I actually joined Ofcom from a role at Google.

Q113 Sara Britcliffe: You never know, you might become shadow Minister when you move on from the job at Ofcom, as we have seen. My question is quite simple: do you believe that the Secretary of State is the right person to exercise the powers?

Lindsey Fussell: Are you referring there to the high-risk vendor powers?

Sara Britcliffe: Yes.

Lindsey Fussell: Yes, I think so. 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. In relation to telecoms security, that has enabled us to take the very detailed work and the threat assessment that the NCSC has done, which have been translated into a set of requirements in the code of practice, and to apply those and work with operators to monitor and enforce that compliance without having to make those national security judgments ourselves. On high-risk vendors, I think it inevitable that there will be more national security judgments to be made, so it is quite proper that that role sits with Government rather than the regulator.

Q114 Mr Jones: Your responsibilities are quite broad, and this is an expansion for you. You have already talked about recruiting staff for this task. How many of those staff will have to have STRAP clearance?

Lindsey Fussell: As I say, we have existing networks security responsibilities, so the issue of security clearance is one that we already need to deal with. I think the point that I have just made is important: we will not be making national security judgments, and that means that we will need access to less national security information than you might imagine. I do not think that we will be routinely handling national security information, but where the NSCS feels that it is required, there are clearly provisions in place for that.

Having said that, as now and in future, there are occasions when we have to handle sensitive information, and we do have the necessary security clearances in place at different levels for our staff to do that. As we recruit, we will obviously ensure that people have those necessary security clearances so that we can handle any sensitive information that we are given.

Q115 Mr Jones: I am sorry, but I do not accept what you have just said. If you are going to be the guardian of security as a member of the ISC who has STRAP clearance, you are talking about highly sensitive information, which, quite rightly, is guarded by the agencies for national security reasons. You will have to have a number of people who are STRAP-cleared. All I am asking is what that number is.

Lindsey Fussell: We would clearly take guidance from the NSCS and others on whether they think STRAP clearance is required, because of course, it is for the agencies to have STRAP clearance and to classify information. I have had STRAP clearance in the past, in my previous roles in Government, for example, so I am well aware of the different security classifications that are required and the nature of the information that is to be handled. At the moment, the NCSC has not signalled to us that it thinks we require staff with STRAP clearance, but clearly, if it feels that that is needed for the type of information that we may need to handle, we would make sure that happened.

Q116 Mr Jones: Personally, I do not see how you can do the job without having STRAP clearance making these decisions. As you know, you may have had STRAP clearance in the past, but it is not historic; you need to have it currently.

Lindsey Fussell: Of course.

Q117 Mr Jones: You said in response to Sara's question about whether the Secretary of State is the right person to make these decisions that you are not necessarily making the decisions. Clearly, however, there will be a pull between your role in promoting the sector in terms of economic development, and national security. You will have an opinion on that. How will you balance that judgment?

Lindsey Fussell: Our role in relation to the requirements is pretty clear. The Government, through the legislation that is being considered by this Committee, are setting out a series of duties on providers and then giving us a code of practice, which has been developed through the work that the NCSC did. That sets out in some detail what operators, in particular the larger operators, will be required to do to meet those requirements. What we will be doing is monitoring, discussing with and talking to those operators as they go on that journey, and ultimately—of course—enforcing compliance, if we think that is needed. Of course, our trade-off is always to be

proportionate in the application of our powers, but it is quite clear that the expectation is that we will enable, encourage and require operators to comply with the requirements.

Stepping back from that, there is clearly a balance of judgment that the Government have taken in bringing forward these measures. We all want, for example, to see people across the UK getting the best connectivity possible as fast as possible. This Bill may well have an implication for some of those plans, albeit that operators are well aware of what is coming. But of course the balance of judgment is the importance that security plays for consumers, in making sure that they have access to secure networks, and bearing in mind the significant costs that can be incurred by companies and ultimately by consumers if there are cyber-attacks.

Q118 Mr Jones: That will be a very difficult judgment to balance. I suggest that you read the 2013 ISC report, which is very informative on this issue and about where the balance went the other way, in terms of civil servants arguing then that economic development was better than actual security. So I think it will be a very difficult judgment to make.

