PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

PRODUCT SECURITY AND TELECOMMUNICATIONS INFRASTRUCTURE BILL

First Sitting

Tuesday 15 March 2022

(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 19 March 2022

The Committee consisted of the following Members:

Chairs: Caroline Nokes, † Graham Stringer

† Baynes, Simon *(Clwyd South)* (Con)
Bhatti, Saqib *(Meriden)* (Con)
† Brennan, Kevin *(Cardiff West)* (Lab)
† Double, Steve *(St Austell and Newquay)* (Con)
† Edwards, Ruth *(Rushcliffe)* (Con)
† Elmore, Chris *(Ogmore)* (Lab)
† Grundy, James *(Leigh)* (Con)
† Hart, Sally-Ann *(Hastings and Rye)* (Con)
Hollern, Kate *(Blackburn)* (Lab)
† Long Bailey, Rebecca *(Salford and Eccles)* (Lab)
† Lopez, Julia *(Minister for Media, Data and Digital Infrastructure)*
† Mishra, Navendu *(Stockport)* (Lab)
† Osborne, Kate *(Jarrow)* (Lab)
† Randall, Tom *(Gedling)* (Con)
† Vara, Shailesh *(North West Cambridgeshire)* (Con)
Warburton, David *(Somerton and Frome)* (Con)
Whitley, Mick *(Birkenhead)* (Lab)

Huw Yardley, Bethan Harding, *Committee Clerks*

† **attended the Committee**

Witnesses

Anna Turley, Chair, Protect and Connect

Dr Charles Trotman, Chief Economist, Country Land and Business Association

Eleanor Griggs, NFU Land Management Adviser, NFU

John Moor, Managing Director, IoT Security Foundation

Dave Kleidermacher, VP for Engineering, Android Security and Privacy, Google; Director, Internet of Secure Things Alliance

Dan Patefield, Head of Programme, Cyber and National Security, techUK

Public Bill Committee

Tuesday 15 March 2022

(Morning)

[Graham Stringer *in the Chair*]

Product Security and Telecommunications Infrastructure Bill

9.25 am

The Chair: We are now sitting in public and the proceedings are being broadcast. I have a few preliminary announcements. If hon. Members with speaking notes could email them to hansardnotes@parliament.uk, that would be very helpful to *Hansard*. Similarly, officials in the Gallery should communicate with Ministers electronically. All electronic devices should be switched to silent mode. Unlike in Select Committees—although these proceedings are similar—tea and coffee are not allowed during sittings.

We will first consider the programme motion on the amendment paper, and then a motion to enable the reporting of written evidence for publication, and a motion to allow us to deliberate in private about our questions before the oral evidence session. In view of the time available, I hope that we can deal with these matters formally. We discussed the programme motion last week at the Programming Sub-Committee.

Ordered,

That—

1. the Committee shall (in addition to its first meeting at 9.25 am on Tuesday 15 March) meet—

(a) at 2.00 pm on Tuesday 15 March;

(b) at 11.30 am and 2.00 pm on Thursday 17 March;

(c) at 9.25 am and 2.00 pm on Tuesday 22 March;

(d) at 11.30 am and 2.00 pm on Thursday 24 March;

(e) at 9.25 am and 2.00 pm on Tuesday 29 March;

2. the Committee shall hear oral evidence in accordance with the following Table;

Date	Time	Witness
Tuesday 15 March	Until no later than 10.25 am	Protect & Connect; The Country, Land and Business Association; The National Farmers' Union
Tuesday 15 March	Until no later than 11.25 am	The IoT Security Foundation; The Internet of Secure Things Alliance; techUK
Tuesday 15 March	Until no later than 2.40 pm	Professor Madeline Carr, University College London; Copper Horse Limited
Tuesday 15 March	Until no later than 3.40 pm	Openreach; CityFibre; Speed Up Britain
Tuesday 15 March	Until no later than 4.20 pm	BUUK Infrastructure; The Internet Service Providers' Association
Tuesday 15 March	Until no later than 5.00 pm	Which?; Refuge

3. proceedings on consideration of the Bill in Committee shall be taken in the following order: Clauses 1 to 66, the Schedule, Clauses 67 to 78, new Clauses, new Schedules, remaining proceedings on the Bill;

4. the proceedings shall (so far as not previously concluded) be brought to a conclusion at 5.00 pm on Tuesday 29 March.—*(Julia Lopez.)*

Resolved,

That, subject to the discretion of the Chair, any written evidence received by the Committee shall be reported to the House for publication.—*(Julia Lopez.)*

The Chair: Copies of written evidence that the Committee receives will be made available in the Committee Room and circulated to members by email. I would usually call on the Minister at this stage to move the motion for the Committee to sit in private, but I do not think that the Front Benchers on either side want to move into a private session, so we will continue sitting in public and the proceedings are still being broadcast. Before we start hearing from the witnesses, do any hon. Members wish to make declarations of interest in connection with the Bill?

Ruth Edwards (Rushcliffe) (Con): I am a former worker in the cyber-security industry, and have worked for a couple of the witnesses giving evidence today. One is techUK; I have also worked for BT, which of course owns Openreach. I also draw the Committee's attention to my entry in the Register of Members' Financial Interests: I undertook some work in cyber-security for MHR between May and December last year.

The Chair: Thank you. The Clerks will note that declaration from Ruth Edwards; and Ruth, if you wish to refer to it later in the proceedings, do so.

James Grundy (Leigh) (Con): This is slightly tangential, but better declared than risked. The Grundy family farm has a mobile phone mast, for which my father receives yearly payment.

The Chair: Thank you. The same applies.

Examination of Witnesses

Anna Turley, Dr Charles Trotman and Eleanor Griggs gave evidence.

9.29 am

Chair: I welcome the witnesses to the meeting, and thank you for your time. Before calling the first Member to ask a question, 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 to which the Committee has agreed, so this session will end at 10.25 am sharp, or earlier if we run out of questions. I ask the witnesses to introduce themselves briefly.

Anna Turley: My name is Anna Turley and I am chair of the Protect and Connect Campaign.

Eleanor Griggs: I am Eleanor Griggs, land management adviser for the National Farmers Union, representing about 47,000 farming members.

Dr Trotman: I am Charles Trotman, chief economist at the Country Land and Business Association. We represent 28,000 members across England and Wales. I am also chair of the rural connectivity forum, which represents rural organisations to industry and Government.

The Chair: Thank you. Let us move first to the Minister to ask any questions that she may have.

Q1 The Minister for Media, Data and Digital Infrastructure (Julia Lopez): Thank you for coming, Anna. It is good to see you again, and I am grateful to you for taking the time to meet me earlier. It would be helpful to understand how the curve of difficult cases has changed. You will know that in 2017 a lot of reforms were made to the electronic communications code and, initially, there were difficulties in finding the right balance between the rights of landowners and the interests of telecoms operators. A larger a number of cases arose, but certainly from my experience as a Minister, the number of difficult cases seems to have evened out. Is that the experience of Protect and Connect?

Anna Turley: Thank you for meeting us to discuss our campaign. I should have mentioned at the outset that we represent all the site owners around the country who host telecoms communication infrastructure on their land.

I am afraid that we are not seeing the same tailing off of difficult cases; a number of cases are continuing to come to us where leases are up for renewal, yet telecoms companies are behaving in quite an appalling way. We have cases of rent reductions, often starting at 90% to 95%, and that is par for the course—it is not a small handful of extreme cases. In a large number of cases across the country telecoms companies are coming in often with very aggressive legal notices, which are quite intimidating and making people feel that they are being steamrollered by those large companies. People feel that they have no ability to participate in the legal process, and are obliged to take those cuts of 90% to 95%. If you are small community group, a church or a sports club, the difference between £4,000 and a couple of hundred is huge and has a great impact, especially when you believed that you had that income for the next 10 years. The impact on people has been huge and it has been pretty devastating since 2017.

Our frustration with the Bill is that it fails to address the root causes of that problem. The valuation issue is affecting people deeply, and the Bill will not deal with that. Those cases will continue to arise, and in fact the Bill will expand the number of people who will be affected by the 2017 code through the Landlord and Tenant Act 1954 and the Business Tenancies (Northern Ireland) Order 1996. Between another 3,000 and 4,000 people in Ireland will be affected by the 2017 code changes, as well as thousands of others across the UK. Those cases will not diminish, nor will the huge drops in rent, and that is having a devastating effect on a lot of small landowners and property owners around the country.

Q2 Julia Lopez: Could you be a little bit more precise on case numbers? How many people have directly approached Protect and Connect to ask you to lobby on their behalf? You have said that there are still a large number of cases, so can you put a number on that?

Anna Turley: I would say that we are dealing with in the region of a few thousand. I have a number of case studies from Members' constituencies around the country. I am afraid that I do not have a total overall figure, but there are 33,000 site owners around the country who are affected by this. Thousands of affected people have come forward to us via social media and lobbied their MPs. I would be happy to write to the Committee with a full number, but as I said, it is in the thousands. This is not a small number of unique people; this is par for the course. Colleagues here will represent their members in such cases, too. They are not a small minority that we have cherry-picked; this is happening across the board.

The campaign was set up because there was no way for, say, a church in Scotland, a rugby club in Wales and a farmer in Surrey to come together to stand up for their rights as landlords, to talk about how this was affecting them, and to have their voice heard by Government. Legislation was continuing to be developed, through pressure from mobile operators, which have long-standing and strong connections with Government through their large lobbying organisations. The views of ordinary people about the impact of the legislation on them were not being heard.

Q3 Chris Elmore (Ogmore) (Lab): On the 90% to 95% reduction that you mentioned, will you set out some examples of the impact that is having on site owners, churches and community groups? What challenges will they face as a result of these significant reductions?

Anna Turley: Absolutely. Someone in Cambridgeshire wrote to us who has two masts on their farm:

> "I have recently gained Planning Approval for 5 Houses on my land Immediately next to the mast positions. Not only do I appear unable to refuse to renew the Lease…their current offer is derisory at £750 per annum which is less than 10% of the current rent."

Another, in Peterborough, said:

> "It's been two and a half years out of lease, they had agreed all the new terms of the lease, just about to sign off. Then all change and they pulled out, and offered £500 per year and not heard anything since. These tower operators make dodgy used car salesman seem like Saints."

We have hundreds and hundreds of those. Churches, for example, are saying that they can no longer keep to their plans for the upkeep of their buildings. Sports clubs say that they will have to ask parents for more, so that their kids can play on the team. The impact of a rent cut from £4,000 to just £350 is devastating for small community groups and small businesses. They feel that nobody is standing up for them or listening. The impact of the new legislation will make that even worse.

Q4 Chris Elmore: In your organisation's view, how is the imbalance between providers and telecoms companies resolved? How could we improve the Bill?

Anna Turley: The first recommendation would be to go back to the Law Commission proposals of 2013. The Law Commission suggested a market-based valuation approach that was closer to the previous approach but still delivered savings to the operators. That was widely accepted as a very positive way forward. If that were taken as the approach to valuation, it would deal with the root causes of the issues and the imbalance brought by the 2017 changes, which essentially gave all the power to the operators.

As for the Bill, a number of further changes will damage and affect smaller landlords. For example, the Bill brings in backdated payments. Again, that could have a devastating impact on a small community group that is being asked not only to accept huge cuts in their rent, but to backdate their bills. There are issues on the definition of "occupier", which others will talk about. That could give operators the opportunity to change or

modify agreements that were entered into in good faith and still have time to run. We would like more protections for landlords, to protect them against poor behaviour by operators. For example, alternative dispute resolution should be mandatory. There should be the power to impose fines on operators for bad behaviour. We would like a statutory code of practice for them as well.

We are also very concerned about changes to the Landlord and Tenant Act 1985. We do not believe the reforms to valuation should be extended to the new legislation. That could set a huge precedent for all kinds of things such as wind turbines, and could bring the 2017 changes into effect for thousands of people who previously were not covered.

We would also like to see an evidence base; that is one of the most important things. Five years after the changes were brought in, there has been no full impact assessment of the 2017 changes. There is no evidence base, but it was promised, during the passage of the Bill in 2017, that there would be a full assessment by 2022. We have not got a clear enough sense of the impact of those changes. Here we are again, bringing forward new legislation without having a proper evidence base for those 2017 changes.

Finally, we would also like more reporting requirements on the operators. We have no evidence that the money they have saved since 2017 has gone back into building new infrastructure. Everybody wants connectivity. All our members want better connectivity and wi-fi, but the reality is that money is not being invested back into the infrastructure. It is disappearing into the profits, and there is no onus on operators to show where that money is being saved and how it is being used. We would like there to be more reporting requirements on them.

The Chair: Before Chris Elmore asks another question, let me say to the other two witnesses, who are appearing virtually, that if at any stage they wish to add anything to what has been said, please indicate that to me, and I will call you.

Q5 Chris Elmore: Dr Trotman, do your association and your members think that the Bill addresses the imbalance between site providers and telecom companies?

Dr Trotman: No, it does not. The Minister hit the nail on the head: you need balance in the market. What the 2017 changes did and what the part 2 changes will do in this Bill is further skew the marketplace. As Anna said, if the Government had taken forward the Law Commission's recommendations back in 2013, we would not be in this situation. We would be moving far faster towards universal coverage, which we all want, and which, as the covid-19 pandemic proved beyond all reasonable doubt, we all need. The problem we have is that this element of distrust between site providers and operators has shifted clearly in favour of the operators. The market is not working as it needs to.

As far as the CLA and I am concerned, it is incumbent on the industry, rural organisations, telecom companies and trade associations to come together and work out the differences. It is the role of the Government to assist in that process. If we cannot get the balance right, effective deployments will be delayed. That delay will severely limit the ability of rural communities to increase social inclusion, and reduce the ability of rural businesses to pick up and recover from the pandemic, and from the cost of living crisis that we are likely to face in the next six to 12 months. We need to get the balance right, and we still have not got it right.

Q6 Chris Elmore: Does part 2 of the ECC improve communications and engagement with the industry?

Dr Trotman: No, it makes it worse. That is our concern. We have an opportunity here to bring the industry together. Unfortunately, what part 2 of the Bill does is pull the industry further apart. The sector and the market was beginning to settle down after the 2017 changes. The Government then decided that the changes were necessary. We do not know why—as Anna said, there has been no real assessment of the impact of the changes on the market place.

On the case numbers that the Minister was talking about, you have to bear in mind that a lot of these agreements are placed under non-disclosure agreements, so we do not have the information we need to assess how wide the problem is. Given all the cases we have, it is clearly a very serious problem. The key is for the industry to get the balance right and for the Government to assist.

Q7 Chris Elmore: Should the alternative dispute resolution mechanism be mandatory, or voluntary, as is proposed in the Bill?

Dr Trotman: If the Government could give us the assurances and safeguards that we need that a voluntary system would work, I think that would be satisfactory. However, we have not seen that so far in our discussions with Government officials. If it is going to work as effectively as we want it to, it will have to be a mandatory mechanism.

If the ADR system works, it will reduce tensions in the market, because it means that site providers, for example, who are in dispute with the operators, would not be threatened with going before the courts. There would be an opportunity to negotiate under the premise of an arbitration process. However, we must ensure that that is available. That is where we need the safeguards. If we have those safeguards, and they are clear and consistent, then a voluntary system may be appropriate. However, from what we have seen so far, that will not be the case. We are not certain that the Government's guarantees will work—that is the key point—so it has to be a mandatory system.

Q8 Chris Elmore: Ms Griggs, good morning. Could you also answer that question on the AGR, please? Should it be compulsory, or voluntary, as set out in the Bill?

Eleanor Griggs: My opinion is very similar to Charles's, really. As it stands, I cannot see any option other than to make it mandatory to protect our members, who do not necessarily have that negotiating power, given the statutory powers that operators have, which could potentially be increased should the Bill, as introduced, go through.

Q9 Chris Elmore: I have two last questions for you, Ms Griggs. First, I am interested in some examples of where tenant farmers are being impacted by the reductions—similar to Ms Turley's point on some of the broader community groups. Secondly, in moving forward, does the risk lower rents impact on farmers' decisions regarding land access for masts and other

telecoms devices? In essence, what are your members saying on the broader NFU's work around the Bill and improving infrastructure for digital communications?

Eleanor Griggs: Yes, a lot of members have contacted us over the past few years, including quite a few recent cases. Obviously, those are under the 2017 changes. Many do focus on the rent, because that seems to be the trigger point, but then, when you look at the 90% decrease in rent, and then at the further terms that operators are trying to claim on renewals, those too are very unfavourable. They are not included within the code—they are not code powers—and have the impact of limiting what members can do across not just a small area contained within the deeds, but sometimes much larger areas, and sometimes an entire farm.

On the valuation itself—the reduction in rents—at a time when agriculture is seeing the loss of its EU subsidy payments under the common agricultural policy, it needs to be looking at alternative income streams. That, in itself, means that they will not be looking at mobile phone masts, as they did pre-2017, to get those income streams, but—this is leading on to the second part of the question—farmers will be looking to try to get income streams from every little piece of their land now. That will mean that there will not be any scope for something that does not pay very much money, but also does, or potentially could, include quite a lot of hassle through behaviours of operators and contractors when they are on land. It is not a very attractive prospect to have an operator on land now.

The Chair: Thank you. Will any Members wishing to ask questions please indicate that? Ruth Edwards.

Q10 Ruth Edwards: I refer the Committee to my previous declaration of interest. Ms Turley, I want to ask a point of clarification, please. You mentioned that 33,000 site owners across the country were affected by the legislation. Is that 33,000 site owners in total or 33,000 whom you believe have been particularly badly affected?

Anna Turley: That is in total.

Q11 Ruth Edwards: And roughly what proportion of them have reached out to your campaign?

Anna Turley: Well, we know that a third of them have had reductions of around 90% or 95%; that is from our own survey approaches. Going back to the Minister's first question, I could write to the Committee afterwards with the exact number. Thousands of people have written to us through social media and email, and have responded to our website. I do not have a total number for all those who have contacted us, but there are thousands of case studies across the country.

Ruth Edwards: You must have a rough idea. Is it something like 10% or 50%?

Anna Turley: I would say that probably about 4,000 people have reached out to us, but again, people have to be aware of our campaign. They have to have found us—come across us on social media. They have to have been engaged with us. It does not mean that there are not an awful lot of people sitting and suffering in silence. Part of the reason for setting up this campaign was that there were people who were just in despair and really struggling. Our campaign was set up to give them a voice and to give them access. I think this is really important. When the legislation was made previously, you were hearing only from mobile operators—those on the other side. There is no roll-out and no connectivity without people hosting a site on their lands. These people are fundamental to us hitting our targets, and we need to make sure their voices are heard in this campaign.

Q12 Ruth Edwards: How does the current rent valuation for phone masts compare to rents that other utility providers pay to landowners?

Anna Turley: I am not sure about that, but I know that internationally we compare very well. Our rents pre-2017 were not significantly higher than those in other countries, like Germany, Spain, Italy and others that are substantially ahead of us in the roll-out. I do not believe, and evidence does not suggest, that cutting these rents has actually increased our roll-out and our connectivity.

If you want to make the comparison with other utilities companies, the issue for all of those is that they are very tightly regulated industries, whereas there is very little regulation, and very little accountability and transparency, on the telecoms industries. If they are to become an essential utility—that may be the way we go, down the line—it is fundamental that the same kind of transparency, accountability and regulation is placed on them as is placed on utilities at the moment. That is not the case. We have no idea whether the savings that have been made through this have been reinvested in new infrastructure. There is no onus on these companies to do that. The Government are continuing to subsidise them with things like the shared rural network. It seems to be money after money towards these companies, without any indication of whether that money is actually being invested in helping us to achieve our connectivity outcomes.

Q13 Ruth Edwards: Tell me more about your campaign. How is the organisation set up?

Anna Turley: We are funded by an organisation called APW, which is a company that is a telecoms—sorry, a company that owns a land infrastructure itself. But as I say, we are supported by colleagues like the NFU, the CLA and others who back our campaign, and we represent all the site owners that have contacted us over this time to get their voices heard.

There are huge organisations, like Speed Up Britain and Mobile UK, that have very good connections with Government and are able to lobby and present their side of the argument. Until Protect and Connect was set up, there was no collective voice—no unified way in which site owners could speak to Government and tell their story. I think it is really important that we hear about this. I have examples here of constituents of your own who are saying, "We have telecoms masts. In view of the impact on our rent, I would certainly not have allowed the siting of masts on my property." A number of people and organisations around the country would not have had this voice if we were not providing this campaign.

Q14 Ruth Edwards: Is APW APWireless?

Anna Turley: Yes.

Ruth Edwards: So that's the phone mast lease investment firm?

Anna Turley: Yes.

Ruth Edwards: What's their interest in this?

Anna Turley: Obviously they are a site provider—

Ruth Edwards: So they would stand to gain substantially financially if we increased rent valuations.

Anna Turley: They have been losing substantially since 2017, so, yes, of course there is a financial interest. The point of the campaign is that they, by themselves, do not have a voice, and without their funding this campaign neither would all the other affected organisations—charities, community groups and others. If a representative of Speed Up Britain were here, you would recognise that there is a financial interest for mobile operators as well.

We have been very clear about the issue. Of course, the valuation is important and the money is important. I am a member of the campaign because bad policy has been developed over the past few years that has basically put all the power in the hands of a large number of mobile operators. Ordinary people around the country have been absolutely hammered by that and have not had the opportunity to express the impact on their lives and livelihoods. The campaign is a really important one to address that balance.

Ruth Edwards: Just to be clear, I do not think that there is anything wrong with APWireless lobbying for their interest; like you say, big telcos would as well. For clarity and transparency, however, I think it is important for people to note that Protect and Connect does not just represent small landowners and community groups; it also represents APWireless, which describes itself as one of the world's leading mast lease investment firms, with thousands of leases in 21 countries across the world. I think it important that we have that on the record.

Anna Turley: Absolutely; no problem with that.

The Chair: I remind Members that we should confine ourselves to questions, not to straightforward dialogue.

Q15 Kevin Brennan (Cardiff West) (Lab): This is quite an interesting Bill. I served on the 2017 Bill Committee, and at the time I thought it was interesting that a Conservative Government wanted to severely restrict private property rights. Nevertheless, I think we were content to support the principle that the legislation might unlock a problem. But, Anna, are you saying that that is not what has happened? Is that a fair assessment of the overall criticism of the Bill by both large and small landowners who have an interest in this?

Anna Turley: Yes, I think that is the case. The fact that we are back here again shows that roll-out has not improved, nor has connectivity. We have had further subsidies through the shared rural network. More than 300 cases going through court have been bogged down, whereas prior to the 2017 legislation barely a handful of cases went to court. That has resulted in a huge amount of litigation and conflict between site owners and operators, which simply did not arise before. That is holding back our roll-out and affecting GDP. We are falling behind our international competitors. The changes in the 2017 code mean that there is now so little incentive for people to host sites on their land that we are at risk of further jeopardising our connectivity goals and achieving the outcomes that we all want.

Q16 Kevin Brennan: You presented the case that someone might own a bit of land, and they would have previously got £1,000 for the site and now they are only getting £50. I can honestly say that that was not envisaged when the Bill was discussed in Committee in 2017. The Government never suggested that; everyone knew that the legislation would suppress rents for private property owners, but no one really understood that there would be a 90% suppression. Is that genuinely typical, or are those outliers in terms of what has happened to people's private property rights and their ability to raise rent from their property?

Anna Turley: Going back to your point about the Bill, that was not what was envisaged at the time. The impact assessment predicted a reduction of around 40%. Even Speed Up Britain has said that the average reduction is around 67%. We would dispute that, but without the evidence it has been incredibly difficult to show that. We have a huge number of cases where the operators have come in at a 90% to 95% reduction. That is par for the course.

There is an incentive for the operators to take cases to court to try to push for the biggest cuts that they can, because they can apply that across the board. The frustration is that we see them come in with large rent reductions, often bullying small landowners, families, small charities and community groups. Those people are having to accept cuts of between 90% and 95% because they simply do not have the wherewithal to go through lengthy legal processes to combat the huge strong legal arms of those organisations. They are simply having to submit to that.

To go back to your point about outliers, we have also tried to get information about the impact on local authorities, because a huge number of local authorities host these sites, as well as a number of hospitals and other public buildings. Again, we are seeing 80% to 85% cuts to local authorities. Leeds City Council, for example, has taken a reduction of 85%. That is thousands of pounds lost to local authorities. At the same time as we have heard that dairy and other farmers are being encouraged to expand and diversify their income, or local community and charity groups are being told to be entrepreneurial and to diversify their income, local authorities have had huge cuts over the past decade, as we know, and they are trying to get their income wherever they can. It seems crazy for them, essentially, to be subsidising private companies that might be making £10 billion in profit last year. That is money taken away from our local authorities, small charities and community groups, and it is not a small handful of them; this is happening across the board.

Q17 Kevin Brennan: My final question is to Dr Trotman. What is your response to the charge that you are in effect trying to thwart the Government's levelling-up agenda in what you are doing? Are you trying to stop essential national infrastructure rolling out? The state can reasonably suppress private property rights in order to bring about such a policy aim. This is a case in which the state, reasonably, is doing just that. What is your response?