Can I ask you about an issue regarding oversight? Frankly, I am not a great fan of quangos, because I think their accountability is limited and they allow Ministers to offload difficult responsibilities on to people who have very little parliamentary oversight. Regarding the oversight of your organisation from Parliament's point of view, some of these decisions will clearly be highly classified. The Digital, Culture, Media and Sport Committee will not be able to look at them, because of the security classification. So how will we ensure that you and Ministers will consider the importance of security around these issues?

Lindsey Fussell: That is a really important question. Clearly, we are accountable to Parliament—

Mr Jones: Sort of.

Lindsey Fussell: And we are ready to come and give evidence about our work to any Select Committee that would like to hear that evidence.

As I say, we ourselves will not make national security judgments, but I hear your point that the relationship and the role that we play in monitoring telecoms security, and enforcing those obligations on operators, is a very important one. Under the legislation, we are required to provide an annual report to the Secretary of State about what we find on the state of play regarding how operators are moving towards compliance, and indeed on any security compromises or incidents that we have uncovered and the action that has been taken in relation to those, and on any new threats or other issues that we have identified.

It will then be for the Secretary of State to consider whether they publish that report, and how much of it they publish. We will publish a summary of our work in our annual Connected Nations reports; we do that now. And as I have said, of course we will be ready to talk to any Select Committee that wishes to hear evidence of our role and how it is playing out.

Q119 Mr Jones: But the Secretary of State is not Parliament. The Secretary of State can hide behind things, or choose what he or she wants to put in the public domain. Do you think that the Bill needs to establish some role for Parliament at least to have an annual report, whether it is to the DCMS Committee or, if it has classified information in it, to the ISC?

Lindsey Fussell: I think that is really a question for Government rather than the regulator. We will be ready to provide whatever accountability the legislation requires of us, as well as providing direct accountability by talking to Parliament and Select Committees.

Q120 Christian Matheson: To follow up on one of Mr Jones's questions, you say that you will not be taking decisions on national security matters. Who decides within Ofcom whether it is a national security matter or not?

Lindsey Fussell: I think the structural framework helps us a great deal here, as I have already indicated. Clearly, the NCSC carried out a really detailed supply chain review, which identified the threats that could occur in different elements of the network, and it has now turned that into telecoms security requirements and, ultimately, into the code of practice. We will be giving—indeed, the legislation requires us to—considerable weight to that code of practice and the judgments that the NCSC has reached on what is required to combat threats. That will then enable us to judge and monitor whether operators are doing what is said in the code of practice.

If, for example, an operator were to say to us that it was not going to meet something set out in the code of practice because it considered that an alternative way would meet that threat, we will have arrangements in place with the NCSC to enable us to seek its advice and guidance at that point on whether that satisfies the requirements of national security.

Q121 Christian Matheson: Who takes the decision, then, to refer it to the NCSC? Where in Ofcom does that decision sit?

Lindsey Fussell: Clearly, we would start that conversation within the team and escalate it if necessary, but I do not think that it will actually be an issue in practice. We already have very good working relationships in place with the NCSC, and regular collaboration and discussion. The legislation enables us to share information with the NCSC to enable either it or us to perform its duties. I do not think that there will be any issue in practice, or any surprise in terms of our regular interactions with it.

Q122 Christian Matheson: Can I ask something slightly different now? Do you have much internal movement in Ofcom? Do you have an internal jobs board? Do people move around and develop their careers there?

Lindsey Fussell: Yes, we do. Of course, like any organisation, you would expect that. Ofcom has a range of people with different skills in it, as you would expect. It is actually far broader than, for example, some of the Government Departments that I have worked in before. We have people who are specialist technologists. Simon has talked about his experience. We have economists, lawyers, colleagues who specialise in enforcement, colleagues who specialise in policy, and many other professions. Although people absolutely do move and develop their career, and certainly in relation to these kinds of new responsibilities we will look to upskill existing colleagues where that is possible and where it makes sense to do so, we also employ an awful lot of specialists who will tend to stay more in that specialism and apply that to our work.