Dr Trotman: First, we have to understand what the Government's levelling-up agenda is to begin with. If we look at the levelling-up White Paper, out of 332 pages, there are only 39 references to "rural", so maybe the Government's objectives do not relate to rural areas. There needs to be a levelling up not just of north and south, but of rural areas compared with urban.

We have always said—I said this earlier—that, as far as we are concerned, our overall objective is universal coverage, because we can see the benefits. The very fact that I am Zooming into this meeting at the moment illustrates the benefits of effective and affordable broadband connections. We understand what the benefits are and we want to see faster deployment, but we also want to see both parties playing fair. This is where I said that the ADR mechanism is a workable solution, if we can get it right.

We have to look at the positives of this as well. There is one big positive in terms of rural wayleaves on fixed-line infrastructure. With the NFU, we secured from Openreach and Gigaclear—the two big infrastructure providers for fixed-line connectivity—a wayleave agreement. We have had that since 1 October 2018, and it works. If we can get it right for fixed-line rural wayleaves, what I do not quite understand is why we cannot get it right for fixed-line urban wayleaves—Anna's point about local authorities is a good one—and in the mobile sector.

The major criticism that we have of the 2017 changes and of this Bill is the fact that we are talking about mobile infrastructure. We are also talking about the tactics being employed by mobile operators, which at the beginning of 2018 were not that conducive to effective negotiation. Basically, it was, "We'll offer you a little carrot, but if you don't agree, we will hit you over the head with a big stick." Hopefully, we are getting away from that, but again, it underlines the point that we have a major market imbalance, which we have to get right if we want to get to the point of universal coverage.

The Chair: Before I bring in Rebecca Long Bailey, Eleanor Griggs, did you wish to say something?

Eleanor Griggs: I have just a couple of points. If statutory powers are given, there needs to be some sort of accountability on the part of operators, with, essentially, sanctions if those powers are abused or not used responsibly. That sort of thing needs to be considered, because at the moment there does not seem to be any comeuppance for the poor behaviour that my members have had to endure. Are we looking at consensual agreements that are reached by negotiation, or are we looking at consensual agreements that are reached because somebody cannot afford to defend their position or get slightly more favourable terms at tribunal? It is quite cost-prohibitive, certainly for the smaller individual landowners. I do not know about the monopoly landlords that the Bill's impact assessment talks about quite a lot, but it is quite prohibitive for our smaller members.

I would also like to make the point that the NFU has an annual digital technology survey. The most recent figures—we have not quite had the 2021 figures in yet—are the 2020 figures. Going back to 2015, 29% of our members reported that their outdoor mobile signal was reliable. By 2017, that had risen to 42%. Obviously, that is a really big increase from 29% in 2015 to 42% in 2017. By 2020, it was still at 42%, so no advances have been made from the introduction of the code, essentially; that is quite important. Various other figures mirror that—smartphones with access to 4G and things like that. It just shows a stagnation from 2017 onwards. We just need to be careful that that does not continue or, in the worst case scenario, get any worse.

Q18 Rebecca Long Bailey (Salford and Eccles) (Lab): One observation that I have certainly made as a constituency MP is that community groups and small businesses that are faced with applications from telecoms companies often tell me when I assist them that they feel powerless, either in objecting to the proposals themselves, or in negotiating decent terms and conditions for the licence or lease agreement. They simply cannot afford the costly legal advice that would be required to get a decent deal or to object. How will the Bill exacerbate that inequity, and what amendments should be put in place to ensure that we level the playing field?

Anna Turley: That imbalance of power is absolutely something that we see throughout our case studies. If I may, Ms Long Bailey, there is someone in your constituency who has had a mast and a hub on their property for 25 years, and EE is now trying to force a rent reduction of around 86%. They said:

"On this basis we will not renew any lease"

and that they will do everything in their power

"to have the site removed, all land owners near us are aware of the situation and will not entertain the idea of situating on their property."

That goes exactly to the heart of it; people just feel powerless. Many often cannot have the site removed even when they want to, because of the legislation. It is having the knock-on effect that people do not feel incentivised, or do not want to have the site on their land, not only because of the lack of income, but because of the disparity in power and the threatening legal pressure from those companies. It is a David and Goliath issue. People are having to take on huge companies with huge legal arms, and they just do not feel that they can compete with them. That is a real issue.

We have suggested a few ways in which the Bill could at least make the negotiations fairer by making the ADR mandatory so that operators are obliged to undertake that. There ought to be fines for poor behaviour. There ought to be more scrutiny and a code of practice to put an onus on better behaviour from the operators in the way they deal with site owners. We think that would go a long way to addressing that balance, as well as putting some reporting requirements on them.

Eleanor Griggs: Yes, I would say pretty much what Anna has said. For us, it is about looking at the Landlord and Tenant Act and how it will affect a lot of our members who are currently on landlord and tenant leases that are due to expire or perhaps already have. According to the figures from Mobile UK that were used in the impact assessment, there are just over 7,000 expired leases, with another 2,000 due to expire within one year. Bringing the Landlord and Tenant Act valuation for renewals in line with the code removes the transitional provisions that were intended to ease landlords into the new 2017 code. It means that the holders of the leases that are going to expire will have no time to prepare financially for the sudden income loss that they will face. We would look at removing that proposed amendment to the Landlord and Tenant Act.

We would also look at the interim rents side of things. As Anna has alluded to, there are potential issues that could mean that a small landowner would end up having to pay back rent to a large operator. We have a member in Mr Double's constituency who had a lease that was due to expire that was achieving a rent of £3,500 a year. The renewal figure that he received was £17.50 a year. If the operator were to apply for an interim order and that order took a long time to come through, or the court took a long time to make that order, our member would still receive the £3,500 in the meantime. Then, if that took a year, he would have to pay back almost £3,500. Operators could use the proposed interim arrangements for indefinite periods of time, rather than looking to eventually get to either a court or tribunal-imposed agreement, or a consensual agreement. There are implications for landlords.

Rebecca Long Bailey: Thank you. Dr Trotman?

Dr Trotman: There are two things here. First, we understand that there is a lack of awareness as to what the code is, what it is meant to do, how it actually operates and the various tactics that are used, whether they be operators or site providers. Secondly, leading on from the lack of awareness, there is a lack of education. We are not just talking about on a wider scale—the general public, or site providers who may be in your constituency or anywhere across the UK; there is a lack of understanding and a lack of awareness within the industry itself. That is an important point.

One of the key fundamentals in resolving that issue is to have a code of practice that actually works, which we have from the 2017 revision of the code. At the moment, the code is doing absolutely nothing. Eleanor and I were part of a working group that drafted the initial form of the code of practice. What we have now—how it actually works in practice—is not worth the paper it is written on.

If we are going to have a code of practice and that is going to be a requirement of the revised code, let us make sure that that code of practice has some legal teeth. The only way it can have legal teeth, at the moment, is if it is appended as an annex to a code agreement. Very few site providers would understand that, and from what we have seen it is likely that very few agents and solicitors who deal with the code agreements understand that either.

Again, it is a case of getting the information out there, getting people educated as to what the code is and how it works and increasing the level of awareness. By doing that—again, going back to the point I made right at the beginning—you are creating a balance in the marketplace; you are having a more equitable system as we move forward. That then leads to faster deployment, and our ultimate objective of universal coverage. With what we are doing, if we have a deadline of 2025 or 2030, it is highly unlikely that those will be met, because there are too many problems and complexities within the system as it operates at the moment.

The Chair: If you are finished, are there any other questions?

Q19 James Grundy: I refer the Committee to my earlier declaration of interest. We mentioned the issue of particular sites and the considerable reductions in rent. Is that a universal problem across all telecoms companies, or are there any particularly egregious offenders regarding the practice of aggressive rent reduction?

Anna Turley: That is a really interesting question. We have not seen particular companies standing out any more than others. I think that they all have strong legal arms and come in with a very strong approach. However, what we have seen change, even since the 2017 code changes, is the development of tower companies, which I think is an interesting thing that has not really been taken into account when looking at the new changes.

These middlemen have been created, where tower companies will now rent the site from the landlord and use the code to cut the rent that they are paying, but will continue to charge high amounts of money to the telecoms companies—Vodafone, EE, Three, and others. The savings are not actually going back to those original companies, but somebody is making money in the middle. I think that is an important change in the market, partly, I think, because of the 2017 changes, which has not been properly explored.

Again, I think that we should be looking at that before we change this legislation, because the development of tower companies has distorted the market even further. It has not resulted in reinvestment in infrastructure, and is essentially creating middlemen who are profiting off the changes brought in to essentially accelerate 5G roll-out, and that money is not going back into the development of infrastructure.

Q20 James Grundy: Are those changes, with the creation of those middlemen tower companies, largely developments since the 2017 review of the legislation?

Anna Turley: Yes, that is when we started to see them emerge. They are a recent phenomenon.

Q21 James Grundy: Just for clarification, on that basis, do you think that the pressure for dramatic rent reductions is coming from those middlemen companies, rather than the telecoms companies themselves?

Anna Turley: I think that they are certainly playing a role in it. We have seen examples where, as I said, they have continued to charge, say Vodafone, £17,000 a year for a site, but then slashed the rent to the actual site owner to a few hundred pounds. That is absolutely a huge driving force, coming from profiteering, from those guys in the middle.

The Chair: If there are no more questions, I thank our three witnesses for a very informative session, and for giving us their time. Thank you very much.

Examination of Witnesses

John Moor, Dave Kleidermacher and Dan Patefield gave evidence.

10.19 am

Q22 The Chair: We will now hear oral evidence from John Moor, managing director of the IoT Security Foundation; Dave Kleidermacher from Google and the Internet of Secure Things Alliance; and Dan Patefield, head of programme, cyber and national security at techUK. We have until 11.25 am for this session. Can I ask the witnesses to introduce themselves, starting with Dan?

Dan Patefield: Good morning, everyone. I am Dan Patefield. I lead the cyber-security programme at techUK, which is the national trade association for the digital and technology sectors.

John Moor: Just before I introduce myself, let me say that it is an honour to be here. This represents a milestone moment for me, seven years in the making. Seven years ago, I set out on this journey to understand what IoT cyber-security was about and its challenges, so I am honoured to represent our membership and the executive steering board. I am John Moor, managing director of the IoT Security Foundation.

Dave Kleidermacher: Hi, everyone. My name is Dave Kleidermacher; hopefully you can hear me okay. I am the Google vice-president of engineering responsible for the security and privacy of the Android operating system, the Google Play app store, and "Made by Google" products including Pixel phones, Nest smart home products and Fitbit wearables. I am responsible for security and privacy, including the certification strategy for the company—how we assess and demonstrate compliance with security standards and privacy standards.

The Chair: Thank you. I will move straight to the Minister for questions.

Q23 Julia Lopez: Thank you, Mr Stringer, and thank you to all the witnesses who have come here today.

John, you rather touched on the challenge: this is an area that is very dynamic. All of us are learning what the security risks are, and in Government—which often moves very slowly—it is a particular challenge to manage such a dynamic, changing picture. That is why in this legislation, we have set out some broad principles and basic requirements, but a lot of this has to be secondary legislation so we can keep up to speed with all the changes that are going to be happening to connected devices, and some of the risks that will come with that. I think it would be very helpful if you could set out for the benefit of the Committee how this picture has changed over the past few years, where you think things will be moving, the extent to which connected devices will be in our homes in future, and some of the security risks that will present.

John Moor: When I started out seven years ago, I was invited to take a look by the chairman of the organisation I was working for at the time, the National Microelectronics Institute. He was the CEO of an IoT company. I confess, I had not seen what the challenge was, so when he invited me—"John, go and take a look at IoT cyber-security"—I thought, "Why me? What's the challenge? Isn't this thing just a tiny part of a well-established body of knowledge about cyber-security, and why me?" My background is in electronic engineering—semiconductors.

As it turned out, when I went and had a look, it did not take me very long to realise, "My goodness, there is a real problem here." I remember that at the time, a word I was using often was "egregious". As effectively a student coming into it, trying to understand the space, I looked at the evolution of computing, broadly speaking. In one era, we had computers—desktops, laptops—and we connected them up, and the security around those was pretty dire at one point, but we started to get on top of that. It is not perfect now, but it is a lot better than it used to be, and we are all very familiar now with doing security updates. The next phase was mobile. Mobile was not quite as bad as the era of PCs. It was better—still a few problems, but much, much better. Then we got to this thing called IoT, and it took a complete reset. It was totally egregious.

I come from the world of embedded systems engineering, and one of the first events we did was a summit we ran at Bletchley Park in 2015, just to do a landscape piece—just to try to understand it from chips to systems, bringing in the regulator. We had a representative of what was then the Communications-Electronic Security Group, but is now the National Cyber Security Centre, to try to understand where the issues are. Part of the problem, I think, is what I learned there as an embedded systems guy. We had a pen tester there, and he said, "If a researcher comes knocking on your door, don't turn him away." I thought, "That is a really interesting thing. What is he talking about?" We were talking about vulnerability disclosure. For someone who comes from embedding air gap systems, security was not a thing. It does not take you long to realise that when you start connecting things up, suddenly you expand this thing called an attack surface. Attackers can come from many sources, not in proximity to the thing that you are working on. Suddenly, you have this massive attack surface.

The whole idea about IoT—internet of things—is about connecting things up, so by its very nature, you are vulnerable. These things can come at you from many angles. What does that mean? It means different things to different people. I tried to understand what this thing called security was about. I immersed myself in the security community and straight away I realised there were different groups. If people start talking to me about data, they are usually coming from a data security or information assurance-type background. If they talk to me about availability of systems—keeping systems up—they usually come from an operational technology. What I mean by that is the sort of things we find in industry—process and manufacturing.

Then we have this thing called IoT. One of our board members expressed it very well. He called it the "invasion of IoT". What I took from that is that this technology is coming at us, ready or not. We established in those early days that we needed to have a response. The need is now. We could not wait for new standards and regulation, which is why we set up the IoT Security Foundation. Our centre of gravity is in best practice. It is saying, "Can we help manufacturers who do not yet see that the very fact that they are starting to connect things up poses a risk?" They did not, but now we are in a much better state. The body is developing.

I am delighted to be here to talk about this regulation. More needs to be done, without a doubt. A seminal moment for me was at the very first summit that I talked about. We had the chief technology officer of ARM, a chap called Mike Muller, give a talk in which he said, "The ugly truth is this: you will get hacked." That was quite an epiphany for me, because coming from an engineering background, we engineer our systems to be virtually perfect, but what we are witnessing now is that security is a movable feast that evolves. Out in the wild, things change. New vulnerabilities are discovered. Yes, you can do all you can to engineer it up front, but guess what? Once it is in the wild, this thing called resilience is so important. What that means, especially in terms of this regulation, is the software updating part

and especially the vulnerability disclosure. They are absolutely essential parts. That is part of what I have learned on the way.

I come to refer to IoT security as a "wicked challenge". By that I mean that I do not think we will ever perfectly fix it, because it is always moving, but we can address it. We can mitigate the risks to a level that we are comfortable with and can accept. Again, another phrase I learned is, "Don't let perfect be the enemy of the good." This is all good. This is progressive. This is what the world needs. Being part of the regulatory process to get here today, it became apparent that getting regulation right is so difficult. It is so easy to get it wrong, but going through the process, this is a regulation that we can wholeheartedly back. We think it is absolutely the right thing. It takes a step; it gets us on that security journey. We often talk about an on-ramp of security. It is about maturity. In terms of regulation, this is a fantastic first step, but more will come. The way it has been set up is exemplary. We can evolve it over time as we have to ratchet up the security for the benefit of consumers and society. I hope that little ramble gives you some idea about my journey and where I think we are at.

Q24 Julia Lopez: It would be helpful if the other witnesses could also set out the context from their perspective. I am particularly interested in Google's view, given it is a company with vast resources and a lot of expertise. There is a challenge for smaller operators about how to fulfil basic security requirements and how you think the basic set of requirements will help start that conversation with people who may not have even thought about the security of their devices before the legislative requirements come in.

Dave Kleidermacher: Let me start by saying I am so appreciative of the leadership role that the UK Government have taken to help us get to a better place for IoT security. I have been working closely with the Department for Digital, Culture, Media & Sport and NCSC for the past couple of years leading up to this. I have worked on how to measure security in digital technology for almost 20 years, and I believe that the lack of transparency in what the security ingredients are for digital technology has been one of the headwinds facing the entire digital world, even before the IoT was called the IoT. Of course, the IoT has made it much more urgent that we address this.

I agree that the minimum requirements we are talking about here are a really good starting point, but as we move forward and look at the secondary legislation, the really big challenge is how we scale this. The question about smaller developers is something that I am quite concerned about. At Google, we build our own first-party products but we also develop global-scale platforms. On Android, we have many manufacturers of devices across all different price points. We have millions of app developers across the world with whom we connect and work in all sorts of different environments.

One of the biggest challenges is how to monitor and measure these requirements, and how to make that work for small businesses in particular. That is the area I have personally been putting a lot of time into over the past couple of years. How do we build and establish an actual practical mechanism or scheme for measuring security at scale? There are a lot of details that go into that, but at the end of the day, we need a hub and spoke model. I can give you an example of a failure mode. The UK is, again, taking a leadership role, but many countries are looking at similar kinds of ideas and legislative concepts. The problem is that if every single country decides to create its own testing scheme for how to measure this, imagine how difficult it would be to have, say, a webcam or smart display, and then go to each country and provide documentation, provide the test results, explain how it works and go through a testing mechanism for every country.

As an example, for our Nest Wifi products, Google has had public commitments and transparency about our desire to have third-party independent security labs to test the products and assess compliance to these common-sense requirements. We have been doing that for a while now. We certify all of our products that way, but then a couple of countries at the leading edge of this started to ask us to certify again their schemes, and we did. That was a lot of work, to test to one scheme and certify and then do the same for another country with a different set of rules. The product did not change at all; it did not get any better because we were already certifying it. However, the work and the cost of doing that were significant. If we scale that to the full IoT, to all the countries which are interested in this—they all should be—then you can imagine how quickly it breaks down.

The hub and spoke model is looking at how we can work together to build a public-private partnership where there are non-government organisations, typically well-regarded international standards bodies, which take the great standards that we are developing, such as the ETSI EN 303 645 international specification on security requirements, which the UK has led in developing, and translate that into a practical conformance regime. An NGO can take that specification and the test specification—a sister specification, ETSI TS 103 701—and test a product once to have it certified for use in all of the different nations which adopt the same standard. That is the trick to this—the hard part that has to be solved as we move forward.

Dan Patefield: I think John and Dave have already mapped out the ever-growing risk landscape, so I will not reiterate that. From an industry perspective, there is clearly strong support for the ambitions of the Bill we have been discussing today, in implementing a minimum baseline that everyone should work to. Certainly, large swathes of industry are going beyond that, as Dave has outlined. I think I would join the other panellists in commending DCMS on the leadership that it has shown in developing the framework, not just with this legislation, but with the code of practice in 2018. I also commend it for playing a key role in developing the globally recognised standard in this space, EN 303 645—I always get that number wrong. The challenge that we have, and I am sure that we will come on to this, is that the code of practice—we supported its development and engaged industry in it—created an outline for best practice. However, it was never prescriptive; it was broadly focused. The practical challenge now is translating that into regulation that is workable for industry and consumers. I am sure we will move on to that, so I will leave it there.

Q25 Julia Lopez: Dan, you touched on the challenge about the need for simplicity, so that this very complex area is at least understood on a basic level—a general hygiene that everybody needs to apply. Ultimately, there is a need to thrash out a lot of this via secondary

legislation. I wondered to what extent that basic requirement has helped you have conversations with other members of your organisation who may not have been aware of some of the challenges coming down the line. Also, does the basic three-point requirement that we will be introducing help the conversation with consumers about what they need to do, and some of the things that they need to be demanding of products when it comes to security?

Dan Patefield: Going back to the code of practice, I am confident that across all 13 of those areas many companies have made good progress, and will continue to develop best practice that goes far beyond those requirements. I think it is a good approach to start with the three requirements that are included in the Bill; it is not the case that industry will be surprised by what comes out in secondary legislation. The practical challenge is translating the non-prescriptive code of practice into something that will be more prescriptive by definition.

There are a number of areas where I think there is more work to be done to smooth the path to compliance, if you like. We have got various elements. We have got the standard—that is not going to be a surprise. We know the security requirements—they are not a surprise. What we have not got is the boring bit—the technical specification that people in compliance teams within manufacturers are worried about. Quite often they have to then communicate that to their HQs—which are often in different parts of the world—and say, "We have got legal certainty that this is how it is going to work and this is how we achieve compliance". That is the bit that we have not yet got.

Q26 Julia Lopez: Just one final question for Dave Kleidermacher. You talk in your submission about not having static labels, but live labels. Can you take me through how that would look in practice for the consumer?

Dave Kleidermacher: It is a really important distinction, as we look at the so-called security ingredients in digital products. The analogy to food is a good one—but it also has its limits. What is good about it is that consumers deserve to have information at their disposal to be able to make better decisions about their health; in the case of food, that is their physical health, but in the case of digital technology it is their digital health. The concept that a consumer should easily be able to get a sense of the security status of a product is a very good idea. However, the main challenge is that food contents do not typically change—there can be a printed label that works okay. However, in the digital world, it could happen that you ship a product today and then there is a severe critical vulnerability, perhaps a hardware problem, that cannot effectively be mitigated or even patched. If that happens in the future, even a day after you have shipped it—this is a worst-case scenario—then if you try to put an attestation on the static label that the product is "secure" or meets these requirements, that attestation could be immediately incorrect. In fact, it could be dangerously misleading, and give consumers a false sense of security, so I believe that, while the ingredients label is essential, the user needs to have transparency. The consumer needs to have visibility here.

That label needs to be a live label. A simple example would be a QR code on packaging, although I am not sure how much consumers really go back to their packaging. We should also stress in-product experience wherever that is practical. It will not be practical in the case of every electronic product, but there is typically an app to manage many of our consumer IoT products. The app can provide an experience where the consumer can get the real-time, current status. That status can be as simple as a link that takes you to the certification page. As I mentioned earlier, we can have NGOs that establish the conformance programmes that we need to help to measure the security. It could just take you to the certification page to see the real-time status. If a product is deemed unsafe for use, it will become decertified, and the user will then know it.

The Chair: We now move on to the shadow Minister, Chris Elmore.

Q27 Chris Elmore: Thank you, Mr Stringer. This is only for Mr Patefield, unless anybody else wants to come in, of course. You talked, in answer to the Minister, about implementation and getting to the specifics of how that is delivered. In your evidence you refer to manufacturers and retailers being concerned about the timescales of the Bill, specifically the 12 months. I wonder whether you could expand on that, as I think you wanted to in your previous answer, and specifically on how secure devices could become obsolete because of the speed that it would take to implement the changes within the 12 months of the Bill's introduction.

Dan Patefield: There are two points on the timescales. There is the point at which the grace period will begin. For industry, we strongly think that that should be when the regulatory framework is confirmed and we know who the regulator is. That is the point at which that countdown should start. There are different views in industry on how long an appropriate grace period would be. Obviously, DCMS has confirmed that it will be no less than 12 months. Once we see that technical specification, a lot of parts of industry will have interpreted the code of practice in such a way that complies, so that will not be a problem for them, but some might have an interpretation that the compliance framework rules out—for example, around passwords. They might have to go back, certainly for security requirement 1, and make a hardware change. For a lot of these products, the supply chains are enormously long. Take a projector coming over from Malaysia. That will be 15 weeks in transit, and eight weeks getting through the broader supply chain in the UK through distributors and re-sellers. That already reduces the 12 months to seven months for manufacture and design. That is the difficulty that some manufacturers might face.

To the obsolescence point, there are two points again. In terms of when this comes in, we have to communicate it to consumers in such a way that it does not cause them to think that any devices that they currently have are obsolete in any way. That is a communication piece. It is about DCMS and the Government broadening that out, and helping consumers to understand what the legislation is for. More broadly, I am sure that we will come to the timescales for security updates but we do not want that to turn into some kind of perceived sell-by date. That is the minimum we will give you security requirements for, but the device is not useless after two or three years. Both those elements might lead to an increase in electronic waste and the kind of things that we want to avoid in a practical framework.

The Chair: Do either of the other two witnesses wish to comment?

Dave Kleidermacher: I would like to make a quick comment. Especially as we look forward in time, beyond the minimum requirements to the larger set that are codified into the ETSI EN 303 645, and extended requirements even beyond that, in different vertical markets there will be a desire to have additional requirements. For example, on the Android side, a Google-certified Android device already meets baseline requirements, so we are working with NGOs on how to define higher levels. For example, the strength of a biometric is really important on a smartphone, and that is not currently covered by the baseline requirements.

As we go forward, there will be an increasing set of requirements, and there is a way to balance that challenge. You will always hear of some manufacturers, including smaller ones, that have more difficulty meeting a certain requirement in a certain timeframe, and one way to help balance that is by focusing more on transparency about whether the requirement is met, versus requiring that all those requirements be met. I like to say that transparency is the tide that raises all boats. That is the key.

To go back to our analogy with food, it is not that on a label it says that you cannot have more than 50 grams of something; it is that you can compare the number of grams of carbohydrates and other ingredients between products. If you look at EN 303 645 and all its provisions—there are many—you could ask manufacturers simply to attest as to whether those are met. Yes, I still believe that there are minimum requirements that are critical, but in as much as we run into some difficulties on timeframes, you could just ask them to state whether they meet those requirements. That transparency will still be really valuable for consumers. Again, the NGOs that are setting up those conformance schemes can take the attestations of yes or no across the requirements and translate that into a health score, if you will, to help consumers make better decisions.

The Chair: Thank you. John, did you wish to add anything?

John Moor: Yes, I have a few points to make. First and foremost, most of my comments are about the here and now: what we are looking at, what is in front of us and the three requirements that are coming. Our assumption and that of our members is that, as we add to that, there will be an equally robust and rigorous process to determine what might follow. That is essential.

The labelling question is really interesting, along with certifications and attestations. All we can say about certification is, under these conditions, on this day, in these tests, those conditions were satisfied. I have heard the discussion about food labelling schemes come up time and time again as a "We ought to do something like that", but in our view that is not really practical.

One of the things that I had to get my head round when I came into this space was some people talking to me, saying, "Safety and security are the same, aren't they, John?" I had never had to get my head around that in the past, but I thought about it for about an hour, and I concluded, "Actually, they are not the same." They are not the same because safety is much more determinable. You can define the situation, the operating environment, the characteristics, the materials, etc., and you can figure out, "This is safe under these conditions." The difference in security is that it is dynamic—there is a changing environment, there is a human adversary at the other end. We might consider something to be safe today, as David said, but that changes over time.

Where do we place our trust? Do we place it in the product? I do not know that we do. Do we want to be looking up thousands of products to see what the certificates are? Where we really place our trust is in the companies that provide those products. It is interesting that, of the three provisions that we are talking about, only one is really related specifically to the product, and that is passwords. The other two are really about the processes that are involved in the providers of the technology—vulnerability disclosure and keeping the software updated.

I do think that certification is useful, but it is not a panacea; it only goes so far. What we are really looking for is something that we would term "continuous assurance". How do you do continuous assurance? That is the question for the industry to answer going forward, but some of the mechanisms that we have done in the past do not map well into a future world that is changing rapidly.

That is on the labelling front. It should be as simple as possible for consumers and for the producers of the technology. There is a discussion about whether we need another label. Certainly, many of our members favour integrating this into something that is already known. For example, could it become part of a CE labelling scheme, so that we add the security elements too? Those processes are well known.

Some of the discussions among our members about keeping software updated come down to considering what is a reasonable time to keep software updated. If you make it too short, that process is almost meaningless, and means that consumers probably will not buy a product if the update is, let's say, after only six months. If that update is too long, the company is carrying a financial legacy burden. What is the right point? I think we will find that out. Is it three years, five years, one year? We do not quite know yet. My own view is that it should be a length of time that is beyond the life cycle of the product. In that regard, it is variable and I do not know how that would quite be implemented, but that is what we have in front of us. For the here and now, this is what we are talking about; as for the future, we are assuming the rigorous.

In my view, security is an awful lot like quality. As we go into the digital world, we will see profound changes not only in the way that we use products, but how they are produced. We already know that: among our membership whole engineering teams have been reconstructed. The selling of physical products must be reviewed too, because are we buying a physical product? Often we are not, often we are buying a service. Do we actually own it? No, we don't.

Those are things that we will be working out as we go forward. We must understand those limitations as we do that, because we do not want to be taking the past into the future when the future looks quite a lot different from the past.

The Chair: Thank you.

Q28 Chris Elmore: One final question for techUK about part 2. Lots of organisations that you represent talk about the digital connectivity divide within cities

and large towns between flats and access for upgrading and automatic upgrading. You have said that the Bill could go further to deal with overground infrastructure and automatic upgrades for flats to resolve the problem. Could you expand on that and tell us what your members say about the challenges they face, because this is not just about rural roll-out or semi-rural roll-out, but changing infrastructure, including in boroughs such as Hackney and Camden—places where you would not automatically think there were connectivity issues?

Dan Patefield: I will lead on that question. techUK would be happy to give more thoughts on that in a written submission, but it is not an area I focus on. Internally, we split the Bill; I lead on the cyber-security element and another colleague leads on telecoms infrastructure. I am happy to get that question answered in a written submission.

Chris Elmore: Thank you.

The Chair: If there are no other questions from Committee members, I thank our witnesses for their time and contributions. I am sure that when Committee members come to consider the Bill in detail they will find those comments very helpful. Thank you.

Ordered, That further consideration be now adjourned. *—(Steve Double.)*

10.54 am

Adjourned till this day at Two o'clock.

PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

PRODUCT SECURITY AND TELECOMMUNICATIONS INFRASTRUCTURE BILL

Second Sitting

Tuesday 15 March 2022

(Afternoon)

CONTENTS

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

not later than

Saturday 19 March 2022

The Committee consisted of the following Members:

Chairs: † Caroline Nokes, Graham Stringer

† Baynes, Simon *(Clwyd South)* (Con)
Bhatti, Saqib *(Meriden)* (Con)
† Brennan, Kevin *(Cardiff West)* (Lab)
† Double, Steve *(St Austell and Newquay)* (Con)
† Edwards, Ruth *(Rushcliffe)* (Con)
† Elmore, Chris *(Ogmore)* (Lab)
Grundy, James *(Leigh)* (Con)
† Hart, Sally-Ann *(Hastings and Rye)* (Con)
Hollern, Kate *(Blackburn)* (Lab)
† Long Bailey, Rebecca *(Salford and Eccles)* (Lab)
† Lopez, Julia *(Minister for Media, Data and Digital Infrastructure)*
† Mishra, Navendu *(Stockport)* (Lab)
† Osborne, Kate *(Jarrow)* (Lab)
† Randall, Tom *(Gedling)* (Con)
† Vara, Shailesh *(North West Cambridgeshire)* (Con)
Warburton, David *(Somerton and Frome)* (Con)
Whitley, Mick *(Birkenhead)* (Lab)

Huw Yardley, Bethan Harding, *Committee Clerks*

† attended the Committee

Witnesses

Professor Madeline Carr, Professor of Global Politics and Cybersecurity, UCL

David Rogers MBE, CEO, Copper Horse; IoT Security Foundation Executive Steering Board Member, IoT Security Foundation

Catherine Colloms, Director of Corporate Affairs, Openreach

Simon Holden, Group Chief Operating Officer, CityFibre

Mark Bartlett, Director of Operations, Cellnex UK, representing Speed Up Britain

Juliette Wallace, Business Planning and Property Director, MBNL, representing Speed Up Britain

Till Sommer, Head of Policy, ISPA

Rocio Concha, Director of Policy & Advocacy, Which?

Jessica Eagleton, Senior Policy and Public Affairs Officer, Refuge

Public Bill Committee

Tuesday 15 March 2022

(Afternoon)

[Caroline Nokes *in the Chair*]

Product Security and Telecommunications Infrastructure Bill

Examination of Witnesses

Professor Madeline Carr and David Rogers gave evidence.

2 pm

The Chair: We are now sitting in public and the proceedings are being broadcast. We will start this afternoon's session with oral evidence from Professor Madeline Carr, professor of global politics and cyber-security, and David Rogers MBE, the chief executive officer of Copper Horse and an Internet of Things Security Foundation board member. We have until 2.40 pm for this session. May I ask the witnesses to introduce themselves for the record, please?

Professor Carr: Good afternoon. Thank you for having me. I am a professor of global politics and cyber-security at University College London in the computer science department, though I am actually an international relations academic, so I blend those two. I am also the director of the Research Institute in Sociotechnical Cyber Security, and I am the deputy director of REPHRAIN, the National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online, which looks specifically at protecting citizens online. It is a big consortium.

David Rogers: I was the original author of the code of practice and the lead editor during the process that is the basis for the legislation. I also chair the fraud and security group at the global mobile industry association, the GSMA. As you mentioned, I am also on the board of the IoT Security Foundation.

The Chair: Thank you very much. Members of the Committee will ask you questions in turn, but we will start with the Minister.

Q29 The Minister for Media, Data and Digital Infrastructure (Julia Lopez): It would be helpful if, for the Committee's benefit, you could set out your own background and interest in this area. I would specifically like to ask you about how this fits with international regulation of this space. What are other countries doing? Some of the witnesses on the last panel discussed the potential challenges if different countries are doing different types of regulation in this area. How can the UK show leadership in this space and try to minimise the burdens on businesses while protecting, and maximising the protection of, consumers?

Professor Carr: That is a very good question. In terms of international alignment, aligning these kinds of laws across jurisdictions is a challenge. I want to say from the outset that regulating emerging technology is understood to be a deeply problematic and challenging area. It is something that the UK in many ways has led on. A lot of thought leadership has come out of the UK on this. As David said, the work that has led into the Bill has been going on for many years in the UK, and has been funded by the UK Government through universities and industry. A tremendous amount of background work has gone on. There is the PETRAS—privacy, ethics, trust, reliability, accessibility and security—consortium, which was originally the cyber-security of the IoT consortium. We have worked on that for many years with David and others. The UK really has led on this. When we look at what is happening here and now, you would have to say that this is a country that is able to confront those kinds of difficult challenges and think about ways through them. No one is saying that it is easy; it will not be, but this is a very good start.

When it comes to looking at international alignment and the impact on industry, and particularly the manufacturers of these devices, there is already a lot of alignment. I have been doing some work through the World Economic Forum, where I am chair of the Council on the Connected World. On 15 February, we launched a global statement that spoke to the three initiatives that are being considered here, and an additional two in terms of IoT consumer devices. That statement has been endorsed by more than 110 organisations around the world, including Microsoft, Google, Qualcomm, DCMS, RISCS—my institute—and indeed David's organisation. There is a tremendous amount of international support for these initiatives and more. A lot of them are big industries, so I do not think there is necessarily a disconnect between governance of emerging technology and what is helpful for industry actors; I think there is actually a lot of alignment.

David Rogers: I will just point to some specifics. There is work ongoing in India, Australia, Singapore, Turkey, and the US, and many of those countries—and many I have not listed—base their work on what was originally the UK code of practice. The UK's code of practice was taken to ETSI, the European telecoms standards body, and was made into a European norm. That really, I think, has given the confidence for other countries to be able to adopt that as a scrutinised and good piece of work.

That is obviously not in isolation. ETSI is an industry-led organisation, and a lot of the work that has gone into that in advance, including through DCMS and NCSC, has been about looking at industry-based best practice. Organisations such as the GSMA worked on this in 2014, and, prior to that, in the smartphone world, have been building in hardware security and other measures, which have hardened connected consumer devices, so that work is certainly not in isolation. We are really standing on the shoulders of giants here, because a lot of the work is done; it is in endorsing good practice, and I think that is what the other countries are seeing, and they really have seen leadership from the UK in this space.

Q30 Julia Lopez: I wonder if you could set out some of the challenges in this space, in relation to the fact that there is such a breadth of devices that need to be governed, with different vulnerabilities, and how we try to ensure that we keep pace with all of the changes in technology that will be coming down the line. There are also the specific requirements of different types of connected devices, whether watches or fridges.

David Rogers: I will address that. The beauty of the IoT is that there are all these fantastic things being developed. When we started to look at what we could do, and a code of practice, we wanted to ensure that we

did not constrain innovation by mandating specific technical measures that might prevent some fantastic product being created. That is why we took quite a high-level outcome-based approach.

That also meant that it was measurable, even by consumers. If you look at the top three guidelines of the code of practice that have made it into the draft legislation, a consumer can look at those things, which I would call "insecurity canaries". If you see that a manufacturer does not have a vulnerability disclosure policy—so hackers and security researchers, for example, cannot report things to them—that is a big red flag, and I would not be buying that product. It is the same if the product does not have software update support, and so on.

We took a proportionate approach to the code of practice, and I think that that also led to the industry endorsement of it. This morning, I heard the techUK gentleman saying it is not specific enough; well, actually, the ETSI EN 303 645 is quite specific, and the compliance specification that goes with it is even more specific. For some bad practices, I do not think that we could be more specific than saying "Don't have default universal passwords". We want to get rid of "admin" and "admin". That is a ridiculous situation, in some parts of the market, that is unacceptable, and we must eliminate it from the market.

Q31 Julia Lopez: Do you have anything to add on this, Madeline?

Professor Carr: Just to say that we cannot anticipate all of the new devices that will come on to the market, of course. I think what David is saying is that it is necessary to have that kind of flexibility to adapt and accommodate those, as they come on to the market. However, it is really long overdue that we do something about this.

There are two types of security in these devices that we understand at this point, which need to be taken into account. The first is the security of the data that flows through them. Although they are very different devices, that is, in many ways, a common problem in securing data—particularly, of course, personally identifiable data. The second issue arising from IoT devices is that many of them have an impact in the physical world. That then begins to blur cyber-security with safety, and we have very different ways of approaching cyber-security and safety. What we tend to do with safety is test things, over and over again, until they break; then we know how they need to be built or constructed. That kind of homogeneity in an approach to design is very bad for cyber-security, because that is what gives us vulnerabilities across the whole landscape. Those are the kinds of issues that we need to grapple with. The devices themselves will continue to emerge and evolve, but the problems that we are grappling with now are common across devices, in a way. Legislation such as this will go some way towards addressing those problems.

Q32 Julia Lopez: David, I was interested to know that you were involved in the kind of practice being drawn up. I would be interested to understand the journey we have been on here; there has been an acknowledgment that a voluntary code of practice is not enough and legislation is required. Can you take us through that journey to legislation?

David Rogers: Yes, originally there was a "secure by design" committee set up with various companies—Madeline and I were on that committee. There were various discussions about the best way forward. I remember one suggestion being that all we needed to do was to educate consumers. After I banged my head on the table quite a lot, I think that in the end we realised that it should not be on consumers. They are not the ones who are creating the insecurity in the product and they are not in a position to do anything about it either—they are mainly victims. It was recognised that a lot of those issues have been in products for many years; I go back to the default password issue, but there are many issues around things such as lack of support for software updates.

I drew up the original code of practice and worked closely with National Cyber Security Centre and the Department for Digital, Culture, Media and Sport. I also worked with academia and the security research community, who are hackers from around the world who have been campaigning for those issues to be dealt with for years, because they are seeing it directly in their work. We spent a lot of time getting it right; we worked at the Information Commissioner's Office on some of the elements related to GDPR.

A voluntary code was published in 2018. However, manufacturers were put on notice at that point. By 2018, it was made public that this was the expectation; we expected the industry to improve. Some quarters were probably already compliant; you heard from Dave Kleidermacher this morning, who led the way in security improvements on mobile devices—from their perspective a lot of the stuff in the 13 requirements was already done. However, many parts of the industry have done nothing. It seems to me that they are quite happy to sit back and do nothing. That is why I think this work is necessary; there is a need for the big stick of enforcement, to be honest with you. They have been given plenty of chances, and not just since 2018—it is since the 1990s. It seems acceptable to them to carry on doing the same things that they have always done, such as buying in the really cheap software that is completely open and has old protocols and legacy issues that should have gone years ago. I am entirely supportive of taking action now—they have been given enough time. They should not wait for the 12 months—or whatever it is—for certain things to become mandatory. They should be doing this because it is the right thing to do for their customers.

My company carried out some research for the IoT Security Foundation on vulnerability disclosure. Again, that is something that is very visible; you can go to the website and see whether that company is open to security researchers and hackers reporting security issues to them. There is then a process that has been ISO-defined since 2014; it is dealt with and then the issue is made public once it is fixed so that consumers are secure. We discovered that about one in five of the companies that we surveyed—there were about 330 companies from around the world, representing thousands of products—was actually providing that to security researchers. That means that four in five IoT manufacturers did not have any way for security researchers to contact them. That is totally unacceptable, so we do need to take action. The companies have been given enough chances.

Q33 Julia Lopez: Finally, I just wonder how we use this as a moment to increase consumer awareness. You both suggest that the onus should not be on consumers,

[Julia Lopez]

but as a Minister I am still concerned that people do not entirely understand what we mean by "internet of things" and the extent to which we will have even more connected devices in the future. Could you set out what the security challenge will be in the future, in your opinion, and how we try to use this to educate consumers so that there is an informed customer base when product decisions are made in this area?

Professor Carr: I think the element that will impact consumer decision making the most will be the length of time for which the product will be supported. I remember having the conversation in a room in DCMS all those years ago about how we could possibly be expected to spend £1,000 on a phone that will not work in 18 months, that the company knows will not work in 18 months—it will not be supported—and to not have access to that knowledge. This is not just about putting labels on things; it is about the fact that we could not find out even as an informed consumer. I think the length of time for which the device is supported will have a major impact on consumer decision making and probably more than the other two things, because a lot of people do not care about passwords and a lot of people do not know what a vulnerability disclosure agreement is or what that means. Knowing for how long the device will be secure is like having an expiry date put on it.

That is an example of where a kind of market driver can impact consumer decision making, but one of the things that we know about cyber-security more generally is that, very often, market drivers do not work in this space. There is not really, to be honest, all that much of a market for cyber-security, as people do not really care about that. That is why we need to think about moving beyond the dominant narrative over the last 50 years that Governments stifle innovation. Even if we go right back to the beginning of digital technologies and the ARPANET and DARPANET, those things were wholly supported by the US Government. They were funded by the US Government; they were invested in by the US Government for decades before the private sector came on board. So there are these points where it is absolutely necessary for Governments to be involved and for governance to happen, because we cannot see the future. If people begin to lose confidence in these devices and they begin to fear—"I don't want my child to have something like that. I don't want Alexa in my house. I don't want people listening to my conversations etc."—all the incredible benefits that we can extract from those technologies will go by the wayside.

I will give just one very clear example of this. If you think about the huge effort that the banking sector put into making sure that people felt confident about banking online, spending money online and tapping their card—"When something goes wrong, the bank will take care of you"—the reason, the logic, behind that was that if people began to think, "It's not safe to bank online; it's not safe to use my card in these little shops," they would stop doing it. It was that investment in regulating it, locking it down and making sure it was safe that has allowed us to get to this extraordinary situation where you can walk around with no wallet and just a phone. It is that thinking that is important now.

David Rogers: I think the transparency point is fantastic. This work is not done in isolation. There is lots of work going on about lengthening software updates for lots of types of products, and there are different regulations happening in Europe and so on. Consumers should not have to know about the details. Madeline has said this. They have an expectation, a very reasonable expectation, that they will not be arbitrarily hacked into. We have all read the stories about things like baby cams being hacked into. That is totally unacceptable, because at the end of the day the company that created and sold that product that was insecure at the time it was created is responsible for it. Of course, they did not hack into it, but they left all the doors open, and they sold that product and made money and profit from it.

Yes, I believe that consumers should know that they are being looked after, and the length of time that that is provided for helps them to make an informed decision—it is a free market. Also, security should not be a luxury for the rich. You should not be required to replace your iPhone, for example, just because the support ends. At the end of the day, we are all impacted by security issues. The Mirai attack, for example, was an extremely large distributed denial of service attack, which basically took down large parts of the internet. It was all those small IoT devices, routers and things that had been taken over. The attack did not discriminate between who had those devices, those older devices or whatever, but the impact and scale of that attack was the problem.

That is why we need to ensure on an ongoing basis that, as the technology develops, we can put new requirements through the standards bodies and endorse them. This is the start of that lifecycle, to ensure that those products do not enter markets like the UK.

Q34 Chris Elmore (Ogmore) (Lab): To keep the conversation on consumers, eBay, Amazon and other platforms are not part of this Bill, but an awful lot of research out there suggests that they do not regulate what they sell. There are an awful lot of suggestions from organisations like Which?, whom we are meeting later, that those platforms' markets are often flooded with devices that are not secure, but are cheaper. Again, to go back to your comment about how security should not just be for the rich, if someone is looking for a cheaper type of product, they can go there and their thought will not be about security, but about how shiny and new, or refurbished, it is—how it looks very good and the same as what the other child in the class has, and so on. What are your views about looking at the online marketplaces? Is that the next step, through secondary legislation or this Bill? Should they be as responsible as the manufacturers, if they are wilfully selling products that they know are not secure?

In that vein, is there something in the idea of a reporting mechanism—either by the Department or some sort of regulator, annually or however long is appropriate—for whether these organisations and manufacturers are working to the standards that you so strongly set out? They have had years to deal with the standards, but many are still not doing it. I am suggesting naming and shaming, if you will, to give consumers better informed decisions.

A lot of people borrow money to buy these devices. On Second Reading, I expressed a concern that many people will look in a retailer or online, and go, "If that doesn't exist for this much time—if it only has two years on it and the loan is three years—why am I bothering to purchase it if it is obsolete in that time?" That is a

concern that many people have. Consumers potentially do not know what this or that means, but they know what "security" means, and if they think something is not secure, then, as Professor Carr mentioned, they think, "Well, I won't bother having that product, because it isn't safe", because that is how they view the word "security", which is logical, but not necessarily the best option given what they are looking for. There are several questions in there, forgive me, but they are interconnected with what the Minister was saying.

Professor Carr: I will try to answer as many as I can, as well as I can. I am sure that David has comments as well.

On educating consumers, that question of "Will the loan outlast my device?" is a very astute one, because consumers do not need to understand—they never will—all the ins and outs of phone or device security, but that is a very pragmatic response: "What actually am I buying? I am spending for three years to buy two years of a phone." That type of consumer education will snowball when people are presented with information on how long the device will last and asked, "Is that what you want?"

I guess online markets are already regulated. There are things that we cannot buy in the UK and that cannot be shipped here. It would certainly have to be a consideration that, ideally, devices that did not meet UK standards were not able to be shipped to the UK, but I guess that is the case with many consumer goods that we cannot buy online. There is a tendency to blame business in this scenario and to see manufacturers as careless or irresponsible, which surely some of them are. However, it is also the reality that businesses have to make a careful calculation on how they invest. If it costs more to produce a product and they are answerable to shareholders, they have to have a conversation about why they are spending more on a device that is already selling well and returning a profit. I am not saying that that is the way it should be, but that is the way the free market works.

Look at what happened with GDPR. In my work, we work a lot with senior business leaders and talk to them about how they respond to cyber-security regulations. They did not push back against GDPR or see it as terribly negative; they saw that it unlocked budget for them to use, because they could quantify what percentage of their global turnover a data breach would cost or what the fine could amount to. They can take that calculation to the board, and say, "Right—we mustn't have a breach or it would cost this much. How secure do we feel we are?" That is where such regulations can have a very positive effect on industries that would like to comply but cannot just invest in all the different aspects of a device without some justification. This gives that justification. It unlocks that funding in those board conversations about where investment in products should go.

David Rogers: Just to address the Amazon/eBay question, I have seen all this stuff. I have bought some of it to have a look at. A lot of counterfeit and substandard—the Chinese call them Shanzhai—products are available. I have conversations in which people say, "This is about buyer beware. You'd never buy a £9.99 smart watch. You should know that that's going to be dodgy," but as you said, people cannot necessarily afford it. There is a peer pressure element to it, and there is a sort of endorsement by the brand. If you go to Amazon, you expect it to be a quality product, so people are lulled into that sense of security that what they are getting is quality. In some cases, that is not the case. I fully agree that the companies that are retailing this stuff cannot just lay the blame at the door of the companies that are stocking and selling it. If it is on Amazon Prime, surely Amazon has a responsibility over that.

Earlier, Dave mentioned different regulatory regimes and that there may be some fragmentation around the world. I actually think that there is probably a lot of alignment and harmony. There has been a lot of work between DCMS and the National Institute of Standards and Technology in the US, so there is a broad understanding of what good looks like. If, either through some self-declaratory measure or by some endorsed mechanism of compliance, those companies are told to come up with a compliance statement, that helps the likes of Amazon and eBay to select their suppliers appropriately and then to remove them from their stores more easily. At the moment, it is kind of a wild west. They do not have any questions or answers.

Q35 Ruth Edwards (Rushcliffe) (Con): Professor Carr, you made some really interesting comments about the balance between regulation and innovation, and how it is not always as it is portrayed to be. Do you think the Bill strikes the right balance in those areas? Is there anything missing from it that should be in there?

Professor Carr: I think the Bill would be a hugely positive step. There is a lot more to be done in terms of regulating emerging technologies. As I said earlier, the UK is a country at the forefront of thinking about these issues and taking action. It is new territory, because we are not used to legislating about these things; it seems somehow interventionist, or that it stifles innovation. Actually, digital technologies have become so integrated into every aspect of our lives, from the most personal level to infrastructure, and we have not caught up with that in what we see as the acceptable responsibility of the Government, of individuals and of industry.

There has very much been a narrative that Governments need to stay out of this area. I think that is very dangerous and wrong, because that is how we have ended up in the situation we have been in. It is certainly a balance between those parties—Government, civil society and industry—but we are a long way from having that balance right. Governments are beginning to see that there is a mandate and that they have a responsibility. We see that not just in the UK, but certainly in the US, Australia, the EU. But there is a long way to go.

Q36 Ruth Edwards: Are there other specific security measures that you would like to see in the Bill?