Q123 Christian Matheson: That is the point I am getting at. If I think about recent changes at Ofcom, you have had responsibilities for monitoring the BBC, for example. Online harms is coming to Ofcom. It seems that quite a lot is being asked of you, and demanded of you. How can we be sure that you have the capacity to manage the workload, and the technical capacity to manage these very challenging issues?

Lindsey Fussell: I am certainly not going to deny that there is quite a lot going on, and the organisation is expanding, as you say, albeit with different deadlines and different timescales for the new responsibilities. I have already talked about our recruitment plans to ensure that we have the specialist skills in place to focus particularly on network security, as well as the enforcement and legal support that we will need to deliver this regime, which is a very important part of it.

It is also worth reflecting, though, that there are some really interesting overlaps between different areas of our new responsibilities. If I think of the responsibilities that we have just taken on in relation to video sharing platforms, we are having to understand, as part of those responsibilities, network infrastructure, data analytics and so on. All that actually calls on similar skills and experience that we will need for the regime that we are talking about today, so there is some crossover that we can draw on. Simon, did you want to add anything on that?

Simon Saunders: Absolutely. We have different teams that we are building for the different responsibilities, but there are definitely overlaps between them, and in particular we have built a team of technologists particularly to inform our work on online issues, including, but not limited to, online harm. That comes with a need for us to have technologists who have worked in, and understand, a range of cloud-based computing platforms and the online social media platforms in general. The underlying *[Inaudible.]* technologies are the ones that increasingly telecoms networks are being built with as well—the so-called cloudification, or virtualisation. So, helpfully, when we recruit specialists in the one area there is the opportunity for them to contribute to the other areas of our responsibilities and to ensure that our approach to these things is *[Inaudible.]* I think we actually get benefits from having multiple of those duties, rather than separating them.

Q124 Chi Onwurah: Thank you very much for sharing your expertise with us. As a previous employee of Ofcom, for six years, I am, not surprisingly, perhaps, a huge admirer of your work, and, to reflect what was implied by the hon. Member for Hyndburn, I think that Parliament will always benefit from increased telecoms expertise here.

I want, with permission, to ask a question about three areas: security, assets and costs, and duties. I share some of the scepticism of my right hon. Friend the Member for North Durham about the statement that Ofcom will not be making decisions on national security. You will clearly have duties with regard to national security and one of the key duties is to ensure compliance of our entire network—all our networks—with national security requirements. So how are you going to ensure that compliance without taking decisions on security? You seem to suggest that it is just going to be a set of protocols, if you like, from the National Cyber Security Centre, and you are just going to look at ticking the boxes to see that they are met; but in practice that cannot be the case. It is far more complex than that, particularly with regard to emerging technologies.

Another issue is that the Bill puts all the requirement to ensure compliance on Ofcom, in terms of Ofcom seeking information, Ofcom requiring information, Ofcom setting out notices to inspect, and so on. For example, let us say that one of our network operators—I shall not name one—decides to buy all its cloud or virtualisation equipment from a Chinese manufacturer that is not designated a high-risk manufacturer. Would Ofcom be informed of that change in its network? How would that pass to the National Cyber Security Centre—or would it not? Without that kind of duty in place, is there a risk of what you do becoming a meaningless tick-box exercise and, particularly, of its not addressing future and emerging security threats? That is my first question.

Lindsey Fussell: The point that you raise about this needing not to be a tick-box exercise is absolutely vital. I think actually what we are talking about in this legislation is changing culture—crucially among operators but also in terms of giving the regulator new responsibilities and changing the culture that we have, and the responsibilities and the range of the role we take on in relation to this. So this is absolutely—the legislation in fact specifically says so—about future technology as well as about existing networks. It is critical, I think, that we and the operators go on this journey together in terms of promoting that security by design, in everything that is done.

Picking up your question specifically in relation to assets, I think it is more or less impossible to meet the requirements set out in the covid practice for the operators unless they have a detailed asset register of everything that is in their system. We would expect to see evidence of that, and that it is regularly checked, audited and so on. That would be an expectation for us.

On the relationship with the NCSC, as I say, we have specific provisions in place that enable us to share information with the NCSC. As we collect that information with operators, we will discuss with them in advance what type of information they want to see on a routine basis, sharing that and clearly taking guidance from them as necessary if they think there are national security issues that we need to be aware of.