Professor Carr: I would like to see the range of devices extended—in particular, where it talks about toys and safety devices. There is a whole category of other devices that should be included, particularly when we think about children. There is a market emerging now for tracking devices for children, or these phones, which are not really phones but communication devices. I think the scope of the devices should be expanded.

If I had a magic wand and it was up to me, I would say that devices had to be supported for a minimum time. Otherwise, you end up with the very distasteful scenario that we were just talking about, where people

who are less resourced are buying less secure devices and living less secure lives. I would like to see a minimum time that devices had to be supported.

I would say those two; I would go much further, but it is a good start.

Q37 Ruth Edwards: Thank you. Mr Rogers, I think you mentioned that four out of five IoT manufacturers still do not have a vulnerability disclosure programme—correct me if I am wrong. I want to put something to you that we received in written evidence from techUK, who gave evidence to the Committee this morning. In its written evidence, it says:

"Current proposals risk unintended consequences for manufacturers and consumers".

It points particularly to security requirement 2, which is to implement a means to manage reports of vulnerabilities, and notes:

"On vulnerability reporting, not all reports/vulnerabilities will require intervention. The Enforcement Body needs to carefully consider when to alert the public about security risks to ensure associated devices are not viewed as obsolete or that vulnerabilities yet to be mitigated are advertised to threat actors."

What is your response?

David Rogers: I will be frank: I think they have misunderstood what vulnerability disclosure is. As I mentioned, there is an ISO specification for this. The security research community and the hacking community have been campaigning for this for years and years. It is well established. A lot of the bigger tech companies have recognised that this is the right way to deal with things. I am sure that you understand vulnerability disclosure, but the process is that if a security researcher or hacker discovers a vulnerability, they have an easy way to report that to the company confidentially. That process typically takes anything from 30 days to 90 days. At the end of that process, a fix is issued, if that is possible. It may even extend for a longer time if it involves other companies. Then the security researcher is able to go public with their work, but that is only after a fix is issued. This has been fought out over a long period, and is the right way of doing things. It is agreed between the hacking and the tech communities.

There may be some education work to be done for those manufacturers who do not understand that this is the right thing to do. They should be implementing vulnerability management schemes internally anyway. I think John Moor mentioned this morning that it is about quality. It is about good software quality measures and good software design. We have seen some really catastrophic problems caused by vulnerabilities that have been sitting there for years. That is the old world. We need to move on from that. The new world is about continuous software updates and a continuous product security lifecycle. People cannot just ship and dump products on to the market and leave them there.

The Chair: Can I bring in Kevin Brennan, as we only have four minutes before this panel comes to an end?

Q38 Kevin Brennan (Cardiff West) (Lab): Professor Carr, you do not need a magic wand to get your wishes; you need an amendment. Would you welcome an amendment to the Bill that specified that devices have to be supported for a minimum time?

Professor Carr: Yes, I would.

Q39 Kevin Brennan: Do you own an Alexa-type device in your home?

Professor Carr: No.

Kevin Brennan: Why not?

Professor Carr: Because I do not trust them. There we go. I will not have one, because I do not trust it.

Q40 Kevin Brennan: Will the Bill give you sufficient trust to purchase and acquire such a device and have it in your own home?

Professor Carr: No, to be honest.

Q41 Sally-Ann Hart (Hastings and Rye) (Con): Very briefly, Professor Carr, if the security threat as regards connected products were substantially to change over the next few years, will the Bill cover those changes, or will some flexibility need to be built into the Bill to address them?

Professor Carr: It is impossible to answer that. That is what makes this type of legislation difficult. We do not know how the threats will emerge or change. A couple of years ago we could not have imagined that ransomware would be the threat that it has become, but the fact that we cannot anticipate the future with certainty does not mean that we cannot act now. Nothing will be sufficient to fix the insecurity of the digital world that we live in. No Bill will change that, but small bits of legislation beginning to address these vulnerabilities is the right way to go. I do not think that anyone should be afraid of doing this. This is the beginning of the future. Governments will not stand by forever and watch the damage and destruction that can be done by digital devices. We have to start somewhere, and I think that this is it.

David Rogers: I am coming from a slightly different position, but obviously I would like to see all 13 requirements implemented. I think that it does provide future proofing, because this provides the foundation of future trust for everything. Everything that we have written in there provides future underpinnings. If we are allowing industry-based organisations such as the European Telecommunications Standards Institute to maintain the specification for the future, that allows organisations to improve and add things. I think Dave mentioned biometrics, for example. They can go to ETSI and add to it, and let's allow industry to develop that. Organisations such as NCSC and DCMS are also there to input into those standard bodies. I think it is a really strong start.

The Chair: Thank you. That brings us to a slightly premature end of this evidence session. I thank the witnesses, on behalf of the Committee, for their evidence.

Examination of Witnesses

Catherine Colloms, Simon Holden, Mark Bartlett and Juliette Wallace gave evidence.

2.41 pm

The Chair: Good afternoon. We will now hear oral evidence from Catherine Colloms, MD for corporate affairs at Openreach; Simon Holden, the group chief

operating officer at CityFibre; Mark Bartlett, director of operations at Cellnex UK, appearing on behalf of Speed Up Britain; and Juliette Wallace, also of Speed Up Britain.

We have until 3.40 pm for this session. Will the witnesses introduce themselves briefly for the record, please, before I turn to the Minister? We will go left to right.

Simon Holden: I am Simon Holden. I am the group chief operating officer of CityFibre.

Catherine Colloms: I am Catherine Colloms. I am the corporate affairs director at Openreach.

Mark Bartlett: My name is Mark Bartlett. I am the operations director at Cellnex UK, representing Speed Up Britain.

Juliette Wallace: I am Juliette Wallace. I am the property director at MBNL, which is a joint venture between EE and Three. I also represent Speed Up Britain.

Q42 Julia Lopez: Thank you for attending the session. I do not know whether you watched this morning's session, but Protect and Connect and other witnesses put it that, since 2017 and the changes to the electronic communications code, roll-out has been even more difficult and slow, and that no progress has been made as a result. What is your response, as providers, to those concerns? Do you believe that the approach by operators has been too heavy-handed in the negotiations with landowners?

Mark Bartlett: On behalf of Speed Up Britain, we very much believe that the changes proposed in the Bill are needed to speed up the roll-out of digital connectivity across the country. Therefore, we believe that changes are required.

In that sense, though, we need to look back to before 2017 to understand the policy behind the changes originally made, and to understand that those were made in order to achieve the outcomes that the Government were already trying to establish. Without the changes in the policy of 2017, this ambition will not be met. Speed Up Britain continues to support the policy ambitions as laid out in 2017, but the fact is that the law as put down at the time is not working and created loopholes, which have been exploited, and that has meant that we have been unable to proceed at the pace we wanted.

Catherine Colloms: To give you a bit of context, Openreach is the national broadband network. We are in the process of upgrading the existing network, which is a hybrid copper-fibre network, to a new full-fibre network. The ambition is to build 25 million full-fibre homes and businesses by the end of 2026. That is a hugely ambitious target. It underpins the Government's 85% manifesto commitment, but we have to get to a ramp of building 4 million premises a year.

We are currently building at 50,000 premises a week, so we are heading up towards the 3 million a year kind of ramp, but from pretty much a standing start in about 2017, as there was very limited full fibre in the UK at that stage. We had finished building the old network and had not transitioned through. It is a really serious challenge. If you think about the pace of build and what we are trying to achieve, being able to do things really rapidly and operationally simply becomes incredibly important.

For us, the two big pieces that the Bill can potentially help us with enormously and help supercharge that fibre build is around access, that is access to multi-dwelling units—the approximately 6.1 million blocks of flats in the UK—and access to rural parts of the UK. There are some urban as well, but if you think about how we build, we have a duct infrastructure but we also have a very extensive pole infrastructure. For most of our rural build—we have committed to building 6.2 million commercial rural, which goes beyond the Project Gigabit programme that the Government are talking about to the hardest-to-reach areas—we are going to have to do most of that over our existing pole network. At the moment, the Bill makes some changes that are helpful and which progress us forward by allowing us access to upgrade our current infrastructure on underground ducts. What it does not do is allow us to upgrade the infrastructure we have in place, either over the pole network or in those blocks of flats.

If you think about what we have in place today, we have our existing network, so we have the ubiquitous either copper or hybrid copper network that is there today in pretty much all of these premises, all across our poles. We are trying to upgrade that network to full fibre as rapidly as possible and to do so, it would be incredibly helpful if we were able to upgrade our existing infrastructure. The Bill at the moment allows us, as I said, to do that through underground ducts. It is not going to allow us to get into either MDUs to upgrade more rapidly—we estimate that something like 1.5 million MDUs could be at risk based on our experience of unresponsive landlords and our inability to get in—and it also does not allow us to automatically upgrade our property and the infrastructure that we have over the pole network.

To give you a bit of context, we have 1 billion metres of cable over poling at the moment. The vast majority of the rural network is served over poles, so for us it is really important to be able to deliver those 6.2 million commercial rural, but also potentially the Project Gigabit programme. We have been working in Scotland on the R100 programme—the "Reaching 100%" Scottish Government programme. We need one wayleave for every 16 premises, to give you the sense of scale. We are finding the ramp very challenging and because of the scale and pace that we are trying to build at, what we really need is ease of access, ease of upgrade and that is the opportunity we think with the Bill.

Simon Holden: I think we are talking about two different sets of infrastructure here, which is worth explaining. We are talking about mobile and then we are talking about fixed-line fibre access. CityFibre is rolling out a fibre access network, mostly to consumers in the home. We are doing that across a footprint of 8 million households in the UK. The reason I wanted Catherine to go first is because we are utilising Openreach's duct and pole infrastructure for three reasons. First, because it will allow us to go faster because we do not have to dig up the streets and lay ducts ourselves or put many more telegraph poles down. Secondly, because we are reusing and so can lower our cost, which means ultimately lower prices for the consumer. Thirdly, because it is just much more environmentally friendly if we can reuse those assets.

We are in favour of that, but at the moment we have this split between pre and post-2017 access. Our view at the time was that that made a lot of sense. Five years on

from that now, it is a somewhat arbitrary split. So we think dealing with that is the right thing to do. In particular, the draft Bill's proposals on ducts look fine to us. We would echo the point about poles. For us, poles are really important in rural, but also in Scotland. It turns out that in Scotland there are a lot of poles sitting in people's backyards and just being able to access those to put our infrastructure on means that we can accelerate getting fibre access to all those homes. In our footprint, there are probably up to about 200,000 homes that we can access quickly if we can get that right, so we think that there is a real advantage to doing that.

For us rolling out fibre, there is a balance that you have to have here between access all the way through into the home, back to the public domain where, as a code operator, we can build in the public domain. I think we would say that our experience of getting landlords to come to the table is mixed and that the alternative dispute resolution mechanism proposed here is a good one to push that timetable down, so we can get to an answer.

I would also say, however, that when we get into the home, into a block of flats, the tenants really want the service. We have found that, once we have got the landlord and the landlord has given us the wayleave so we can connect into the front door of the block of flats, then wiring up inside is not particularly an issue. We are concerned a little with somehow grandfathering old wayleaves inside buildings, first because it does not seem balanced, but also because it will entrench the people who have those, which I would say is mostly Openreach.

In trying to promote competition and accelerate growth—to your question earlier, Minister, about whether growth has accelerated—the answer is that growth has clearly accelerated in rolling out fibre. That is absolutely happening. We have vibrant competition now, with billions of pounds being invested in this sector. Here is an opportunity to make it go faster, for us all to benefit with a frankly lower-cost solution.

We feel that what is on the table with that landlord dispute resolution mechanism is good. We do not feel that we need to go inside the building, frankly because once tenants have access to it, landlords are more than willing to give that connectivity, because they have happier tenants as a result. We have not found that that is a real impediment to us.

Julia Lopez: Juliette, did you want to add anything? You do not have to.

Juliette Wallace: I was not going to add any more to what Mark said on behalf of mobile.

Q43 Julia Lopez: This morning, a rather unflattering depiction was created of the behaviour of operators towards landowners. "David and Goliath" was a term that was used: using financial might to bully landowners. Do you accept that characterisation of operators' behaviour? It was also suggested that people might be disincentivised to have any infrastructure on their land, because of low rents, and that that will therefore slow roll-out to the detriment of everybody who shares our aim of better digital connectivity. It would be helpful to have your response to some of those assertions.

Mark Bartlett: Speed Up Britain represents the MNOs: Cornerstone, MBNL, Cellnex, which is a towerco, and DMSL, WIG and the industry as a whole. I will put some facts, some numbers, on the table to help us understand what we are doing.

Since 2017, we have completed about 1,000 agreements, of which 85% have been consensual and reached without any recourse to any of the processes associated with the legislation. Over and above that, 14.5% approximately required some form of exchange of letters of notice, but then moved quickly to agreement, and only 0.5% of any of those discussions ended up in the tribunal. In my experience, those that ended up in the tribunal have been the industry—us—versus the industry, or land aggregators, to be blunt.

The facts speak for themselves. In the main, as an industry, we run over 30,000 towers, which are visited frequently in order to upgrade, to maintain and to support the connectivity of the country. We do not see a landowner community, a landlord community, our partners as such, in a wall of non-co-operation, but almost the opposite. We speak to our landlords very frequently, we interact with our landlords very frequently, and therefore I do not recognise the characterisation as stated this morning.

Catherine Colloms: I am happy to talk from a fixed perspective. Generally, we have pretty good relationships with a large number of our landowners. Fibre and the copper and duct infrastructure we have is not a revenue generator for most landlords. You will have heard Charles Trotman this morning, from the CLA. We have agreements and rate cards, which were negotiated with the CLA and the NFU. We work closely in particular with those kinds of rural players to ensure that we have those in place. They are very effective and seem to work very well.

Just to give some kind of context for fixed, we do not tend to have these kinds of disputes, to the extent that you are not going to make a ton of money, frankly, by having a few poles on your land. A pole rental is between £10 and £20 a year, so even if you had a couple hundred poles, which would be unusual, that would mean only a couple of grand. If you think about ducting and cabling going through, that is anything from 19p to 49p a metre, so it is not a revenue generator per se. For us, the conversation with landowners is predominantly about access.

To Simon's point, we find that we do have quite a lot of issues when it comes to MDU access, especially given the scale at which we are trying to build. We obviously have a machine of people who sit behind to try to negotiate, wherever possible, consensual agreements or wayleaves, but we would genuinely need an army of people to try to get stuff done.

For example, some of you will know that a couple of years ago we fully fibred Salisbury, which became one of the first full-fibre cities in the UK. We tried experimenting to test the limits of access and find out what would or would not be a problem with the roll-out. After two or three years of really concerted effort, including with John Glen, the local MP, being super-supportive and with loads of local PR, we could still get into only about 79% of MDUs, because of non-responsive and non-communicative landlords. If we were to scale the MDU team that we had for dealing with the amount of

time it would have taken to tackle those unresponsive landlords, we would effectively be scaling from a team of about 17 to over 300.

As Simon says, the ADR processes are helpful predominantly when there are larger landowners, such as housing associations or local authorities. They are less helpful when it comes to the hundreds of thousands of wayleaves that we need in order to get into all the individual MDUs. That is why we think that the ability to upgrade the existing infrastructure, and therefore to give tenants the connectivity they deserve, is still the right mechanism to try to ensure that we can get the upgrade as quickly as possible.

Juliette Wallace: We do recognise, as the operator side of the industry, that in the very early days of the code—early 2018, for instance—the interpretation that we were trying to explore may have been a little too over-enthusiastic, shall we say. A lot of time has passed and we have learnt from that. I think that a lot of the examples that are provided to try to support the allegation of a David and Goliath approach are from very early in 2018, and they do not exist today. I think that we have moved on a lot, but we cannot be stuck with all the allegations of the past as well.

I do not agree that the David and Goliath approach is correct. As Mark said, to the extent that it is, what we are finding with the tribunal element of the approach is that it is actually industry arguing with industry; it is not small farmers, necessarily, who are behind that negativity. It is not David and Goliath; it is Goliath and Goliath.

Q44 Julia Lopez: Catherine, you set out some ambitions on roll-out. Were those ambitions based on the presumption that this legislation will go through, or were they based on the status quo? What would be the impact on the ambitions of your members and your company if the legislation did not go through? What would be the impact on rural connectivity, in particular?

Catherine Colloms: The current target of 25 million full-fibre premises by 2026 did bake in some assumptions about access, particularly in relation to the upgrade rights in clauses 59 and 60, through MDU and through poles. On the impact of not having it, I think there is a kind of overarching impact. If you think of the challenges of the build and the scale of what we are trying to do, the harder it is to build and the slower it is, the less we can do. We are having to re-phase and re-look at the build that we are currently targeting, as a result of potentially not getting some of the elements in the legislation.

If I take the MDU point in particular, we have re-phased some of our MDU work to the back end of the 2026 target, the reason being that at the moment we just feel we are not going to get the access. As I said, our experience is that up to 1.5 million of those total 6.1 million MDU premises will be at risk. We are seeing that in a day-to-day aspect as we build, so we have re-phased 300,000. That will go to the end of the build, which means it does not count towards the 2025 manifesto target. It will still be planned within our build, but I think what will happen is we will just have to build different bits.

When we are building this rapidly, we cannot afford to sit and wait—wait to negotiate a wayleave, wait for an unresponsive landlord to come back, wait for an ADR process. Even though we have some of these mechanisms in place, we frankly do not use them, because there is not the time and we do not have the scalability to be able to wait for all these landlords, so while we are trying to build at such pace and scale, we effectively move on. What will happen in the short term is that we will still aim for our big 25 million target, but you will get a different mix, and we are already seeing that you will have less MDU in the mix. Obviously, the concern with that is that MDU is often urban and is often local housing or in more deprived areas, so there is a risk of creating a new digital divide—in particular, if you happen to live in a block of flats versus not—because of the access issues.

On rural land, we have this ambition to get to 6.2 million. Effectively, the way that we plan and build the network is we will pick an exchange, and we will survey that area and have a plan to build, but if we cannot get the wayleave, we will not build to the village that is beyond the wayleave. We will still get to our target, but you will get more pockets left behind in different places as we build, because instead of being able to build to 80% or 85% of an exchange area, one landlord might potentially be blocking the access that gets you to the village that is over there. If you cannot cross the land, the expense of having to circumvent it and go all the way around it means that that village build is prohibitive.

The Chair: Can I ask witnesses to please keep their answers shorter? I have had a number of Back-Bench Members already indicate that they want to come in.

Catherine Colloms: Sorry. I think it just changes the mix, effectively.

Simon Holden: I might just add that if Openreach is the Goliath and CityFibre is the David—certainly in rural—we would like to go into rural. This would be really helpful for us in order to make sure we can move at speed and at a sensible cost, and take advantage of the opportunities the Government are providing to accelerate growth there, so we would be in favour of that.

Juliette Wallace: On the mobile side, you asked about rural connectivity. Predominantly, that is going to come from new sites, and the code is actually working quite well with new sites—new land build-out. Our biggest challenges come from renewing the agreements that have expired on existing sites. That is where we need the changes in the code that this Bill addresses, and also the amendments to how the Bill is drafted so that it actually addresses the Government's ambitions that came out as a response to the consultation.

Q45 Chris Elmore: I have two very quick questions, because I am conscious of time and Back-Bench colleagues. On the flats and the issues around the digital divide, you mentioned the overall figure—1.4 million, I think it was. It would be good to understand where those places are and how that is impacting on connectivity, poverty, and access to education and services. There is almost an assumption that broadband roll-out is an issue in rural areas, which clearly is not the case if you are talking about mass flat construction. If an amendment regarding access were put forward and accepted, either in the Commons or the Lords, would that be about still trying to engage with the landlords to say that you are gaining access, rather than saying, "Look, we've got the powers. We are now going to start simply entering through this separate law"?

[Chris Elmore]

This is for Mr Bartlett. Forgive me if I am misquoting you, but I think you said 1,000 contracts have been negotiated since 2017. I am assuming those are all new sites, or are some of them renewals as well?

Mark Bartlett *indicated assent.*

Q46 Chris Elmore: To flip it on its head, how many people, companies, organisations or groups have tried to withdraw from contracts dating back more than a decade before 2017? This is purely for the record; it is not a trick question. It is all good and well saying that it is 1,000 since 2017, but how many have tried to walk away or are still arguing that the use of their land, building or whatever should not continue?

Simon Holden: We, CityFibre, are in cities. Probably 10% to 15% of our build is in multi-dwelling units. We are typically in underserved areas around the UK, and I would say that we have a disproportionate share of things like social housing that sit under our built portfolio. No. 1, we think that it is really important to be able to access those properties. I would say that big social housing landlords are embracing that, but it is patchy and we would value having the ability to accelerate negotiations as we are having them and have a really clear process where we can make sure that we get everyone to the table, with a fair resolution at the end of it.

Once you get access to the building, I think it is up to the building landlord and the tenants, obviously, as to how you are going to do the in-building wiring. As I said before, we found that once you have got hold of the landlord and you have agreed it, that does not tend to be a particular problem. What we are concerned about is that if you extend this back to historic wayleaves, all you are doing is effectively entrenching the people who have already got those, which most of the time is Openreach. We would think that that is not helpful for competition. That would be our observation, but in terms of accessing those properties, it is super key to us for our business model to be successful and, of course, for society to benefit from getting the best digital infrastructure to as many households as possible.

Catherine Colloms: As Simon says, most multi-dwelling units tend to be in towns and cities, so looking at the constituencies represented around this table, I can tell you, Chris, that you only have 3%. Hornchurch, in the Minister's constituency, has 13%, and I think Hastings has 24%. They are very concentrated, classically, in urban areas, as Simon says, and often in potential areas of deprivation or areas which are less socially inclusive.

In terms of the access point, you are right. The idea of automatic upgrade would give us the right to do that. You still have to have a relationship with the landlord. That is still always the intent, but it comes down to the obligation. At the moment, there is no obligation for the landlord to do anything. New build legislation obligates them to put in a full-fibre connection, and there is a slightly different conversation you can then have that allows you to proceed with the wayleaves.

Mark Bartlett: To answer your question, first of all the current legislation is not working. At least over a half of all sites are stuck, so the landlord says that they are not renewing or getting new ones. Of those that are under renewal, there are absolute rights in the current legislation for landlords, if they wish to do so, to redevelop at the end of the lease and we have to leave. My estate would be measured in tens a year where it is their right and we move on.

In the current legislation there are also absolute rights for the operators to maintain that equipment if there is no redevelopment need. That is, obviously, very positive, because when we lose a site or a rooftop, whatever the infrastructure might be, that is serving hundreds of people in the community. Therefore, quite naturally, both the investment that we have made and the utility to the public need to be maintained, unless, as I said, the landowner has a genuine need to make that redevelopment, and that is enshrined in legislation, both today and in that passed pre-2017.

Q47 Shailesh Vara (North West Cambridgeshire) (Con): Mr Bartlett, you said that, as far as the agreements are concerned, some 85% are consensual. I would welcome it if you could expand on that, because there is a disproportionate element in terms of bargaining strength. Of the 85%, I am minded to say that there are some small landowners who probably are not happy but feel that they do not want to incur legal costs, that they are up against a David and Goliath scenario, and that they have no option, so they sign up reluctantly but are seen in your statistics as being consensual. Is it not right, then, to put on the record that that 85% is not everybody saying, "Sure, no problem. I have something here; I will just sign it—there you are"? I suspect that a lot of people have concerns about signing, but the cost of legal advice and so on is prohibitive. The way you have portrayed it makes it black and white and very simplistic when, in reality, it is anything but.

Mark Bartlett: I think that would be human. I have never met anybody who wants to take a reduction in the amount of money that they are paid by anyone—that is not something that people work on. However, the policy was put in place to reduce the costs to the industry to allow investment in 5G, which is happening right now for the good of the country.

On the valuation point, it is a fact and a process that if we do not behave properly and that ends up in a tribunal, we would be penalised by the tribunal for the amount of money we have paid, and the judgment would fundamentally go against us, so there is a protection for the landlord there. Secondly, normally—in almost 100% of cases, in fact—we always offer more than the valuation criteria say we should. That results, normally, in a payment of several thousands of pounds, not several tens or several hundreds of pounds.

It is my experience that the majority of people understand that the law has changed and that, like when things change in how you pay your bills, things have fundamentally moved on. So long as we, as an industry, are fair and do not attempt to be over-enthusiastic, as Juliette put it, 85% of people do sign up and say, "Okay, I get it. I am still happy with those several thousands of pounds, and I am willing to make an agreement of that sort." That is not everyone; 15% of people do not feel that, and we have a further conversation with them, and we come to an agreement with the vast majority of them as well.

I would also point out that this is often characterised as an individual change of an agreement—x to y. We often pay incentive payments to achieve an agreement as well. I would like to put that on the record. It is not

just about a reduction in rents. I would also point out that, on average, it is a 63% reduction in rent, not the high 90%-type reduction, that has perhaps been characterised, by the industry.