I mentioned earlier about having security clearance in place. To expand on that answer, we have a small number of STRAP-cleared staff in Ofcom, and we will expand that if need be. Those relationships with the NCSC are already in place and will be productive. I should say also that if the NCSC identifies new threats, or if we identify new threats, I think the legislation is flexible and it is right to be so, in that the code of practice can be updated to reflect that.

Simon Saunders: Could I also add that, in respect of our role in emerging technologies, we are not only awaiting others to tell us which emerging technologies to pay attention to? We have our own independent programme of monitoring and horizon scanning for technologies that could appear and have an impact on the networks and the sectors that we regulate. Clearly, the implications are not only about security. They cover a wider range of issues of performance and costs and flexibility and so on. We actively monitor across these sectors for those technologies.

I mentioned earlier that we recently published something about technologies heading for the future generations of mobile. That also covers fixed networks, the advent of quantum technologies and distributed software technologies in networks, and so on. That programme yields an advance look for colleagues about threats and opportunities that are coming towards us into the markets, so that we can build the skills and consider the implications well in advance of their actually impacting on those networks.

Q125 Chi Onwurah: How can you make that assessment without taking decisions about national security? If you are relying, as you seem to be saying, on the National Cyber Security Centre to make those decisions for you, how are you, or they, accountable to Parliament for that? There is a basic issue here, in that you feel that you are not responsible for national security. However, we do not see how that responsibility for national security is made accountable if you do not have any responsibility for it but you have responsibility for compliance. You have not answered my question as to how a change in the networks would be made known to you or the National Cyber Security Centre when there is no requirement for that at the moment, as far as I can see.

Lindsey Fussell: We would, as I say, expect providers to keep detailed records of the components that they use in their networks. I would expect that that is the type of information that, if a significant new vendor is brought into the market, the NCSC might well be interested in. It is worth saying that, while we do not have any direct regulatory powers over the vendors themselves, under these arrangements operators are required to assess the maturity of the vendors and suppliers they use, and the NCSC has issued guidance to them to enable them to assess that maturity. If the question is: if we see a brand new supplier starting to appear, is that the kind of information that we would expect operators to provide to us and for us then to share it with the NCSC? The answer to that question would be yes.

Q126 Chi Onwurah: With regard to asset registry and expectations of having that, having spent a significant amount of time looking in the back offices of operators as to what they have, I know that they are certainly not up to date. We have heard from other witnesses that they do not always have up-to-date and comprehensive asset registers. To rely on an expectation seems a low bar.

Can I come on to duties? I have the Communications Act here, which has got a lot thicker since I left Ofcom. The two duties are the "interests of citizens" and the "interests of consumers" with regard to competition, but there is not a duty on security. Does that not suggest that if there is a conflict between competition or communication matters, that will be prioritised over security if there is not an explicit duty to maintain the security of our networks?

Lindsey Fussell: I think this legislation quite clearly does place explicit duties on us to monitor and enforce the compliance of operators on network security requirements. I do not see that there is any risk that we would downplay the importance of that duty in comparison with others. Clearly, it is for the Government to put forward any changes to legislation to change the balance of our duties or to add new ones, but I think the Government—and, indeed, Parliament—are asking us very clearly to take on those responsibilities through this new legislation.

To pick up on a point I made earlier, in terms of the interests of citizens and consumers, it is important to say that of course it is in the interest of citizens and consumers to have excellent networks functioning that provide them with great connectivity. If we have learned anything from this most recent period, it is how important connectivity is to everybody's daily life. Of course, that comes across in pricing and support for more vulnerable consumers, and all those other things that we have responsibility for in telecoms.

Actually, promoting secure networks is absolutely in the interests of consumers and citizens as well, not just because of the really damaging consequences of cyber-attacks, but because, ultimately, if we are able to have better networks, that should enable greater economic innovation through 5G use cases and things like that, for example. I think in promoting the interests of citizens and consumers, telecoms security is clearly part of that.

Q127 James Sunderland: The Bill provides powers to fine vendors up to 10% of their annual turnover or up to £100,000 per day for failing to meet standards. Could I ask for your view, please, on how that compares internationally, and whether you feel that that is appropriate?

Lindsey Fussell: It is probably worth saying that, from an international perspective, although there are some other countries—notably Germany and Australia—that have started to explore strengthening their telecoms security framework, I am not aware of another country that is quite as forward leaning in terms of the framework that is being put forward in this legislation.

In terms of the fines, this is an important point—those fines match the level that we are currently able to levy in relation to our other telecoms requirements, such as breaches of our general conditions. Previously, under our past responsibilities, our fines were limited to £2 million, so really quite a small amount compared with the wealth of the largest operators. I think it is appropriate that the telecoms security fines match what we are able to do elsewhere.

The final point I would make is that fining is an incredibly useful power to have because it acts as a significant deterrent and a strong incentive for companies to comply. It is actually not the first lever that we reach for, certainly not maximum fines; it is there and we are ready to use it if we need to, but our starting point would be to work with operators on this journey as they move towards compliance as they respond to new and emerging threats.

Q128 Matt Warman: Thank you for all the work you have done on this matter so far. I wonder if you could just say a little bit more about the responsibilities that Ofcom has had, as you put it, since 2011 on telecoms security. I think that perhaps the extent of that is not as well understood as it could be.

Lindsey Fussell: Yes, of course, I am very happy to do that. As you say, we have responsibility now to monitor and enforce compliance on security. The difference, which is why I think this legislation is so welcome, is that at present we do not have any obligations set out as to how operators need to meet those security requirements. It has been basically up to them to decide what is

necessary. While many companies have invested very heavily in their security—I would not want to suggest otherwise—clearly there is a journey to go on and improvements that need to be made. It is very welcome that we now have this much clearer framework, so that operators know what they need to do and we can enforce against it.

The other point that is worth bringing out is that, at present, operators are under a requirement to report incidents to us, but the nature of that reporting tends to be around incidents that cause outages. We do get a lot of those—caused not just by cyber-security but by wind, weather and other issues. Quite a lot of cyber-security incidents are, frankly, precisely designed not to cause outages, because it is in the interests of the malicious actor to allow the network to keep operating while they do whatever they are up to. The new requirements on operators are to tell us not just if there is an outage but if there is an incident where they believe their system may have been compromised. They are wider ranging and welcome powers.

Q129 Matt Warman: I think you are also aware that this legislation is backed up by a number of statutory instruments to give further powers.

Lindsey Fussell: Absolutely.

Q130 Matt Warman: Would you like to give an assessment of whether you think that is sufficient to address the concerns around, for instance, asset registers, which we have talked about before?

Lindsey Fussell: Yes, so the way the legislation works, as you say, is that there is a primary duty on operators to promote security of their networks, and on us to enforce and monitor compliance against that. My understanding is that the secondary legislation will set out around 40 to 50 sub-duties on operators, which they will all need to meet—that is all operators and providers of electronic communications services.

Underpinning that, each of those sub-duties will be reflected in the code of practice, setting out the details of what the operators need to do to meet each of those sub-duties. As I explained earlier in relation to the questions we discussed on national security, we are entitled, as the regulator, to place quite a lot of weight on the national security judgments that the NCSC and the Government have made in drawing up both those sub-duties in the code of practice, in responding to the threats identified.

The Chair: Any other questions from Members?

Q131 Chi Onwurah: A word on costs, perhaps. You said in your opening statement that you expected it to cost about £6 million to £7 million for Ofcom. How will those costs be funded or raised? In terms of costs on operators, clearly a requirement to do a complete asset register, for example, could be a very significant cost for an operator. What kind of costs do you see? Do you see limits being placed on the costs that operators could incur in complying with Ofcom demands or requests?

Lindsey Fussell: In relation to Ofcom's costs first, Ofcom is funded in two ways: first, by a levy on the sectors and companies that it regulates and, secondly, through the collection of fees, primarily from our spectrum duties. Our overall funding is obviously agreed by our board but also subject to a cap agreed with Government each year. We are currently in discussion with the Treasury about the exact technicalities and which of those routes will be used to fund this, but it will be in line with Ofcom's normal funding arrangements.