Shailesh Vara: Sixty-three per cent. is still a significant sum for a small farmer who is counting every penny in his budget. The Committee can understand your reasoning in terms of policy and so on, but as far as the individual is concerned, I maintain—we will have to agree to disagree—that the 85% figure is somewhat misleading if taken in its individual context. I have made my point. Thank you.

Q48 Kevin Brennan: Just to get the record accurate, Ms Colloms, you mentioned earlier the Government's 85% manifesto target. That was not the target was it?

Catherine Colloms: That is the current target.

Kevin Brennan: The manifesto target was for full gigabit by 2025, but that was dropped to 85% in November 2020, wasn't it?

Catherine Colloms: I think you are right.

Q49 Kevin Brennan: Ms Wallace, you said earlier that your companies were "over-enthusiastic" in the early years after 2017. I suspect that it is not really enthusiasm that you are referring to, but being over-assertive or aggressive with landowners, perhaps—that is probably what they would say. If that were the case after 2017, why would landowners not believe that the same would happen after 2022?

Juliette Wallace: When the new code came into effect, it set out how sites should be valued for the use of mobile infrastructure. Previously, there was no mention of how sites should be valued. Pre-2017, we had an industry that had been built up over the previous 20 years or so and that had got somewhat out of hand. Rather than paying a fair price to install infrastructure on land, a fair price being one that recognises what else the landowner could rent the land for—

Q50 Kevin Brennan: Can I stop you there? I do understand that—I served on the 2017 Bill Committee; obviously, I know about it—but my question is, why would your companies not do exactly the same again? You implied that they did not act very well after 2017 by using the term "over-enthusiastic". Why would they act any better now?

Juliette Wallace: We have learned from the past. My comment about being over-enthusiastic related to the suggestion of David and Goliath with respect to the valuations. The valuations that were proposed very early, in 2018, were much lower than we are going out with now. As this Bill does not intend, currently, to adapt the valuation methodology, there should be no reason to think that the valuations that are currently being offered will change.

Q51 Kevin Brennan: Okay. Finally, Mr Bartlett, you mentioned a figure just now in answer to Mr Vara—was it 64%?

Mark Bartlett: It was 63%.

Kevin Brennan: That is the average. Could you tell us some of the figures for those who were worst affected? If 63% is the average, what were some of the biggest drops in income for people affected?

Mark Bartlett: At this point I obviously do not know—

Kevin Brennan: Would anybody have suffered a 90% reduction?

Mark Bartlett: I was about to say that at this point I can only talk about Cellnex UK, because obviously I am not aware of the commercial agreements of any other members of Speed Up Britain. I can be clear that there have, in a handful of cases, been—we have been open about this—90%-plus reductions in rent. But in the main, that normally means the rent itself was over-rented at the point of agreement—that is, we were paying drastically too much. On average, 63% is in line with the Cellnex UK achievement. We have to understand that we have an ongoing relationship with our landlords above and beyond a renewal. There is no interest in the industry for us to behave in a way that alienates our landlords.

Q52 Kevin Brennan: Ms Wallace, do you have any figures in relation to that?

Juliette Wallace: I was going to pretty much echo the Cellnex example. We have a handful that are towards 90%—in that sort of area. We also have some sites where the rent has gone up as a result of the new code.

Kevin Brennan: But the average has been a reduction.

Juliette Wallace: The average is a reduction, but it is creating a fair environment that says, "We will reimburse you for the land that we're utilising." As I say, we have a lot of sites where there has been no reduction and we have a small number where the rent actually increased.

Kevin Brennan: Thanks. I think everyone understood there was going to be a reduction, but I cannot remember those sorts of figures ever being mentioned at the time of the 2017 Bill.

Q53 Sally-Ann Hart: This question is for Catherine Colloms and Simon Holden to start with. My constituency, Hastings and Rye, has urban and rural areas—we have small Rye—and pre-existing 2017 infrastructure. You have both explained the consequences of the cost if you cannot use existing duct and pole infrastructure. What activities, exactly, would be required to upgrade existing infrastructure, and what reassurance can you give landlords or people who own gardens containing a telegraph pole or that sort of thing?

Catherine Colloms: Effectively—let me take a multi-dwelling unit and then I will take a pole—we need to put a new fibre cable over some of these pieces of infrastructure. I actually have my kit behind me, which I can show you in a second. With an MDU, there is often fibre outside a premises; we will build to the curtilage. What we have inside an MDU is the existing cable—the existing hybrid fibre—that is going up inside the risers. You basically cannot see it. It then kind of pops on to a room. We would reinstall the new part of the full-fibre kit in the classic plant room downstairs, so that it is all with the maintenance bits. We then need a new small cable—this one is basically it; it is called InvisiLight—which we would run up through the risers. This is what you would see, or not see, running through corridors or along the wall. When you put this on a wall, you cannot find it because it is absolutely tiny. This cable has all the fibres running through it.

Sally-Ann Hart: The visual impact is going to be minimal.

Catherine Colloms: It is minimal. You often need a very small box that just sits on the top of someone's door and you effectively put this cable inside someone's flat to a new box. That is for an MDU.

For a pole network, it is similar in the sense that you need slightly more than this amount, because we will probably have some more cables in it. Over the existing pole infrastructure, you will have a new cable that basically has fibres in it. As you can see, this cable is absolutely tiny compared with copper, and it will serve hundreds of premises, as opposed to the copper, which needs to be a different size. You would effectively need a cable that is slightly larger than the one that I have here—because it would be protected—that runs across the existing infrastructure. You sometimes need some termination points, so there might be a few pieces of black plastic, which is effectively where you put various bits of the access network.

Sally-Ann Hart: On the telegraph pole.

Catherine Colloms: On the telegraph pole, but not every pole. It will be only on a few of the access poles, but we try to minimise the impact and keep it as small as we can.

Simon Holden: We are using exactly the same process and procedures, and the ducts and poles that are available, so my answer is the same.

Q54 Sally-Ann Hart: Why do you think the Bill does not cover infrastructure that was there before 2017?

Catherine Colloms: At the moment, the way that clauses 59 and 60 are drafted, they talk about "no adverse impact" as opposed to minimal adverse visual impact. The existing code under which we are currently operating talks about "minimal adverse impact", which is why we have been able to put infrastructure in as we are doing today. That has not been transposed in the Bill. We are suggesting that if we could change the definition to "minimal adverse impact" as opposed to "no adverse impact"—with, for example, the MDU having something like this cable—that would allow us the ability to go in and upgrade with minimal adverse impact where we currently have the infrastructure.

Q55 Sally-Ann Hart: Thank you. I have one more question for you, if I may. In Hastings and Rye, with rural and urban areas, and levels of deprivation, we do not want digital exclusion. Are there any other changes to the Bill that will get full fibre out more quickly to those people who really need it?

Catherine Colloms: For me, it is the critical clauses 59 and 60. If we could extend the measure to multi-dwelling units, that solves your urban problem, but, critically, if we can extend it over the pole network, that is what will make the difference in rural areas. As I was explaining to the Minister, it is not necessarily that the target changes, because we will still try to do everything we can to meet the target, but the danger of not being able to upgrade existing infrastructure over poles is that you end up with pockets that are excluded as you upgrade. We are effectively trying to avoid getting all these pockets of digital divide in MDUs and cities, but also the little pockets as we are upgrading through rural areas at the same time.

Simon Holden: I would add one administrative point. The way that the Bill is drafted at the moment means that the main operator, which would typically be Openreach, has to notify the private landowner. The fact of the matter is that if we wanted to use it, we could equally notify the private landowner. What I do not want to do is either to burden Openreach with lots of my administration, or for that to become a bottleneck to the speed of my roll-out. We would propose that if it is the main operator or the new operator that has utilised that infrastructure, it could give the noticing. By the way, we are giving noticing to local authorities for works all over the place; we have a process for doing that. That would actually accelerate things from our perspective and not create an inadvertent administrative bottleneck from a process perspective. We can provide you wording on that.

Q56 Sally-Ann Hart: Thank you. I have one question for Mr Bartlett. We heard this morning from a colleague who is not here this afternoon that one possible reason for the increase in costs that perhaps Cellnex, for example, has met is that between the landowner and the operator, middlemen became involved. What are your thoughts on that?

Mark Bartlett: First of all, towercos have been around in the industry since the start. The BBC became National Grid became Crown wireless became Arqiva became Cellnex, and so on. This is not a 2017 phenomenon. Secondly, Cellnex itself has invested billions of pounds in the UK over the last couple of years and invests hundreds of millions of pounds a year, whether that is in connecting the Brighton main line or providing DAS, small cells, tower upgrades or new towers. To describe a huge enabler of connectivity across the UK as a middleman is, I think, a step too far. Fundamentally, we are an industry that is bringing connectivity to the whole of the UK; we are part of it, and we believe that these changes are needed to deliver it.

Q57 Rebecca Long Bailey (Salford and Eccles) (Lab): The Bill will give the right to share and upgrade pre-2017 infrastructure. In relation to mobile coverage, to what extent will this dramatically improve the roll-out? The range of 5G, as I understand it, is very limited—is it 500 metres? Perhaps you could confirm that. Beyond that, it would be very helpful for us to understand to what extent telecoms providers are currently collaborating with one another to locate the best sites to situate new masts and to upgrade existing masts, to minimise the impact that communities will face. As we heard from various people this morning, many communities feel very powerless in this whole process, and it would be helpful to reassure them that they are being considered and there is a wider agenda that is being addressed by such companies.

Mark Bartlett: That is a good question. First of all, do we collaborate as an industry to use shared infrastructure? We are required to do so under planning laws. In fact, towercos' reason for being is to create efficiencies and share infrastructure, to the benefit of the community. We are, through the planning process, not allowed to stick one tower next to another. Those sorts of things protect the community, but also make sure that we exploit the infrastructure that we have today to maximum effect.

Secondly, in terms of sharing upgrade rights, obviously we have existing towers. At the point at which we need to upgrade for 5G, often we need to put more equipment on those towers, so it is important that we are able to do that without having to negotiate higher costs under the old regime, and that we are able to do that very quickly. To Catherine's point, where we do not get agreement to upgrade a tower, it simply means—the local community around that tower is much further than 500 metres; depending on which technology you use, it might be 500 metres, but I will not go into that, and one big tower serves many hundreds of people—that that tower does not get upgraded and the money is spent on a different tower in a different community.

The power of the individual to affect the outcomes of the community is very high in the process that we have today, especially where the legislation does not work. To be frank, that is why the changes are required. It is not necessarily to overcome some battle with a land agent. We are simply attempting to create this connectivity solution across the UK as fast as we possibly can, and having the simplicity—while remaining fair to the landlord—of legislation that works and an operational process that works is going to enable that.

Is there anything else you want to add, Juliette? If I may, I will refer to Juliette on the technical—

Juliette Wallace: I do not think there is anything particular to add, other than to say that the shared rural network absolutely relies on the ability both to roll out new sites to new areas that are total notspots at the moment and to roll out sharing and upgrade capability on existing sites. If we do not get the changes in this Bill, we are going to be seriously reduced in our ability to effectively roll out, share and upgrade those existing sites. There are some sites where currently we have no mechanic to be able to renew those agreements. As Mark said, the power of the individual to frustrate the roll-out of new technology or increase technology to a geographical area is huge currently.

Q58 Rebecca Long Bailey: To what extent are mobile providers sharing their proposed network coverage maps with local authorities, so that local authorities could try to match them with other providers, for example, where such collaboration has not been taking place?

Mark Bartlett: With respect, I am unable to answer that question as part of Speed Up Britain, because that is often commercially sensitive, but we can write to you. Mobile UK is part of Speed Up Britain, and they are the best people to ask. I will ask them to write to you directly to give you that clarity.

Q59 Rebecca Long Bailey: I have one final question on the poles issue. I am genuinely inquisitive about this. Is it the case that an area could potentially have a full-fibre broadband network under the road, as it were, but also have a pole network adding competition? If that is the case, are we at risk of creating rural deserts where there are fewer consumers and so less commercial incentive to do that, and overpopulated areas that have many options but a lot of infrastructure in their street scene? That is a question for Simon and Catherine.

Simon Holden: We architect what we call polygons, which basically go around our cities, and our objective is basically to cover every premise in the city polygon that we build. That is a commercial decision that we have made. We think that super-high-density fibre networks are the best way to cover a population and offer the best marketing opportunity to end customers. By the way, they allow you to do the densest 5G networks overlay on those.

In our architecture—which does not follow the Openreach architecture; it is our own—we use a series of ducts and poles in rings going around, and then run off coming from that. We plan, in our builds on our city polygons, not to have notspots. Sometimes we cannot go down a private road, because we need a wayleave and there is a process to go through to get that, but our policy is to try to cover as much as we possibly can. Typically, we cover 85% to 90% in what we call the first pass of the build, and then we start going back to do infill around that. At least where we are building today, we do not have that as a problem.

In rural areas, I think that will be affected by the BDUK process and the roll-out—we would like to participate in that—but our expectation is that we would be building and connecting from our cities all the way out to the deep rural areas, picking up the small towns and villages on the way. In those commuter towns, we would look to cover all those premises; if we are there building, we would rather just build it once and cover everyone. That is the best commercial opportunity that we see.

I do not think that we see what you are describing as a problem that we would be planning in to avoid; it would only be because we could not get particular wayleaves or particular access, a little bit as Catherine described, that we would end up trying to go around that. That is why this legislation will help us.

Catherine Colloms: If you think about the existing architecture—obviously, we have the existing architecture; we are still building new, but we are trying to reuse wherever we can, because that is cheaper and avoids digging up all your constituencies as we go—it is true to say that there is a greater proportion of underground ducting in urban areas, which this legislation, as drafted, would allow us to upgrade more easily than over the pole network or in multi-dwelling units. We have a much denser proportion of poles in suburban and rural areas, so at the moment, as the Bill is drafted, it is harder to upgrade rural areas than it might be to use the existing underground infrastructure, which is predominantly in urban areas, as you say.

The Chair: If there are no further questions from Members, on behalf of the Committee I thank the witnesses for their evidence. I hope I have not hurried you along too much.

Examination of Witness

Till Sommer gave evidence.

3.38 pm

Q60 The Chair: We are now going to hear oral evidence from Till Sommer, head of policy at the Internet Service Providers' Association. We have until 4.20 pm for this session. Please introduce yourself briefly, and then I will turn to the Minister.

Till Sommer: I am Till Sommer, head of policy at the Internet Service Providers' Association. We are basically the trade body for the fixed-line ISP sector in the UK. We represent a whole range of companies, from the

largest infrastructure providers that you heard about from the previous panel, such as Openreach and CityFibre, to the smaller start-up companies and ambitious alternative network providers who roll out their own networks in urban or rural areas. Some of them are focused on Wales, and others are focused on England and Scotland—there are a whole variety.

Then, on top of that, we have a lot of companies in our membership that provide services across these networks. That includes some of the household names, such as Sky Broadband, but also smaller challenger brands or business-focused providers. So it is a really diverse sector and a very ambitious sector. There is a lot of competition in the sector and quite often that gets overlooked when you just look at the sector from the outside and you see a few large companies. As I said, there is a lot of variety in the sector.

Interestingly, because there is so much competition in the sector, our members hardly agree on anything; they always bicker about policy positions. And wayleaves is actually one of the few things where every single member who builds networks is saying, "This is the single biggest barrier to rolling out broadband for me." That is one of the few areas where literally every single ISPA member says, "Something needs to change." That is unique. On almost everything else, I could tell you a variety of views, and this is one of the few areas where everybody says, "Something needs to change."

The Chair: Thank you. We will return to that at the end of the questions, please.

Q61 Julia Lopez: It would be helpful to know how your members believe they stand to benefit from the Bill. You say that there is a strange degree of unity among them on this legislation, but in so far as there is any disparity of view among your members, it would be helpful if you could characterise that for us, so that we have an understanding of where commercial interest sits for different types of internet providers here.

Till Sommer: Yes, sure. The Bill basically does three different things: it is access to third-party land in rural areas; it is the alternative dispute resolution mechanism on a voluntary basis; and the third area is upgrade rights. Upgrade rights, as you heard from the previous panel, is one area where there is slight disagreement because, depending on how you fix that, it might give one set of providers a competitive advantage over the others. For that reason, I do not want to go into too much detail there.

At the basic level, we want more upgrade rights, because it helps to use the infrastructure that is already there, rather than digging up the road again, putting up new telegraph poles or, as was said, just not doing something at all because the money is not there to build in that area if you cannot reuse the infrastructure. Beyond that, I do not want to go into too much detail, or I will get into trouble with my members and they will all talk to you separately.

I will take the other two areas, including access to third-party land. We have a few members who are specifically focused on rural areas. They are effectively going at the moment where Openreach does not have a strong build. They are very ambitious. They have told us quite early on that this Bill is game-changing for them. Access to third-party land in rural areas is simply the one thing that will unlock additional properties in their roll-out plans.

The reason for that is that this part of the Bill effectively mirrors something that was done a year ago for multi-dwelling units in urban areas, because it looks at a problem that our members face; I will use a very simple example. Let us say they want to reach a rural hamlet and there are three routes to it—one across a farmer's field, one across a railway line and one across a hilly area. The most economical route is across the farmer's field, but that field might be owned by someone who is not living in the UK, or who does not look at their emails or their post; that farmer just does not respond. At the moment, there is no mechanism to get any sort of forward movement in that situation.

So, what happens is that the provider either moves on, because they decide that it is not economically viable to take one of the other routes to that hamlet, or they say, "Actually, no, we do go across the railway line, but we descope parts of the hamlet. The money just isn't there any more to connect every single house. It's still economically viable to go there, round the field, but it doesn't quite reach the whole village."

Third-party land access provides a mechanism to get access to wayleaves, or access to land, for a limited period in those very limited circumstances. That will unlock those properties that at the moment are at risk of missing out. I am sure some of you will have seen in the past an announcement from a broadband provider—you might have even done a press release with them—saying that they are building out to x number of houses in the constituency. Then, after two years—after the roll-out programme is done—the number is not quite there. Quite often the reason for that is because the build has been more difficult than expected, there have been unresponsive landlords and the money that was allocated for that area does not quite match the ambitions.

It is worthwhile keeping in mind that roll-out is privately funded. There is Government support for the hardest-to-reach areas and we appreciate that, but outside of that it is privately funded infrastructure, with a return on investment over 20 or 30 years. We need to make an investment case. The companies, our members, need to make the investment case for their investors, for their shareholders and for their owners, that they will at some point get that money back. That is why we sometimes need to make those difficult decisions where stuff is being descoped. That is why the Bill is so important; it helps avoid those areas and unlock that bottleneck.

I mentioned alternative dispute resolution; some of our members are a bit sceptical about it, and that is largely because they roll out on a very large scale. Having to deal with thousands and thousands of ADR processes can be quite daunting, time-intensive and costly. For that reason, we believe it is good that it is done on voluntary basis, with the clear incentive provided in the Bill that the tribunal will take ADR into account. It will help a lot when it comes to negotiations with large landowners; that can include local authorities, where our members often have to negotiate a headlease or a head wayleave agreement. That can be super-complicated, because there is part of the local authority

that is really keen on getting broadband, but the people dealing with the wayleave stuff do not really care because it is not in their portfolio. There are then mixed messages coming from the local authority. On the one hand they are saying, "Can you please roll out broadband as quickly as possible," but on the other hand there are people saying, "It takes another year to negotiate the agreement." ADR will be really useful to make progress in those very large wayleave cases.

Q62 Julia Lopez: The legislation will make it easier to share infrastructure. What is your analysis of how that will change the economics of roll-out, but also reduce visual impairment from having new infrastructure in post? As MPs, we are all familiar with some of the concerns that constituents have about that kind of infrastructure in their vicinity. Will this help maximise the existing networks, such that we do not see more masts and so on?

Till Sommer: Yes, that is exactly right. If you cannot use existing infrastructure but you are still going to roll out the network, you need to dig up the roads. I assume you have all received lots of letters about roadworks and the problems that they cause. You either dig up the roads or put up new telegraph poles, which is more expensive and is another element of visual impairment and disruption. For that reason it is much more economical—and from a visual aspect, less intrusive—to reuse existing infrastructure.

Q63 Julia Lopez: Do your members have any views on the cyber-security aspects of the legislation?

Till Sommer: We do. Basically, a key bit that our members provide to your constituents—their customers—is a router, plus other equipment, that is classed as an internet-connected device under part 1 of the Bill. We are in regular contact with your civil servants on that, to clarify timelines and how the Bill might bite. We do not have any concerns about the idea. We support the idea of the Bill; it is more about the implementation, and ensuring that the supply chain is aware of the new provisions that are coming in.

I have heard from a lot of our members that they have started to talk to their supply chain to say, "By the way, in a year, or in one and a half years, depending on when the Bill will be done, we need to ensure that your products comply with these rules." Because a lot of the manufacturers are overseas, they are not yet aware of them. Anything that can be done to raise awareness among consumer product providers would be welcome. There are a couple of other bits that go very much into the detail around associated software, when it comes to parental controls, which could be affected. I am happy to write to you on that if you want, but we will talk with the Department about it anyway. It is very much nitty-gritty stuff.

Chris Elmore: The Minister took my last question on part 1, so I am happy to give my time to Back Benchers.

The Chair: Do any Back Benchers have further questions for Mr Sommer? In that case, I thank you very much on behalf of the Committee, Mr Sommer, for the evidence that you have given, and we will move on to the next panel, somewhat ahead of time.

Examination of Witnesses

Rocio Concha and Jessica Eagleton gave evidence.

3.52 pm

The Chair: Good afternoon. We will now hear oral evidence from Rocio Concha, director of policy and advocacy at Which? and Jessica Eagleton, senior policy and public affairs officer at Refuge. We have until 5 o'clock for this session if needed, but as we have started ahead of time I am sure that nobody will mind if we finish ahead of time. Please could the witnesses introduce themselves for the record? Then I will turn to the Minister to ask the first question.

Rocio Concha: I am Rocio Concha, director of policy and advocacy and chief economist at the consumer group, Which? Thank you for the invitation to provide evidence. The Bill is quite important for consumers. We have been very supportive of the work that DCMS has done in the Bill. That is very good, and I hope that I will have the opportunity to explain how the Bill can be improved to achieve its objectives.

Jessica Eagleton: Good afternoon, everyone. Thank you for inviting me to give evidence. I am Jess Eagleton, senior policy and public affairs officer at Refuge, which is the country's largest specialist provider of gender-based violence services. We provide a host of services including refuges, community outreach and a specialist tech abuse team. I am here today to speak to you about technology-facilitated domestic abuse.

Q64 Julia Lopez: Thank you both for attending. As a Minister, I am concerned about the general lack of awareness of the risks and vulnerabilities when it comes to internet of things devices. To what extent do you believe that the legislation will help to stimulate a consumer discussion about how we best protect ourselves against some of the threats that are emerging as the technology develops? It would be helpful, Ms Eagleton, if you could set out your own interests in terms of Refuge and the vulnerabilities that have been highlighted in your work when it comes to the impact that an insecure connected device can have on an individual.

Jessica Eagleton: Of course. The first thing to say is that we are seeing technology-facilitated domestic abuse becoming ever more prevailing. Technology in all its varieties is providing domestic abusers with a host of new means and methods to perpetrate abuse—to monitor survivors, track their whereabouts, harass them and stalk them—so much so that, as I said, we set up a tech abuse specialist team a couple of years ago. Of the women and children who we supported last year, 59% said that they experienced abuse involving technology, so we are seeing a growing threat.

The specific devices that we are talking about, which are covered by part 1 of the Bill, offer a whole host of ways for abusers to abuse. I am thinking about home security cameras and home security devices such as doorbells, which provide almost 24/7 oversight of a survivor's movements in the home. Camera and microphone functions can be used to listen in on survivors and capture intimate images without consent, which can then be used later to threaten and coerce the survivor. There are also things such as smart plugs and smart thermostats, which can be remotely accessed and used to frighten survivors—for example, by turning alarm systems on, or putting blaring music on, in the middle

of the night. That is happening in the relationship and after it as well, so we are seeing remote access being used in that way.

Some of our concerns about devices relate to access. Thinking about the power imbalance in a domestic abuse relationship, it is the perpetrator who often sets up such devices. They have the password and full admin access, which means that the survivor therefore has limited ways to access a device. We have had some difficulty when talking to companies to try to support survivors to take back control of devices, particularly once a relationship has ended and a survivor has fled. Where they have devices in their home to which the perpetrator still has full admin access, it is particularly difficult to get companies to override that. That is something that we would welcome further work on, in terms of companies taking steps to support survivors to make changes to settings.

Julia Lopez: Do you have anything to add?

Rocio Concha: Your question was on whether the Bill will help consumers to understand these issues, and it will. As you know, one of the principles in the Bill is transparency—when you buy these products, you will know for how long they will be supported. That will help with awareness. There is a lot more that can be done to raise awareness of these issues. There is a limit on what consumers will know about how to protect themselves, so the direction in the Bill about banning default passwords is quite important, as is the point of contact for security vulnerabilities.

Jessica has explained very clearly the harms. There is an opportunity for the Bill to be more assertive. At the moment, the Bill says that the Secretary of State "may" include baseline security requirements. We know that these are not the right baseline security requirements, so the Bill should be clearer that they will be included. We also think that the Bill needs to list the three security requirements, which would give a clear steer to the industry that they are to be introduced. We are worried that the Bill as drafted could lead to more delays in introducing things.