In relation to company costs, clearly the Government have looked into that, in discussion with operators in relation to the impact assessment for the legislation. I know that there is a plan to do further work on that in relation to telecom security requirements, once companies have had a chance to see the SI and the code of practice.

The point here, which is built into the legislation, is the concept of proportionality. Although we would expect the largest operators—we would work with them intensively throughout the process—to take part in, for example, penetration testing, it is likely we will be more proportionate with the smaller operators and, for example, respond on an incident-based approach, rather than expect them to carry out the same level of detailed work and interaction with Ofcom. In all of that, we would want to be proportionate in the costs imposed on operators, as we are in all our responsibilities, bearing in mind that these are really important responsibilities, as we have been discussing.

Q132 Chi Onwurah: Could you therefore confirm that the costs will be in line with the size of the operator, so small start-ups will not be expected to pay the same as Vodafone, for example? We have not talked at all about the diversification strategy, yet there is agreement that we cannot have secure networks without effective diversification of the supply chain. Are you in a position to monitor the diversification of operator supply chains, and is that something you would expect to be doing?

Lindsey Fussell: If I may, I will bring Simon in on the question of diversification. In relation to costs, the bulk of Ofcom's own costs are paid by larger operators rather than smaller ones, and we have talked about proportionality in the way we operate that. Again, although I understand the tiering of the system will be set out in the code of practice, that will also be based on size and scale. Simon, may I turn to you on diversification?

Simon Saunders: The diversification strategy that the Government have published has set out a desire to attract new suppliers to the UK and further expand suppliers through open solutions, among other means, and to ensure that that is supported by an appropriate regulatory framework. We are ready to do what comes from that, in terms of any objectives the Government set on the level of diversification and to support measures to enable that. There are clearly synergies between the security aspects and the diversification aspects: in determining how diverse the supply base is, having a fully populated and up-to-date asset register from the operators for the security needs will also support the requirement to assess the diversity, if that is what we are required to do.

Q133 Chi Onwurah: But currently your duties are all to do with the stick, in terms of the enforcement of security requirements, and nothing to do with diversification or the incentives for that?

Simon Saunders: Our existing duties around ensuring the health of the communications market for consumers and citizens point in the same direction in many ways, even if diversity is not spelled out explicitly. We see that a functioning, competitive market for network equipment supports the operators' ability to provide cost-effective

networks that perform well, and that supports the needs of citizens to get great services wherever they are and for those services to be reliable and so on. I do not view this as an entirely separate area from our existing duties; whether specific duties around this are needed is part of the work we are doing to support the taskforce and the plans that come from that.

The Chair: This will have to be a very quick answer, because we have to stop at 11.25 am.

Q134 Mr Jones: You have said that you will take advice from the National Cyber Security Centre. What happens if you disagree with its advice? Who takes the final decision on what is national security?

Lindsey Fussell: I think that the National Cyber Security Centre takes the decision on national security. Of course, the Government ultimately have the power for that but on the advice of the NCSC. Decisions on enforcement and compliance are for Ofcom, following the code of practice that the NCSC has created for the Government.

Q135 Mr Jones: Yes, but what happens if you disagree with it?

Lindsey Fussell: Sorry, I had some feedback there; I was having trouble hearing you. Is the question what would happen if we disagreed with the advice given to us by the NCSC on national security?

Mr Jones: Yes.

Lindsey Fussell: I think in that case we would take the guidance of the NCSC. In practice, I really don't think that is likely to occur. Ultimately, the final decision on whether an operator has complied and whether we enforce is with us. The NCSC would not be able to overrule that decision, but we would be taking that decision in the light of the information we would have been given from NCSC about what is required to meet national security.

Q136 Mr Jones: May I suggest that you read the Intelligence and Security Committee's report from 2013 on critical national infrastructure, because exactly that happened when a Department overruled the Security Service? I think you will find yourselves in a similarly sad position with this legislation.

Lindsey Fussell: I have read that report, thank you.

The Chair: Thank you very much indeed to our two witnesses. We are very grateful to both of you for your time this morning and for the expertise you have shared with us.

11.25 am

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

Adjourned till this day at Two o'clock.