If we want the Bill to achieve its objective, we must be careful to ensure that online marketplaces are within scope. I would argue that they have to be because, as a consumer, it makes no difference whether you buy your smart product on the high street or from Amazon, eBay or AliExpress; you assume that the product is compliant with the regulations in the UK, so it is important that the Bill also covers that area. Otherwise, you know where the bad actors will go—they will be selling insecure products on those online platforms.

Q65 Julia Lopez: Do you have any view on the enforcement powers in the legislation? Do you think that they are sufficient to deal with non-compliance?

Rocio Concha: On enforceability, if you do not include online marketplaces, you are leaving a big gap, because these products can come from any country in the world when they are being sold in these online marketplaces.

Another area that is not clear in the Bill is how consumers can get redress. As part of the transparency requirement, suppose that you buy a product that says that it will be supported with security updates for four years, but two years down the line, the manufacturer decides to change its mind and to support the product for only two years. Where would the consumer go in that instance? They bought the product on the basis that it would be supported for a set amount of years.

The other thing that is not clear is who the regulator enforcing this will be. Obviously, we need to make sure that the regulator has the skills, powers and resources to enforce it.

Q66 Chris Elmore: My first question, for Ms Eagleton, is on tech and some of the work that Refuge has done to highlight the fact that, as you said, 50% of all cases of violence against women and girls now involve some sort of device. What conversations are you having with the Government on funding and advertising to try to show that these devices have an impact? On new technology, such as AirTags, we have seen some very good pieces from journalists explaining how that is increasing the options for people to stalk, follow and track others, with terrible cases of people who have been victims of domestic abuses historically finding them in their cars. I am wondering how all that links into the work of the Bill, about areas where you would like to see improvements to acknowledge the fact that technology is moving so quickly, and whether we can do something in the Bill to introduce meaningful support for women and girls who are victims of violence.

Jessica Eagleton: Perhaps I can take your second question first. You are right that we are seeing concerns about these types of products being used to stalk and to monitor. In terms of concrete measures and what the Bill can do in this respect, we welcome some of the security requirements, particularly around the vulnerability disclosure scheme, as a step forward. For example, in the work that we do to support survivors, having that public point of contact and an easily contactable place for a company to go, when we are reviewing these products and putting forward recommendations to companies, is definitely a step forward.

We would have some concerns about situations where companies might publicly disclose security flaws and perhaps not take steps first to address them. We have that concern because that could, in essence, alert an abuser to a new way to abuse a victim. It could alert them to a device that they could purchase or that is already in their home that would provide a new way of compromising, so we would like to see companies taking all reasonable steps to address and action some of these security flaws before there is that public disclosure.

On your second point about services, our tech abuse team is a unique service in the country in providing specialist frontline support to tech abuse survivors, but it is a chronically under-resourced service. Perhaps in the context of this Bill, we would really like to see thought given to a percentage of the fines that the regulators collect for non-compliance by companies going, for example, to fund some specialist support services. I think that would fit within the wider ecosystem of enforcement as well. If we have specialist services that survivors can go to and ensure that they are sustainably funded and able to support survivors, that would contribute to the wider enforcement regime and awareness.

Q67 Chris Elmore: You mentioned the broader point of industry and manufacturer engagement, and situations where they announce that there is flaw but do not think

about the consequence of announcing a way in which someone can hack a mobile phone, for example. Is it fair to say that the industry does not necessarily fully appreciate the impact its technology has on women who are victims of domestic abuse? What work is it doing already, without legislation, to acknowledge that its devices are playing a significantly greater part in impacting on people who are survivors or are being abused currently?

Jessica Eagleton: It is not always thought about that the devices can be used in this way. A lot of the focus of companies in this space has been on how to prevent devices from being compromised by unknown third parties—hackers from overseas, for instance—rather than in the context of domestic abuse. Thinking about things like passwords and default passwords is a welcome step, but in the kind of relationships that we are talking about and dealing with on a daily basis, the perpetrator will force the survivor to divulge the passwords to their devices and all their online accounts. That is not necessarily always thought about by these companies.

However, we are engaging with the companies as much as we can on what we are doing as a smallish team. Thinking through what can be done in future, it is about continuing to place emphasis on and put work into safety by design, which means ensuring that, from the get-go, product manufacturers and designers are thinking about how these products could be misused by domestic abusers. It also means working in collaboration with specialist violence against women and girls services to ensure that those features are designed out as far as possible.

Q68 Chris Elmore: I have a final question for Ms Concha on the online marketplaces, which do significant work in this area. In your view, how easy would it be to change the Bill to ensure that online marketplaces are part of it as well as manufacturers? The argument was made earlier that there most certainly is a responsibility on those who sell the product. Particularly if you are using, say, eBay, there is often limited interaction between the seller, the parent company and the person purchasing. Arguably, eBay as the organisation should take significant responsibility. I am keen to understand whether you think that is a relatively easy change for the Government to make to help close what you describe as a significant loophole in the Bill.

Rocio Concha: In terms of the Bill, an example could be to change or tighten the definition that you have of distributors. In terms of implementation, online marketplaces are the gateway between the consumers and the manufacturers of these products. They are the ones that have the power to make sure that these products comply with the law. Let me give you an example. We routinely do product tests to identify security vulnerabilities with these products. Often when we go to the online marketplaces, we get the answer that, because there is no regulation, they cannot take these products out.

We need the regulation to be clear that any smart product needs to comply with these baseline security requirements. Also, we need regulation to put responsibility on the online platforms to make sure that they are monitoring proactively which products are being sold on their platforms. That is key, and I feel that it is not optional. It is quite clear what is going to happen. There are bad actors out there, manufacturing products that are not going to comply with the baseline requirements. They know that there are not going to be the necessary checks in there by the online marketplaces, but the consumer does not know. It is impossible for the consumer to make an assessment of whether the product will be secure or not. Unless we put in regulation, you can see where all these bad actors are going to go.

Q69 Sally-Ann Hart (Hastings and Rye) (Con): Good afternoon to you both. It is clear that in the Bill the onus is on the manufacturers to meet the product security and safety requirements. Clearly, consumers also need to be aware of security threats both within the context of domestic abuse and otherwise. Should the Government be giving guidance to consumers? I do not know what the current situation is, but is it the role of the Government to give guidance to consumers?

Rocio Concha: I personally think that yes, the Government should provide information to consumers so that they are aware of this. Organisations such as ours also play a role, and we play it. We continuously publish our findings on security vulnerabilities and the sorts of things that consumers can do to protect themselves. There is a need for more information for consumers in general so that they can be aware that when they put these products in their homes, unless they take certain steps and buy products that meet the regulations that we hope will soon be introduced, they are putting themselves at risk.

Jessica Eagleton: I would agree with what my fellow panellist has said. When we think about tech abuse, we see that awareness of it is quite low among the general public. In fact, in a survey we ran last year the results were that two thirds of women did not know where to go for information if they thought that a device in their home was compromised. There is a role there for that awareness piece. At Refuge, the approach we tend to take is to empower survivors to use technology safely and to take back control of their products and technology. We have developed a range of resources to do that, but we would welcome more work and more efforts on this more widely.

Q70 Sally-Ann Hart: Where would a woman go as a first point of call if she discovered that something in her house was monitoring or stalking her?

Jessica Eagleton: The national domestic abuse helpline is the gateway to a wide range of domestic abuse services across the country. If she phoned the national domestic abuse helpline, we would be able to help her there, and help her with safety planning and next steps. We have some resources on our website and have recently developed a home safety tool that talks you through various devices in the home and gives tips on how to secure them.

Sally-Ann Hart: Thank you. I have no further questions.

Q71 Kevin Brennan: On the Which? side, Ms Concha, one of our earlier witnesses said that they thought it would be a good idea if the Bill were amended to establish in law a minimum time limit for which this type of device is supported. Is that something that Which? would support?

Rocio Concha: Yes, we would support that. If it is not possible to include it in the Bill, we would ask that the Bill allows for it to be included in secondary legislation in the future. We would be very supportive of introducing minimum supporting periods for products.

Q72 Kevin Brennan: You have not drafted an amendment by any chance, have you?

Rocio Concha: No, we have not, but we have provided amendments in other areas. We have provided an amendment to allow the Bill to introduce this through secondary legislation in the future, and there is an amendment there. We would be happy to discuss that in more detail.

Q73 Kevin Brennan: Genuinely, do you think that it is a preferable outcome for the measure to be in secondary legislation so that it might be a little more flexible, rather than putting it on the face of the Bill?

Rocio Concha: It depends. On these baseline security requirements, we firmly believe that the Bill should list them and be very clear that they will be included. In terms of the minimum security periods you provide to different products, it will depend on the different products and we do not want to delay the legislation to get to the bottom of that. It would be preferable to allow that legislation to be introduced as secondary legislation.

Q74 Kevin Brennan: Understood. Ms Eagleton, what are the devices that cause the most problems in relation to cases of domestic abuse and violence against women and girls?

Jessica Eagleton: Some of the most common devices we see reported to us include your smart home hubs, smart voice assistants, smart TVs, plugs, light switches and fitness trackers. Those are some of the most commonly misused. I myself have various different connected products at home.

Perpetrators quite often set up a host of different devices in the home. Recently, we supported a woman whose former partner had bought a whole host of devices, including smart cameras, a smart doorbell, a smart thermostat—all those kinds of things. She and her child felt like they were constantly being monitored; they talked about how exhausted they were by that constant surveillance.

Q75 Kevin Brennan: You mentioned that people could report that sort of thing using a helpline, but are women concerned that, if they make a report using the internet on their computer or telephone, that might be detected by the abusive partner?

Jessica Eagleton: It is definitely a big consideration. That is why we advise that people get in touch with us and then we can help with safety planning. If a perpetrator has access to those devices and a survivor moves to take back control of them and change the settings, that can be detected by someone with that access. We would work with a survivor to safety-plan how to control her technology.

Q76 Kevin Brennan: Finally, should the Government provide clarity by detailing measures that industry could take on the face of the Bill?

Jessica Eagleton: My fellow panellist may have some thoughts here as well, but that could certainly be useful for industry. Thinking about the general low awareness of tech abuse, it could be useful to provide industry with some certainty. It could play into that broader awareness piece, as well.

Kevin Brennan: Thank you.

Q77 Ruth Edwards: Ms Concha, you represent the consumer perspective. I wanted to ask about some concerns around labelling that were put to us this morning. In particular, Google mentioned that it has concerns about having a static label on the product because security information changes all the time—a product might be fine today, but it could discover a vulnerability about it tomorrow. It strikes me that we are dealing with a really wide range of security awareness, and ability to use and understand technology among consumers. Google suggested a sort of live label, such as a QR code, which could give the real-time security status. What do you think is the best way to communicate security information to consumers—such as the information in requirement 3, about the minimum time for which a product will receive security updates—bearing in mind the huge range of understanding and ability that we have in this area?

Rocio Concha: Is this about the length of time a product will be supported for? That information should be provided clearly at the point of sale, before you make a decision, so that you know you are going to buy something that may be supported for only two years, versus another product that may be supported for longer. That will hopefully provide everyone with the incentive to extend the number of years for which a product is supported.

We also need to make sure that that information is very clear. We should avoid "up to three years" and "for the lifetime of the product", which do not really mean much for the consumer. For the consumer to be able to act on that information, it has to be very clear and easy to find when they are making that decision. That is what I would say.

On changing the security, I am a little worried about the industry saying that it may change the period during which a product will be supported. If that change is to extend that period—great; if it is to reduce it, that is very bad. At that point, the consumer has made a decision and bought a product because that product was going to be supported for longer.

If someone was told that a product would be supported for four years, and they later found out it was two years, that product would not be fit for purpose. Under the Consumer Rights Act, you have a right on the same grounds as the Consumer Protection Act 1987.

The Chair: If there are no further questions from Committee members, that brings today's sitting to a close. On behalf of the Committee, I thank the witnesses for their evidence this afternoon. The Committee will meet again on Thursday at 11.30 am in Committee Room 14 to begin line-by-line consideration of the Bill.

Ordered, That further consideration be now adjourned. *—(Steve Double.)*

4.20 pm

Adjourned till Thursday 17 March at half-past Eleven o'clock.

Written evidence reported to the House

PSTIB01 Protect and Connect Campaign
PSTIB02 Openreach
PSTIB03 Speed Up Britain
PSTIB04 APWireless
PSTIB05 LPA Group Plc et al.
PSTIB06 CityFibre
PSTIB07 Littlehampton Sportsfield Charitable Trust
PSTIB08 NCC Group
PSTIB09 David Kleidermacher, on behalf of Google

PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

PRODUCT SECURITY AND TELECOMMUNICATIONS INFRASTRUCTURE BILL

Third Sitting

Thursday 17 March 2022

(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

Monday 21 March 2022

The Committee consisted of the following Members:

Chairs: Caroline Nokes, † Graham Stringer

† Baynes, Simon *(Clwyd South)* (Con)
Bhatti, Saqib *(Meriden)* (Con)
† Brennan, Kevin *(Cardiff West)* (Lab)
† Double, Steve *(St Austell and Newquay)* (Con)
† Edwards, Ruth *(Rushcliffe)* (Con)
† Elmore, Chris *(Ogmore)* (Lab)
† Grundy, James *(Leigh)* (Con)
† Hart, Sally-Ann *(Hastings and Rye)* (Con)
Hollern, Kate *(Blackburn)* (Lab)
Long Bailey, Rebecca *(Salford and Eccles)* (Lab)
† Lopez, Julia *(Minister for Media, Data and Digital Infrastructure)*
† Mishra, Navendu *(Stockport)* (Lab)
† Osborne, Kate *(Jarrow)* (Lab)
† Randall, Tom *(Gedling)* (Con)
† Vara, Shailesh *(North West Cambridgeshire)* (Con)
Warburton, David *(Somerton and Frome)* (Con)
Whitley, Mick *(Birkenhead)* (Lab)

Huw Yardley, Bethan Harding, *Committee Clerks*

† attended the Committee

Public Bill Committee

Thursday 17 March 2022

(Morning)

[Graham Stringer *in the Chair*]

Product Security and Telecommunications Infrastructure Bill

11.30 am

The Chair: We are now sitting in public and the proceedings are being broadcast. Before we begin, I have a few preliminary announcements. *Hansard* colleagues would be grateful if Members could email their speaking notes to hansardnotes@parliament.uk. Please switch electronic devices to silent. Tea and coffee are not allowed during sittings, but I have no guidance on jelly babies.

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

The Member who has put their name to the leading amendment in a group is called first. Other Members are then free to catch my eye to speak on all or any of the amendments in that group. A Member may speak more than once in a single debate. At the end of debate on a group of amendments, I shall call the Member who moved the leading amendment again. Before they sit down, they will need to indicate if they wish to withdraw the amendment or seek a decision. If any Member wishes to press any other amendment in a group to a vote, they need to let me know.

Clause 1

Power to specify security requirements

Chris Elmore (Ogmore) (Lab): I beg to move amendment 6, in clause 1, page 1, line 17, at end insert—

'(2A) The Secretary of State must exercise the power in subsection (1) so as to specify security requirements which make mandatory each of the first three guidelines in the Code of Practice for consumer IoT security published by the Department for Digital, Culture, Media and Sport on 14 October 2018 ("no default passwords", "implement a vulnerability disclosure policy" and "keep software updated")."

This amendment would set out the three security requirements expressly in Part 1 of the Bill rather than it being defined in future regulations.

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

Clause stand part.

Clauses 2 and 3 stand part.

New clause 3—*Report on security risks to UK consumer connectable products—*

'(1) The Secretary of State must prepare a report on the security risks to UK consumer connectable products—

(a) within the period 3 months beginning with the day on which this Act receives Royal Assent, and

(b) every 12 months thereafter.

(2) Any report prepared under subsection (1) must be laid before Parliament.'

This new clause would require the Secretary of State to lay before Parliament a report on the security risks to UK consumer connectable products.

Chris Elmore: It is a pleasure to serve under your chairmanship, Mr Stringer.

This important legislation establishes, through regulations, three core security requirements for "connectable products". The requirements derive from the voluntary 2018 "Secure by Design" code introduced by the Department for Digital, Culture, Media and Sport. The inclusion of these three requirements is, without doubt, a step that the Opposition welcome. However, we believe that the legislation can be improved, and that the three security requirements, rather than being defined in future regulations at the discretion of the Secretary of State, should be expressly set out in the Bill. That would be beneficial for two reasons. First, it would give manufacturers and distributors a greater understanding of the legal obligations that they face, thus speeding up the entire process. Secondly, it would ensure that the consumer was better protected, which I am sure we all agree would be a good thing. The consumer rights group Which? emphasised that when it gave oral evidence on Tuesday.

New clause 3 would require the Secretary of State to publish a report on the security risks to UK connectable products. On Tuesday, Madeline Carr, professor of global politics and cyber-security at University College London, said that she does not have an Alexa in her house because of the security risks that those devices, and others like them, pose. Tellingly, she also said that the Bill as constituted would not give her sufficient confidence to purchase one. Given that, and given the tragic scenes unfolding following Russia's invasion of Ukraine, and the willingness of that rogue regime to engage in state-sponsored cyber-warfare, the Opposition believe it is in the public and national interest to understand how secure our connected products really are. We are becoming more reliant on smart devices in our daily life, both professionally and personally. It is imperative that the security of these devices is routinely monitored and reported on.

As I stated on Second Reading, the Opposition support the Bill, but believe it can be strengthened. Amendment 6 and new clause 3 would ensure that consumers were better protected and more aware of the threats facing their connected devices. As such, I believe that all Committee colleagues should support amendment 6 and new clause 3.

The Minister for Media, Data and Digital Infrastructure (Julia Lopez): It is a pleasure to serve under your chairmanship, Mr Stringer. I apologise for giving you a dilemma about the advice on jelly babies. I will start with a few words about the importance of the Bill. As we heard from our panels of witnesses this week, and as

we know from our increasing dependence on technology, improving protection for consumers and networks from a range of harms associated with cyber-attacks is incredibly important. In the first half of last year, there were 1.5 billion attempted compromises of internet of things devices—double the 2020 figure for the same period. Voluntary standards, such as the 2018 code of practice for consumer IOT security, are not being adopted quickly or consistently enough. That is why we need legislation to progress security in the design of consumer connectable products.

Before turning to amendment 6, I thank the hon. Member for Ogmore for the constructive and helpful way that he has approached the legislation and for the Opposition's broad support of it. As this is the first Bill that I am taking through the House in its entirety, I am particularly grateful for that constructive approach. It may reassure him that the Government are committed to introducing security requirements based on the first three guidelines through regulations at the earliest appropriate opportunity. We have consulted on those security requirements and have communicated them extensively.

We have not been vague on the matter. In April 2021, we published our response to the call for views on consumer connectable product security legislation. We stated in detail how the three security requirements would work. When the Bill was announced by Her Majesty at the start of the Session, we repeated that commitment. Indeed, as hon. Members will see in the Bill's explanatory notes, we have again committed to those three requirements. We made that clear from the start for an important reason: we need industry to act and prepare for implementation. We do not want surprises for manufacturers, importers or distributors. They know what they have to do.

Amendment 6 is unnecessary, but might also be dangerous. We are keen to ensure that the legislation retains flexibility, so that it can adapt to and reflect the changing threat landscape, and the security requirements needed to address it. What might seem like a no-brainer security requirement today might become a security threat or barrier to security innovation in years to come.

Amendment 6 reaches back to 2018, when our code of practice was first published. Security requirements have developed since then. When the Bill is implemented, we do not think it should be constrained by what was appropriate five years ago. The requirements we will introduce are based on the first three guidelines in the code of practice, but they also contain necessary improvements. They are up to date, more detailed and have been translated into practical requirements that businesses can implement to get the right security outcomes without unnecessary burden. Stakeholder engagement and impact assessment work conducted since 2018 ensures that the guidelines are nuanced, and are in a robust and enforceable statutory framework that delivers optimal security outcomes.

Finally, hon. Members may not be aware that because this new legislation will impact on manufacturers globally, we have given notice of the Bill to the World Trade Organisation. We invited comments on our proposals two years ago, and when the Bill was introduced to Parliament, we gave notice again. We have worked to ensure that all manufacturers understand our intentions. Amendment 6, if accepted, would cause confusion by taking us back to 2018, and away from the more developed position we have reached on the three principles. That would cause market confusion, require new notification to the WTO, and potentially delay this vital regime from coming into force. With those reassurances, I hope the hon. Member will feel able to withdraw his amendment.

Clause 1 is needed to provide the Government with the necessary powers to specify and mandate security requirements, through secondary legislation, that businesses must comply with. There is a common notion that Governments are behind the curve when it comes to regulating technology. not in this case. By establishing a flexible and futureproof regulatory framework in this way, the Government can be agile and proactive in amending and introducing security requirements through regulations, in lockstep with tech innovation. Parliament will be able to scrutinise any future security requirements designated through the secondary legislation process and, as new threats emerge and international standards develop, we can act and set new security requirements, keeping consumer connectable product security up to date and fit for the future.

The purpose of clause 2 is to provide further detail about how the Secretary of State's power to specify security requirements can be used. Clause 3 is essential because it provides the Secretary of State with powers to specify circumstances in which a person is deemed to have complied with the security requirements. The clause, when exercised, would provide more than one route to compliance and would provide the necessary flexibility to accommodate and recognise international standards and mutual recognition agreements where appropriate.

I turn to new clause 3. In practice, it would commit the Government to reporting on a fixed basis on the security risks posed by products affected by the Bill. Those reports would be laid before Parliament. Cyber-security is definitely not an area where the Government hold back on publishing information. If we are to raise the cyber-resilience of the nation, we need to ensure that everyone is clear about the threat. In December, we published our national cyber strategy. The Government will continue to publish regular reports on our progress on that strategy, as we did with regard to the previous strategy. The Government also publish an annual report that surveys cyber-breaches across the economy. This report, together with others, forms a key part of the evidence base used to inform organisations about action to take to raise security standards. Indeed, the breaches survey meets the quality threshold to be managed as a set of official statistics.

Our National Cyber Security Centre is also a model of transparency. It is there to advise businesses, and guide them towards better managing cyber-threats. It publishes an annual report, and for those who want to focus on consumer connectable products, it provides specific advice on those, too. Parliament is already regularly kept informed of cyber-security matters; our regular publications are placed in the Library. Our national strategy, implemented with £2.6 billion of investment, is overseen by the Public Accounts Committee. The Intelligence and Security Committee and the Joint Committee on the National Security Strategy provide further oversight. Also, there are mechanisms for holding the Government to account in the manner intended by the provision, such as regular parliamentary debates and questions.

[Julia Lopez]

Cyber-security is a fast-moving and sensitive topic. A fixed-period reporting clause that imposes an obligation to report on security risks may duplicate existing activity. Such a system would also lack the agility necessary to enable us to report quickly when threats are identified. It may reassure the hon. Gentleman to know that the Secretary of State will be required to review the effectiveness of the Bill's enforcement regime; they, or the designated enforcing authority, will be required to report on that to the relevant departmental Select Committee after Royal Assent. The enforcement authority will also report its activity and findings, where appropriate. The measures already in place will likely meet the intention behind new clause 3. For the reasons that I have set out, I do not accept the need for the new clause.

I turn to the points that the hon. Gentleman raised about Dr Carr's concerns about Alexa, which I also found eye-catching. A lot of secondary legislation comes with this Bill, and that will hopefully reassure Dr Carr. I also note the comment made by a lot of our witnesses: we can never have 100% security with those devices. I therefore commend clauses 1 to 3 to the Committee.

Kevin Brennan (Cardiff West) (Lab): Good morning, everybody. Happy St Patrick's day to everyone. I congratulate the Minister on her first Bill. I have been through the process many times, and it is an exciting and proud moment to lead on a Bill for the Government for the first time. When I did it, my father, who was from West Cork, said, "Not bad for someone from the peat bogs of West Cork." I am sure that the Minister's family are equally proud of her achievement.

I want to raise a couple of general issues, as we are debating the first three quarters of the Bill in this grouping. I congratulate the Minister for providing such a comprehensive impact assessment on the Bill. I was slightly confused by the figure for the cost of business, which is set at net present value, and is put at "£1,246.9.9" million. That figure looks like a typo. I wondered what the correct figure was, and if the Minister could provide it. I suggest it is just the one "point nine".

This is a very significant piece of legislation, given the impact it will have on consumers and business. It is very technical. Page 8 of the impact assessment details the Government's key assumptions about how the Bill will impact on businesses. Businesses will have to dispose of devices that no longer satisfy the criteria that the Minister is likely to set. The impact assessment's optimistic assessment of what percentage of devices will have to be disposed of is 5%. Its working assessment is 45%. The figure it is using, however, for the impact on business is that 10% of devices will have to be disposed of by businesses.

11.45 am

I know that making impact assessments is not a precise science—to a certain extent, it is about trying to look into a crystal ball—but there seems to be quite a difference between the assumption that the Government are making of 10%, their best case scenario of 5%, and the worst-case scenario of 45%. Can the Minister explain to the Committee why there is such a wide range of figures? As far as business is concerned, those figures are very different. If the Government have got this wrong, and we are in the worst-case scenario, businesses will dispose of four times as many devices as the Government thought. I would be very grateful if the Minister could fill the Committee in on how there can be such a difference between those figures.

I have another point on the impact assessment; my hon. Friend the Member for Ogmore raised similar issues. It is about smart speakers and an exchange that took place in the evidence session. It is not the first time that I have asked someone whether they would regard it as safe to have one of these devices in their home—smart speakers; an Alexa-type device. Nevertheless, it seems extraordinary that a cyber-security expert giving evidence to this Committee should say that they would not have such a device in their home, because they do not trust them. That is basically what the witness told the Committee. I then asked her, "Well, following the passage of this Bill, would you have one in your home?", and her response remained no; she still would not trust them. A cyber-security expert giving evidence to the Committee said that even if the Bill contained the measures that the Minister is proposing, she still would not have such a device in her home.

The Minister might be interested to know that I asked the same question of the outgoing Information Commissioner when she appeared before the Digital, Culture, Media and Sport Committee, and she gave exactly the same answer; she, too, did not trust these devices sufficiently to have one in her home.

The Minister gave reassurances to my hon. Friend the Member for Ogmore, but how much further can she go to reassure this Committee that the Bill, and the subsequent regulations, will mean that consumers can safely have these devices in their home, and trust them? How can she ensure that security experts, the Information Commissioner and others will be able to say to the public, "It is largely safe to have these devices in your home"?

I say that because page 13 of the Government's impact assessment says that smart speakers are present "in 22% of households" in the UK, which means that over one in five households in the UK already have devices of this kind. I presume that in general we would want a roll-out of safe connectable devices, because of the benefits that they can bring; they have huge benefits for people who are disabled, who use them to improve their quality of life hugely. It is worrying, is it not, to be told that they are not to be trusted. Could the Minister give us any further reassurances on that point?

Finally, I understand that at a later date, a new clause may be introduced on the issues that were raised with Which? in the evidence session. Which? was keen to emphasise that it would like something done to alleviate inappropriate minimum periods for security updates in support of these connected devices. I will not pursue that further at this point, because I understand that there may well be an opportunity to debate a new clause on that at the end of our proceedings.

Julia Lopez: I thank the hon. Member for Cardiff West for his contribution and his kind comments. I will have to get back to him on the precise figures that he identified in the impact assessment. However, in relation to the breadth of the impact assessment, he will know from this legislation that we are taking a broad range of powers. As we debated earlier, that is very deliberate because this is a fast-moving area. Technology is developing

faster than Parliament can regulate it, which is a major challenge for Governments around the world. The Bill will help us to be nimble and agile in how regulate that technology.

A lot of the issues that the hon. Gentleman has concerns about will be something for secondary legislation, which we will be developing hand in glove with businesses so that we understand what is changing in the technological world and what impact that will have on matters such as the disposal of devices. I share his concerns about the environmental impacts if we get the regulations on that wrong—none of us wants to see a lot of technology become redundant.

We are trying to help consumers have more information so that if someone buys a device, they do not necessarily have to dispose of it simply because the period for which the manufacturer says it is covered has expired. It will be up to the consumer to decide whether to keep that device if they think it is less secure than it otherwise might be. It has been controversial to take these broad powers. We understand the concerns that any Parliament would have about the level of scrutiny it will have. However, the Government think that this is right because, as I say, we have to maintain that agility.

The hon. Member for Cardiff West referenced the points raised by Dr Carr. As I said earlier, I share those concerns. What we are trying to do is raise the level of security overall; we want to help consumers and manufacturers to understand this as an issue. This was initially a voluntary code, which did not do enough to make manufacturers take the cyber obligations seriously. There was an interesting discussion on the panels earlier this week when one contributor—I cannot remember who it was exactly—said that the legislation will give boards the spark or impetus to discuss and get funding for these kinds of cyber-security requirements for their products. If it is voluntary, it is very hard for anybody to make the case within their company that they need to take cyber-security seriously.

We hope that the secondary legislation will allay some of Dr Carr's concerns. We will never have 100% security, but we hope that these provisions will raise the bar overall and help to raise consumer and manufacturer awareness of cyber as a whole. I hope that those comments will reassure the hon. Gentleman. I also assure him that we will look at how to get the balance right in the secondary legislation, and we will be in close contact with businesses as we do so.

Chris Elmore: I listened to what the Minister had to say, in particular in relation to amendment 6. I take her at her word; it is a probing amendment, so I will withdraw it on the basis that she will bring forward secondary legislation in relatively short order. As she mentioned, cyber-security is a fast-paced and changing environment, so it is important that we do not wait a number of years for additional improvements to legislative competence.

On the basis of what the Minister said, I am also happy not to move new clause 3. However, I wonder whether she could write to me setting out the reporting periods that she mentioned, particularly in terms of the DCMS Committee, following Royal Assent—assuming that the Bill gets Royal Assent, which I am sure it will—as well as the other reporting obligations that she says the Secretary of State or reporting officer will have. The new clause seeks to place a requirement on the Secretary of State specifically in this new legislation. If the Minister feels that those things are already in train or are part of the reporting process, that is fine, and I am happy not to move the new clause. However, it would be good to have that list for future understanding—particularly if reporting does not take place, in which case the Opposition will hold the Government to account.

Julia Lopez: I am happy to write to the hon. Gentleman and offer those assurances. A new body will also be set up, which will probably have its own reporting requirements in relation to this legislation. These things will be developing, but I am happy to offer him the assurances he requested.

Chris Elmore: I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Clauses 1 to 3 ordered to stand part of the Bill.

Clause 4

Relevant connectable products

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

The Chair: With this it will be convenient to discuss clauses 5 and 6 stand part.

Julia Lopez: Clauses 4 to 6 define the products to which the new regulatory regime will apply. Clause 4 introduces the terms "internet-connectable product", "network-connectable product" and "excepted product". Clause 5 defines the terms "internet-connectable" and "network-connectable". It is a pivotal clause in capturing the necessary products that make up a huge part of the internet of things threat landscape. Any network is only as secure as its weakest link, and that could be a single consumer connectable product.

Focusing on a product's capabilities—instead of attempting to exhaustively list all consumer connectable products—is part of our agile, future-proof approach. We are ensuring that the Bill will remain relevant and effective by capturing new consumer technologies that come to market, based on their capabilities and the risks they present.

Many products captured by the Bill are capable of connecting to the internet, exposing them to remote access and attack. Those are "internet-connectable products", such as routers, smartphones and certain smart appliances. Some products captured by the Bill are not able to connect to the internet directly, but can connect to other products. In doing so, they can form, and contribute to the formation of, networks, meaning that vulnerabilities in those products can open the door to cyber-attack. Those are "network-connectable products", such as certain smart lightbulbs, smart home products, and headphones.

Clause 6 defines the term "excepted product". It allows the Secretary of State to except products from the scope of the Bill via regulations. The Government intend to except products from the scope of the Bill where inclusion would subject them to double regulation or be disproportionate to their risk profile. The Government have consulted on that approach. Products such as electric vehicles, medical devices and smart meters will

[Julia Lopez]

be excepted from scope because they are already, or soon will be, covered by alternative regulation. I therefore commend clauses 4 through 6 to the Committee.

Question put and agreed to.

Clause 4 accordingly ordered to stand part of the Bill.

Clauses 5 and 6 ordered to stand part of the Bill.

Clause 7

RELEVANT PERSONS

Chris Elmore: I beg to move amendment 7, in clause 7, page 5, line 24, at end insert—

"(5A) A person who provides an online facility through which a distributor makes a product available in the United Kingdom is also a distributor."

This amendment would ensure that online marketplaces are considered to be distributors and are thus subject to the security requirements of the Bill.

The Chair: With this it will be convenient to discuss clauses 7 to 25 stand part.

Chris Elmore: The amendment itself is fairly self-explanatory. However, I will take the opportunity to speak briefly on it in the hope of persuading Conservative Members—and indeed the Minister—to support it.

Clause 7 defines the relevant persons subject to the security requirements as being manufacturers, importers and distributors. Crucially, however, online platforms such as eBay and Amazon are not defined as falling under any of those categories. To my mind, that is both deeply concerning and preposterous, given that, under any definition, online platforms such as the two I have just mentioned are without doubt distributors themselves.

I am sure everyone in this Committee has either sold or bought something through eBay or Amazon. The oversight in the Bill has real-world consequences, as products sold on those online platforms will not be policed in the same way. That is problematic, as research by groups such as Which?—which we heard evidence from earlier this week—has consistently shown that online marketplaces are flooded with insecure products, while the Bill would do nothing to increase the legal responsibility online marketplaces have for the safety and security of products sold through them.

In tabling the amendment, we are merely expanding the number of organisations that the security requirements would apply to, in order to better protect all our constituents, which is the expressed aim of the Bill according to the Minister's opening remarks and indeed those of the Secretary of State at Second Reading. I therefore urge the Minister and all Committee members to support the amendment.

Kevin Brennan: I support my hon. Friend in pressing the amendment to a vote. As we heard from the Minister, the Bill covers quite a lot of different devices. The examples given by the Government in their impact assessment include the following:

"Smartphones; connectable cameras, TVs and speakers; connectable children's toys and baby monitors; connectable safety-relevant products such as smoke detectors and door locks; Internet of Things base stations and hubs to which multiple devices connect; wearable connectable fitness trackers; outdoor leisure products, such as handheld connectable GPS devices that are not wearables; connectable home automation and alarm systems; connectable appliances, such as washing machines and fridges"

and, as we have heard, "smart home assistants", including things such as Alexa-type smart speaker products.

12 noon

I would like to understand from the Minister why online marketplaces are not included, and how many of the devices that the Government list in their impact assessment are acquired from online marketplaces and would therefore be outside the Bill's scope, if my hon. Friend's amendment and the concerns Which? has expressed are right. Of the products I listed—the Government's own list—how many are purchased through online markets and how many are purchased in a more traditional fashion? It seems likely that the numbers of products purchased online will only increase over time; I have personally purchased several of the products on that list online, and I am sure other members of the Committee have as well. Can the Minister explain in a bit more detail the Government's thinking as to why they are excluding online distributors from the Bill, such as those outlined by my hon. Friend and those of concern to consumer organisations such as Which?

Julia Lopez: I thank the hon. Members for Ogmore and for Cardiff West, and I am happy to address their concerns. The Bill covers obligations on manufacturers, importers and distributors, but I will provide a bit more detail.

Clause 7 specifies which relevant persons will be responsible for ensuring that the security requirements are properly complied with. In that regard, a "relevant person" is defined as a manufacturer, importer or distributor of a relevant connectable product. As a result, amendment 7 is wrong to suggest that online marketplaces are exempt from this new legislation. Online marketplaces do not just offer products on behalf of third parties, but are often acting as the retailer, so in those cases the full security requirements apply. I accept that there may be instances in which the online marketplace is not the distributor. None the less, it is necessary for the third party operating in the marketplace to comply with the security requirements, and it is not just that one party who carries liability under the Bill: the manufacturer and importer also have responsibility. We think we have taken a belt-and-braces approach in that regard.

We have also worked closely with industry to make sure the regulation is proportionate and fits the wider regulatory environment for product safety. Manufacturers care a great deal about these regulatory requirements. On Tuesday, we heard from a representative of Google, who described how it works to comply with requirements in many different jurisdictions. Over the past three years, hundreds of manufacturers have engaged with my Department through the many public consultations and industry discussions we have had. The hon. Member for Ogmore gives the impression that amendment 7 would provide consumers with a vital line of defence, but that is not the case: there are already multiple lines of defence in this Bill.

It is also worth noting that consumers can never be 100% protected by regulation—a point that we have already discussed this morning. We need to have a broader approach to raising national cyber-resilience, which is why in December we published our national

cyber strategy. The Cyber Aware campaign is ongoing—hon. Members may have seen the advertisements last weekend, or the ones on the radio and online this week. We also have a range of school programmes designed to reach parents and teachers in order to raise cyber-security awareness, and the Home Office, the police and the NCSC run regular campaigns at a local level in every region of the country. In relation to the comments made about Ukraine, the point is even more important because of the context in which we are operating.

Kevin Brennan: Just to be clear, if, for example, I purchased a connectable baby monitor online through Amazon, but it came from a third-party supplier—which is quite common when customers are given that list of products to buy—how would the Bill impact on that device and its availability in the UK?

Julia Lopez: As I say, we are putting requirements on not just manufacturers, but the importer. The importer would be under an obligation to check whether the product fulfilled some of the requirements we would have for it, as would the distributor. I would hope that, along the chain, that product would have been checked several times to make sure it complies.

We have done a lot of work on general cyber-resilience. I will take this opportunity to add that it is also important that we as Members of Parliament try to make our constituents aware of the increasing challenges we face with cyber-resilience, and that we all need to have our own cyber-hygiene in that regard.

The amendment is well intentioned—we understand where the hon. Member for Ogmore is coming from—but it is drafted in a way that would have a much broader reach than just online marketplaces. It would impose security requirements on businesses that cannot comply with them, such as advertising platforms and website hosting services. Distributors use many online facilities offering a vast array of cloud services to support e-commerce to make their products available. As drafted, the amendment would extend duties beyond what is intended.

The Government have carefully considered the amendment. It is clear that our intention is to secure consumer connectable products in the most effective and proportionate manner, without hindering business growth and the online retail facilities enjoyed by consumers. For the reasons I have set out, I am not able to accept the amendment. I hope the hon. Gentleman will consider withdrawing it.

I turn now to chapter 2 of the Bill and clauses 8 to 25. These clauses place duties on businesses in the supply chain of a consumer connectable product to comply with security requirements. Compliance is fundamental to the operation of the regulatory regime. Under these clauses, manufacturers, distributors and importers must prepare, or ensure the presence of, a document to accompany the product that states that, in the opinion of the manufacturer, it has complied with the security requirements, before that product is made available in the UK. I note the point that was made about baby monitors. I hope that, in that process, there would be clear information and a record provided with the product that stated compliance.

The clauses in chapter 2 also require that businesses take all reasonable steps to investigate a compliance failure or potential compliance failure. That is vital to hold businesses accountable for complying with their security requirements and to mandate investigation of potential compliance failures. If compliance failure has occurred, businesses in the supply chain must take all reasonable steps to prevent the product from reaching UK customers and remedy the compliance failure. The measure is needed to ensure that insecure products do not remain on the market and that those that have not yet reached UK customers are prevented from doing so.

Finally, the clauses in chapter 2 require manufacturers and importers to retain records of compliance failures and investigations for at least 10 years. The Secretary of State is able to request this information to investigate and to enforce the legislation. These duties encourage ongoing compliance and accountability. The records will allow a clear audit of the importer's and manufacturer's activities, so that we can have effective enforcement.

Chris Elmore: I have listened to the Minister. The Opposition are not in any way suggesting that the Government do not do an awful lot on cyber awareness-raising. All Governments could do more—that is the nature of teaching and learning and of being able to get our constituents to understand the cyber-security space and the impact that it can have on their homes.

In response to my hon. Friend the Member for Cardiff West, the Minister mentioned the belt-and-braces approach. However, organisations such as Which? say that there is an exemption for online marketplaces such as Amazon and eBay. The Online Safety Bill has of course been published today, and there are economic crime impacts linked to this. If this is a belt-and-braces approach, as the Minister says, surely another level of protection would be to include the online marketplaces. She says there are three stages that could be protected—importer, product design and distribution—but there is this gap through which some products could come. Therefore, I am not minded to withdraw the amendment and would ask the Committee for a decision.

Question put, That the amendment be made.

The Committee divided: Ayes 4, Noes 8.

Division No. 1]

AYES

Brennan, Kevin	Mishra, Navendu
Elmore, Chris	Osborne, Kate

NOES

Baynes, Simon	Hart, Sally-Ann
Double, Steve	Lopez, Julia
Edwards, Ruth	Randall, Tom
Grundy, James	Vara, Shailesh

Question accordingly negatived.

Clauses 7 to 25 ordered to stand part of the Bill.

Clause 26

ENFORCEMENT OF PART 1

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

The Chair: With this it will be convenient to discuss clauses 27 to 52 stand part.

Julia Lopez: Clause 26 gives the Secretary of State responsibility for enforcing the product security provisions in the Bill, and clauses 27 to 52 create the regime. This allows the Secretary of State to authorise another person, and pay them, to carry out enforcement functions. The provisions provide powers to issue enforcement notices—including compliance notices, stop notices and recall notices—as well as powers to forfeit products and issue monetary penalties.

Additional enforcement powers include the power to seize and detain products, publish information about compliance failures and the details of the enforcement action taken, recall products, and disclose information as necessary to conduct enforcement activity. The Bill includes two offences—the offence of failure to comply with an enforcement notice and the offence of purporting to act as authorised to exercise enforcement function—as well as adopting within the PSTI regulatory regime the offences found in schedule 5 to the Consumer Rights Act 2015. I commend the clauses to the Committee.

Question put and agreed to.

Clause 26 accordingly ordered to stand part of the Bill.

Clauses 27 to 52 ordered to stand part of the Bill.

Clause 53

GUIDANCE

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

The Chair: With this it will be convenient to discuss clauses 54 to 56 stand part.

Julia Lopez: Clauses 53 to 56 cover guidance and interpretation of the Bill. They allow for guidance to be issued to support relevant operators to meet their obligations. They also set out the technical terms and interpretations of the commonly used terms throughout the Bill. I commend the clauses to the Committee.

Question put and agreed to.

Clause 53 accordingly ordered to stand part of the Bill.

Clauses 54 to 56 ordered to stand part of the Bill.

Clause 57

MEANING OF "OCCUPIER" IN RELATION TO LAND OCCUPIED BY AN OPERATOR

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

Julia Lopez: It is crucial that, where telecoms operators have apparatus installed on land, they can request new or additional code rights, allowing them to maintain, expand and improve their existing networks, improving service and connectivity, to the direct benefit of consumers. I hope we all wish to see that. At present, this is not always possible. There are some specific scenarios in which operators with apparatus already installed on land, such that they occupy the land, are unable to obtain new code rights or follow an existing statutory process to have an agreement that has run its course replaced by a new agreement, which I will refer to today as a renewal agreement.

For example, in some cases the parties might have an existing agreement that, for whatever reason, proceeds on a more informal basis and is not set out in writing, or otherwise does not meet the necessary criteria for it to be renewed under an existing statutory process. The operator is therefore still authorised under the existing agreement to keep their apparatus on the land, but under the current legislative framework cannot pursue a renewal agreement through an existing statutory process.

12.15 pm

At the same time, the operator cannot seek a completely new code agreement because only an occupier of land can grant code rights. Some operators with apparatus installed on land could be, in legal terms, occupying that land. Where that is the case, clearly the operator cannot enter into a legal agreement with themselves. In theory, an operator could dismantle and remove their apparatus from the land so that it is no longer in occupation, and then negotiate new rights with the landowner, but that would mean service disruptions for consumers, as well as unnecessary costs and delays. We need to address that and ensure that operators with apparatus installed on land who do not currently have code rights for that apparatus can request them without having to take unnecessary and impractical steps, such as vacating the land.

A different scenario arises where an operator has an existing agreement to which the code applies, but needs to do something that falls outside the scope of that agreement. For example, the operator might need to upgrade their apparatus to improve capacity or deliver 5G services, but their rights under the existing agreement may not cover that. Under the code, there is no ability to apply to the court for modified terms to be imposed until the agreement has run its initially agreed course, or until the point at which the site provider could normally have sought to bring the agreement to an end. We think it right that terms, once agreed, be settled for the duration of an agreement.

However, the situation is different where an operator who already occupies the land needs a new code right to enable them to undertake additional activities, such as upgrading apparatus, as I mentioned. The length of agreements to which the code applies can be in the region of 10 years, or potentially much longer. It is therefore feasible that, with continued advances in technology, an operator may want to carry out activities that were not envisaged when they entered into the agreement. The restriction on their ability to seek new code rights for those activities prevents operators from taking advantage of the latest tech and improving digital services and coverage quickly to meet customer demand.

The policy intention behind clause 57 is to resolve the situations that I have outlined by giving operators who are in occupation of land an alternative party from whom they can obtain new and additional rights. Primarily, that will be any other person who for the time being exercises powers of management or control over the land. If no such person can be identified, the operator can seek code rights from every person who has an interest in the land that would be prejudicially affected by the exercise of the code right sought.

The clause deals with very complex and technical issues. Since the Bill was introduced, my Department has been testing the provisions to ensure that they meet

the policy objectives and that they have no adverse impacts on other parts of the code, or on how the code operates in practice. Should we consider it appropriate to make further changes to the clause, in line with our policy intentions, we will table an appropriate amendment.

Kevin Brennan: The Minister says that the Government might revisit the clause, perhaps in the other place. If somebody who is operating equipment on the land is potentially deemed legally to be the occupier, under the provisions in the clause would the person who would then be asked to consult about further extending any arrangements be the landowner? Is that the assumption in the clause, in most instances?

Julia Lopez: As I said, this is a very complex and technical area. I do not want to provide the hon. Member with an incorrect answer, because this is one of the issues on which we are still in discussions with industry to ensure that we get it right. I believe that is the intention, but I will have to get back to him.

Kevin Brennan: Some inspiration might come to the Minister during the course of the debate. It seems to me quite an important question. I thought that what she meant was that, in an instance where somebody is deemed to be the operator on the land, because they have the equipment there, they obviously cannot grant themselves an extension of permission, and so it would be sensible for there to be a way to go to the landowner in order to achieve that further agreement. If that is not the case, that is quite important, because who will they go to in that instance? She said that if the landowner or interested party could not be identified, it would be people with a principal interest. What sorts of people would that be? Would it be the local community, or neighbours of the land involved? Even if she cannot offer an explanation now, it is quite important that the Committee at least has a grasp of what is intended by the clause.

Julia Lopez: This is tricky, because I wish I could provide greater clarity, but I cannot, which is obviously an unsatisfactory position to be in. In this case, I think the court would be approached to make a decision if the landowner was not in a position to grant those rights and they could not get a position out of the landowner. The intention, I think, would be for it to be decided at a legal level. I apologise that I cannot provide clarity.

Without the clause, there is a gap in the legislation that prevents operators who need code rights from being able to obtain them. This has potentially adverse consequences for consumers and businesses, with the risk of service disruptions and unnecessary delays in the delivery of improved capacity and enhanced services. As we all increasingly rely on digital services, it is important to address this situation. This is an area of active discussion, because we want to make sure we get it right. I believe it would be the case that, if the landowner were not in a position to offer the rights, the operator would go to the court to seek redress.

Kevin Brennan: I understand the difficulty the Minister faces, but it would be helpful if there was official support for her at times when technical questions are asked. It is important that the Committee gets a full explanation before agreeing to a clause. The sensible thing to do in this instance would be for the Government to revisit the clause—possibly on Report. It would certainly be of help if, by then, a clearer view as to the intention could be given to Members of the Committee and people interested in the Bill. I am sure there is a fairly straightforward answer to the question, so we should make note of the fact that it needs to be dealt with at some point.

Julia Lopez: I acknowledge that this is legally a very complex area. It is something that we have not entirely settled on, and it is under active consideration. We will come back to the Committee if we believe we have not got the policy intention correct. I am sorry that I was unable to address the hon. Member's point in greater detail, but I am reluctant to provide information that might not be correct.

Question put and agreed to.

Clause 57 accordingly ordered to stand part of the Bill.

Clause 58

Rights under the electronic communications code to share apparatus

Julia Lopez: I beg to move amendment 1, in clause 58, page 41, line 25, at end insert—

'(4A) In paragraph 13 (access to land)—

(a) in sub-paragraph (1)(a), for "paragraph 3" substitute "paragraph 3(1)";

(b) in sub-paragraph (2), for "paragraph 3" substitute "paragraph 3(1)".

(4B) In paragraph 38 (right of landowner or occupier of neighbouring land to require removal of electronic communications apparatus), in sub-paragraph (3), for "paragraph 3(h)" substitute "paragraph 3(1)(h)".'

This amendment is consequential on the amendment made by clause 58(2)(a) to paragraph 3 of the electronic communications code.

The Chair: With this it will be convenient to discuss clause stand part.

Julia Lopez: Clause 58 deals with the sharing of telecommunications apparatus between operators within the electronic communications code. It inserts a right to share apparatus into paragraph 3 of the code, which sets out a list of rights that are statutory "code rights." The code rights in paragraph 3 must be conferred on an operator by an occupier or imposed by a tribunal. The 2017 code reforms introduced paragraph 17 automatic rights, allowing operators to upgrade or share their apparatus without the need for an agreement. Those automatic rights are separate from the paragraph 3 code rights and are subject to strict limitations.

Since their introduction, there has been confusion about the interaction between the paragraph 17 automatic rights and the paragraph 3 code rights. In particular, while "upgrading" is a paragraph 3 code right, sharing is not. Clause 58 addresses this by making apparatus sharing a paragraph 3 code right that an operator—the "first operator"—can request to be included in an agreement to which the code applies. Clause 58 also amends the statutory purposes in paragraph 4 of the code to include sharing activities.

Apparatus sharing is a cost-effective way for operators to extend their networks without having to build extensive infrastructure themselves, helping to deliver greater coverage,

[Julia Lopez]

capacity and consumer choice, while reducing impacts on the environment and disruption caused by installation works. As with the other code rights, if agreement on rights to share cannot be reached consensually, an operator may ask a tribunal to impose the requested rights. In those circumstances, the tribunal will apply the public benefit test and the statutory valuation regime, as it already does for other code rights.

If the right to share is a statutory code right, the factors that a tribunal will consider in deciding whether such a right should be imposed—and if so, on what terms—will be the same as those for all other code rights. Including a right to share apparatus in the paragraph 3 code rights will therefore provide greater certainty for all parties and support smoother negotiations.

Code rights can only be obtained in relation to land. Consequently, the new right to share apparatus can be requested only by the first operator that is keeping apparatus installed on, under or over land. A second operator that wishes to share the use of that apparatus will not be able to request from an occupier a paragraph 3 right permitting them to do so. Instead, once the occupier has conferred such a sharing right on the first operator, the second operator will need to negotiate the sharing of the apparatus with the first operator.

The first operator's right to share their apparatus will, like other code rights, be exercisable only in accordance with the wider terms of the agreement. It will therefore be important for the first operator to consider carefully any terms that it may need included in its agreement with an occupier, such as additional access rights, to enable any subsequent sharing of the apparatus with other operators. To that end, clause 58 inserts corresponding code rights for the first operator to enter and carry out works on the land for the purpose of such apparatus sharing.

Finally, it should be emphasised that the new right to share introduced by clause 58 is entirely separate from the automatic rights to share that are currently available under paragraph 17 of the code, and to the rights introduced by clauses 59 and 60. Those are automatic rights—subject to specific conditions—that do not need to be agreed with a landowner or imposed by the courts. The rights in clause 58 cover situations where the operator wants rights to share over and above those automatic rights.

Government amendment 1 is a consequential amendment that reflects the restructuring of paragraph 3 provided for by clause 58(2)(a) of the Bill. It replaces cross-references to paragraph 3 of the code with cross-references to sub-paragraph 3(1).

Clause 58 introduces rights to share apparatus to the menu of code rights that is currently set out in paragraph 3 of the code. In doing so, new sub-paragraph 3(2) will be inserted into the code, setting out who can obtain a right to share apparatus. The current paragraph 3 will therefore become sub-paragraph 3(1) of the code. As there are references to paragraph 3 in other parts of the code, consequential amendments are necessary so that anyone reading the code is referred instead to the new sub-paragraph 3(1).

Amendment 1 agreed to.

Clause 58, as amended, ordered to stand part of the Bill.

Clause 59

Upgrading and sharing of apparatus: subsisting agreements

Chris Elmore: I beg to move amendment 9, in clause 59, page 41, line 42, after "agreement" insert

"other than with a private landlord".

This amendment, together with Amendments 10, 11 and 12, would apply a different regime under the Electronic Communications Code to private landlords, giving automatic upgrade rights for operators to properties owned by private landlords subject to the condition that the upgrading imposes no additional burden on the other party to the agreement.

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

Amendment 10, in clause 59, page 43, line 26, at end insert—

"5B (1) This paragraph applies where—

(a) an operator ('the main operator') keeps electronic communications apparatus installed on, under or over land, and

(b) the main operator is a party to a subsisting agreement in relation to the electronic communications apparatus.

(2) If the conditions in sub-paragraphs (3), (4) and (6) are met, the main operator may—

(a) upgrade the electronic communications apparatus, or

(b) share the use of the electronic communications apparatus with another operator.

(3) The first condition is that any changes as a result of the upgrading or sharing to the electronic communications apparatus to which the agreement relates have no adverse impact, or no more than a minimal adverse impact, on its appearance.

(4) The second condition is that the upgrading or sharing imposes no additional burden on the other party to the agreement.

(5) For the purposes of sub-paragraph (4) a burden includes anything that—

(a) has an adverse effect on the person's enjoyment of the land, or

(b) causes loss, damage or expense to the person.

(6) The third condition is that, before the beginning of the period of 21 days ending with the day on which the main operator begins to upgrade the electronic communications apparatus or (as the case may be) share its use, the main operator attaches a notice, in a secure and durable manner, to a conspicuous object on the relevant land.

(7) A notice attached for the purposes of sub-paragraph (6) must—be attached in a position where it is reasonably legible,

(a) be attached in a position where it is reasonably legible,

(b) state that the main operator intends to upgrade the electronic communications apparatus or (as the case may be) share its use with another operator,

(c) state the date on which the main operator intends to begin to upgrade the electronic communications apparatus or (as the case may be) share its use with another operator,

(d) state, in a case where the main operator intends to share the use of the electronic communications apparatus with another operator, the name of the other operator, and

(e) give the name of the main operator and an address in the United Kingdom at which the main operator may be contacted about the upgrading or sharing.

(8) Any person giving a notice at that address in respect of that electronic communications apparatus is to be treated as having been given that address for the purposes of paragraph 91(2).

(9) Any agreement under Part 2 of this code is void to the extent that—

(a) it prevents or limits the upgrading or sharing, in a case where the conditions mentioned in sub-paragraphs (3), (4) and (6) are met, of any electronic communications apparatus to which the agreement relates that is installed on, over or under land, or

(b) it makes upgrading or sharing of such electronic communications apparatus subject to conditions to be met by the operator (including a condition requiring the payment of money).

(10) Nothing in this paragraph is to be read as conferring a right on the main operator to enter the land which the main operator would not otherwise have, when upgrading or sharing the use of the electronic communications apparatus.

(11) References in this paragraph to sharing electronic communications apparatus include carrying out works to the electronic communications apparatus to enable such sharing to take place.

(12) In this paragraph—

'the relevant land' means—

(a) in a case where the main operator has a right to enter the land, that land;

(b) in any other case, the land on which works will be carried out to enable the upgrading or sharing to take place or, where there is more than one set of works, the land on which each set of works will be carried out;

'subsisting agreement' has the meaning given by paragraph 1(4) of Schedule 2 to the Digital Economy Act 2017."

This amendment, together with Amendments 9, 11 and 12, would apply a different regime under the Electronic Communications Code to private landlords, giving automatic upgrade rights for operators to properties owned by private landlords subject to the condition that the upgrading imposes no additional burden on the other party to the agreement.

Clause stand part.

Amendment 11, in clause 60, page 43, line 38, after "land" insert

"not owned by a private landlord"

This amendment, together with Amendments 9, 10 and 12, would apply a different regime under the Electronic Communications Code to private landlords, giving automatic upgrade rights for operators to properties owned by private landlords subject to the condition that the upgrading imposes no additional burden on the other party to the agreement.

Amendment 12, in clause 60, page 44, line 47, at end insert—

"17B (1) This paragraph applies where—

(a) an operator ('the main operator') keeps electronic communications apparatus installed on, under or over land owned by a private landlord,

(b) the main operator is not a party to an agreement under Part 2 of this code in relation to the electronic communications apparatus, and

(c) the electronic communications apparatus was installed before 29 December 2003.

(2) If the conditions in sub-paragraphs (3), (4) and (6) are met, the main operator may—

(a) upgrade the electronic communications apparatus, or

(b) share the use of the electronic communications apparatus with another operator.

(3) The first condition is that any changes as a result of the upgrading or sharing to the electronic communications apparatus to which any existing agreement between the operator and the landlord relates have no adverse impact, or no more than a minimal adverse impact, on its appearance.

(4) The second condition is that the upgrading or sharing imposes no additional burden on the landlord.

(5) For the purposes of sub-paragraph (4) a burden includes anything that—

(a) has an adverse effect on the person's enjoyment of the land, or

(b) causes loss, damage or expense to the person.

(6) The third condition is that, before the beginning of the period of 21 days ending with the day on which the main operator begins to upgrade the electronic communications apparatus or (as the case may be) share its use, the main operator attaches a notice, in a secure and durable manner, to a conspicuous object on the relevant land.

(7) A notice attached for the purposes of sub-paragraph (6) must—

(a) be attached in a position where it is reasonably legible,

(b) state that the main operator intends to upgrade the electronic communications apparatus or (as the case may be) share its use with another operator,

(c) state the date on which the main operator intends to begin to upgrade the electronic communications apparatus or (as the case may be) share its use with another operator,

(d) state, in a case where the main operator intends to share the use of the electronic communications apparatus with another operator, the name of the other operator, and

(e) give the name of the main operator and an address in the United Kingdom at which the main operator may be contacted about the upgrading or sharing.

(8) Any person giving a notice at that address in respect of that electronic communications apparatus is to be treated as having been given that address for the purposes of paragraph 91(2).

(9) Nothing in this paragraph is to be read as conferring a right on the main operator to enter the land which the main operator would not otherwise have, when upgrading or sharing the use of the electronic communications apparatus.

(10) References in this paragraph to sharing electronic communications apparatus include carrying out works to the electronic communications apparatus to enable such sharing to take place.

(11) In this paragraph 'the relevant land' means—

(a) in a case where the main operator has a right to enter the land, that land;

(b) in any other case, the land on which works will be carried out to enable the upgrading or sharing to take place or, where there is more than one set of works, the land on which each set of works will be carried out."

This amendment, together with Amendments 9, 10 and 11, would apply a different regime under the Electronic Communications Code to private landlords, giving automatic upgrade rights for operators to properties owned by private landlords subject to the condition that the upgrading imposes no additional burden on the other party to the agreement.

Clause 60 stand part.

Chris Elmore: These amendments would apply a different regime to private landlords under the 2017 electronic communications code, giving operators automatic upgrade rights for properties owned by private landlords, subject to the condition that the upgrading imposes no additional burden on the other party to the agreement.

[Chris Elmore]

When we talk of the digital divide in our telecommunications infrastructure, we often speak of it in terms of a divide between rural and urban areas. Indeed, it is true that a divide exists between rural and urban areas in levels of connectivity, and the Bill has been designed to help reduce the rural-urban connectivity gap, which the Labour party wholeheartedly supports.

However, a division also exists within urban areas themselves. Catherine Colloms, the managing director of Openreach, said in evidence that it is particularly difficult for Openreach and similar organisations to upgrade properties that are owned by private landlords to full fibre. Openreach alone currently has 55,802 multi-dwelling unit premises on hold. Based on this, it is forecast that 1.5 million MDU premises could be unserved by the end of the commercial roll-out.

12.30 pm

My hon. Friend the Member for Hackney South and Shoreditch (Dame Meg Hillier) has informed me of blocks of flats in her constituency where tenants have been trying to get superfast broadband installed since 2015, but to no avail. That is hugely problematic, and the pandemic has only served to aggravate the issue. With the rise of home learning and home working, children and workers based in these high-rise tower blocks are having to deal with slower download speeds and inferior connectivity when compared to those who potentially live on the same street as them but are based in a house rather than an MDU.

This is not about gaining unfettered access to properties; it is about gaining better access to MDUs with the express aim of reducing the digital and socioeconomic divide in towns and cities the length and breadth of the United Kingdom. I hope that Members are able to support the amendment for the reasons I have outlined. Reducing the digital divide is something that I hope all members of the Committee can agree on.

Julia Lopez: I thank the hon. Member for tabling these amendments. I represent an urban constituency and, as the Minister for digital connectivity, I am very alive to any concerns about the digital divide. I have tested the legislation to make sure that we are not exacerbating that. The amendments relate to circumstances in which an operator can upgrade or share the use of their apparatus without specific permission from a landowner or a court order. Crucially, the amendments relate to rights that the Bill grants retrospectively to agreements that are already in place. The amendment seeks to expand those rights in circumstances where apparatus is situated on, under or over land owned by private landlords.

Retrospective legislation must take particular care to strike a balance between impacts on individual rights and any public benefit that the legislation aims to deliver. The Government believe at this time that expanding retrospective upgrading and sharing rights in the way these amendments suggest would not be justified. Upgrading and sharing electronic communications apparatus offers a wide range of substantial benefits. Those are benefits that the Government specifically recognised in their 2017 reforms, when limited automatic rights were introduced for operators to upgrade and share their apparatus. The exercise of the new upgrading and sharing rights was made subject to certain conditions. Those conditions were intended to strike the right balance between the rights of individual landowners hosting apparatus and the public benefits delivered by operators upgrading and sharing their apparatus.

The changes made in the 2017 reforms therefore permit upgrading and sharing to take place without a landowner's specific consent only where any impacts on that individual will be limited. However, it was recognised that any use of those rights could have some impact, albeit very limited, on individual landowners.

Ruth Edwards (Rushcliffe) (Con): I remind the Committee of the declaration of interest that I made: I have worked for a number of providers, including BT and techUK, that will be affected by the legislation, and I carried out cyber-security consulting for MHR last year. I agree with the Minister about the need to seek a balance between the rights of landowners and the rights of operators. However, we cannot lose sight of the fact—this is a point she has been making powerfully—that we must get behind upgrading our digital infrastructure as fast as is practicably possible.

I am aware that we are about to debate amendment 8, which would make it more expensive for operators to access land, and put them at a disadvantage compared with other utility companies. Does the Minister agree that adopting amendments 9 to 12—and then 8—would risk sending a mixed signal to the market? On the one hand we are making it more expensive and difficult for our operators to access land, but on the other hand we are rolling back the scrutiny that they have to access private property at the moment.

The Chair: Before I call the Minister, I will take this opportunity to say that interventions should be relatively short and to the point. It will not be difficult for hon. Members to catch my eye to make points in a debate if they wish to.

Julia Lopez: I thank my hon. Friend for her intervention. I know that she has considerable expertise in this field. It is a difficult balance to strike, ensuring that we are protecting landowner rights while making sure we are giving telecoms operators the powers they need to make sure all of our constituents have the digital connectivity that they demand—and will increasingly need—going forward.

For the reasons I have set out and will be setting out in further detail, I do not think the amendments will have the desired effect. It was interesting to hear the oral evidence this week, because there was no consensus among the telecoms operators about what powers are required. We have to ensure that we do not give commercial advantage to one player or the other, as that would also trample over some landowner rights.

The changes made in the 2017 reforms permit upgrading and sharing to take place without a landowner's specific consent only where any impacts on that individual will be limited. However, it was recognised that any use of those rights could have some impact—albeit a very limited one—on individual landowners. The new rights were not applied retrospectively and had no effect on landowners who had entered into agreements before the legislation was passed. The key difference is that agreements made after that date would be completed in the knowledge

that the upgrading and sharing rights would apply. Since the 2017 reforms, however, the public need for robust and up-to-date digital services has continued to grow, and was thrown into sharp relief by the recent pandemic, when many of us were reliant on access to those services at unprecedented levels.

Upgrading and sharing apparatus has a more important role to play than ever before. In the light of this and other market developments, we have revisited the position on upgrading and sharing where the rights introduced by the 2017 reforms do not apply. Introducing specific upgrading and sharing rights for such equipment can play an important role in improving coverage and capacity, and amendment 9 appears to agree with that conclusion. However, we need to ensure that the rights of individual landowners are adequately protected. As I said, agreements after the 2017 reforms will have been concluded in the knowledge that they will give rise to automatic rights for apparatus to be upgraded or shared. That is not true of apparatus that is not covered by an agreement concluded after the 2017 reforms. As such, it is only right that any automatic rights to upgrade and share those types of apparatus should be subject to different conditions.

The amendments suggest introducing specific conditions for retrospective upgrading and sharing rights where private landlords are concerned, and those conditions partly reflect those contained in the rights established by the 2017 reforms and those set out in the Bill. However, the conditions in the new rights that we are proposing have been carefully developed to work as a whole; they are intentionally more restrictive and give rise to more limited rights than those available for agreements reached before the 2017 reforms. Taken together, the conditions mean that the operator will have automatic rights only to carry out upgrading and sharing activity that will have no adverse impact on the land or that will put no burden on a relevant individual, but this will still allow activities, such as crucial upgrading work, to be undertaken in relation to historical copper cables installed underneath land.

Sally-Ann Hart (Hastings and Rye) (Con): I wonder if the Minister could provide some clarity. Underneath the ground, there are ducts that operators can run cables through. We heard in this week's evidence session about telegraph poles. Operators can go to the bottom of the telegraph pole, but will the Minister provide some welcome clarity on whether they can go up to the top and across? It is really important that they can use existing infrastructure and not have to pay to go around because they cannot use the overhead.

Julia Lopez: We are looking at rights that will provide easier access to underground and over, but not on. These are very techy points. If my hon. Friend feels that that does not answer her question precisely enough, I would be happy to ask officials to get in touch with her.

The measures in the Bill as drafted ensure that apparatus installed under agreements concluded prior to 2017 can be upgraded and shared quickly and cost-effectively. At the same time, the specific conditions that we are introducing will ensure that the right balance is maintained between the interests of private individuals and the wider public benefit, which is a difficult balance to strike. We are concerned that the amendments would not maintain that balance. I hope that gives the hon. Member for Ogmore assurance that the provisions in the Bill regarding retrospective rights to upgrade and share represent a balanced approach, and I ask him to withdraw his amendment.

Clauses 59 and 60 are vital clauses that support and encourage greater upgrading and sharing of existing apparatus. The 2017 code reforms provided operators with limited automatic rights to upgrade and share their apparatus, subject to certain conditions. However, the 2017 changes did not introduce paragraph 17 upgrading and sharing rights for subsisting agreements, which are agreements completed before the 2017 reforms came into force. This means that a significant proportion of the UK's existing networks cannot be upgraded or shared without specific permission, despite the fact that apparatus can be upgraded and shared in many situations with no adverse impacts on any individual or private land.

Clause 59 therefore inserts new paragraph 5A into schedule 2 to the Digital Economy Act 2017 in order to introduce rights for operators to upgrade and share apparatus installed under a subsisting agreement. These rights differ from those contained in paragraph 17. They are available in more limited circumstances and will be subject to stricter conditions and specific notice requirements. Taken together, the measures in the clause will ensure that apparatus installed under a subsisting agreement can be upgraded and shared quickly and cost-efficiently, and do so in a way that takes into account both the interests of individuals and the wider public benefit.

Clause 60 deals with the same issue of upgrading and sharing apparatus, but in this case in relation to apparatus installed before 29 December 2003 where there is neither a subsisting agreement nor an agreement concluded after the 2017 reforms. It is right that upgrading and sharing rights should be available for all apparatus installed before the 2017 reforms came into effect. Clause 60 therefore inserts proposed new paragraph 17A into the code, conferring rights to upgrade and share apparatus installed under land before 29 December 2003, where the operator who owns that apparatus is not a party to an agreement under part 2 of the code.

Kevin Brennan: I have listened carefully to the Minister and I do not agree with the Government's position on rejecting the amendment. She is right that large swathes of the Bill are about the difficult balancing act between private property rights and the public interest. It seems to me, in the case put forward by my hon. Friend the Member for Ogmore in support of the group of amendments, that this is an instance where the public interest is overwhelmingly clear, while the private property interest that the Minister defended in her response is not.

My hon. Friend put forward the problem that has been received by the Committee in evidence, which is that many blocks of flats are not updated with their internet connections and so on. There is a huge public policy interest in the digital divide, which we all know about across the country, and in ensuring that the people who live in those kinds of premises have excellent access—as good as someone living with the best infrastructure available in an urban setting. He mentioned the rural-urban divide, but I am talking specifically about the case he made about blocks of flats.

I think what the Minister was saying was that because what is being proposed represents a retrospective change, a higher standard should apply to protecting those

[Kevin Brennan]

private property interests than would apply in the case, for example, of equipment that was installed post 2017. That, however, does not make a jot of difference to a poor child living in a block of flats who does not have good internet access to do their homework. That is a pretty clear judgment for the Government to make, because they have made no real or clear case that any compelling property rights are being imperilled, or that there is any compelling cost—other than minor inconvenience, perhaps—to the landowners who might be affected by the amendment.

There is, however, an overwhelming public policy case for wanting to do everything possible to assist children living in such block of flats. There is an overwhelming public policy case that a child in that block of flats with pre-2017 infrastructure should not be treated any less equally or favourably than a child who lives in a neighbouring block of flats that happens to have equipment that was installed post 2017. I urge the Minister and the Government to rethink their position for those reasons, unless I have misunderstood their case.

Julia Lopez: I reassure the hon. Gentleman that we do not disagree with the ambition. We all want children in such blocks of flats and other difficult-to-reach premises to have excellent digital infrastructure. As the Member for an urban constituency, I certainly want that. We have been testing this extensively, from legal team to legal team of operators. Some operators tell us that the additional rights are not necessary to be able to access buildings in the way that they hope; others say that they are. As I say, we have been testing this. Some of the suggestions would give greater legal access to property than law enforcement has. We have to get the right balance and we have to test whether this proposal will ultimately speed up the roll-out.

Kevin Brennan: That seems to be rather a weak argument. If law enforcement were entering someone's property, it would probably be to search it, make an arrest or something like that. A telecoms operator entering a property to install some cable is a very different proposition, is it not?

Julia Lopez: It is a difficult balance to get right, between having a roll-out and ensuring that somebody's property rights are respected. If we are considering giving greater powers to an operator than to law enforcement, we have to ask whether that is necessary. Operators have told us that that is not necessary to get access and to increase roll-out. On balance, therefore, we are not minded to support the amendment.

12.45 pm

Chris Elmore: I have listened to the Minister and the debate that followed her speech. The argument is slightly confused, because in the oral evidence sessions, CityFibre and Openreach were in agreement on the need to address the issue. They were also in agreement on the huge deficit in meeting the Government's targets because of issues in gaining access to flats and properties through leaseholders and site owners.

In answer to the question about the response of tenants or property owners inside the flats, the providers said that it was overwhelmingly positive; they wanted to gain fibre roll-out. As I mentioned in my opening remarks, nearly 56,000 MDU premises are on hold through the roll-out, so what is the plan? What is the solution to deal with the digital divide that is forming in cities and towns across the UK? It was mentioned in evidence that my Ogmore constituency has only 3% MDUs. If I recall correctly, the hon. Member for Hastings and Rye's constituency was above 13% or 14%—higher again, she is indicating. The numbers increase depending on the area. How will we solve that problem?

Equally, I agree with my hon. Friend the Member for Cardiff West. We cannot simply say that, as we move to more online learning, and more remote working or working from home—business is supportive of that following the pandemic, even if the Government are asking everyone to come back to the office—people now have far greater understanding of their broadband, including its bandwidth, who installed it, who runs it and the costs, than they ever did before the pandemic because everyone needed to use Zoom and Teams; although, personally, there are days when I would rather not use them ever again.

I am minded to press the amendment to a Division, for the reasons that I and my hon. Friend set out. I am not hearing from the Minister what the plan is to rectify the problem. According to Openreach and other providers, the figure for premises on hold is going up year after year, and therefore the target will be missed, despite the Government reducing it at least twice since 2019.

Question put, That the amendment be made.

The Committee divided: Ayes 4, Noes 7.

Division No. 2]

AYES

Brennan, Kevin	Mishra, Navendu
Elmore, Chris	Osborne, Kate

NOES

Baynes, Simon	Lopez, Julia
Double, Steve	Randall, Tom
Edwards, Ruth	
Grundy, James	Vara, Shailesh

Question accordingly negatived.

Amendment proposed: 10, in clause 59, page 43, line 26, at end insert—

"5B Paragraph 17 of the new code (power for operator to upgrade or share apparatus) applies in relation to an operator who is a party to a subsisting agreement with a private landlord, but as if for sub-paragraphs (1) to (6) there were substituted—

"(1) This paragraph applies where—

(a) an operator ("the main operator") keeps electronic communications apparatus installed on, under or over land, and

(b) the main operator is a party to a subsisting agreement in relation to the electronic communications apparatus.

(2) If the conditions in sub-paragraphs (3), (4) and (6) are met, the main operator may—

(a) upgrade the electronic communications apparatus, or

(b) share the use of the electronic communications apparatus with another operator.

(3) The first condition is that any changes as a result of the upgrading or sharing to the electronic communications apparatus to which the agreement relates have no adverse impact, or no more than a minimal adverse impact, on its appearance.

(4) The second condition is that the upgrading or sharing imposes no additional burden on the other party to the agreement.

(5) For the purposes of sub-paragraph (4) a burden includes anything that—

(a) has an adverse effect on the person's enjoyment of the land, or

(b) causes loss, damage or expense to the person.

(6) The third condition is that, before the beginning of the period of 21 days ending with the day on which the main operator begins to upgrade the electronic communications apparatus or (as the case may be) share its use, the main operator attaches a notice, in a secure and durable manner, to a conspicuous object on the relevant land.

(7) A notice attached for the purposes of sub-paragraph (6) must—be attached in a position where it is reasonably legible,

(a) be attached in a position where it is reasonably legible,

(b) state that the main operator intends to upgrade the electronic communications apparatus or (as the case may be) share its use with another operator,

(c) state the date on which the main operator intends to begin to upgrade the electronic communications apparatus or (as the case may be) share its use with another operator,

(d) state, in a case where the main operator intends to share the use of the electronic communications apparatus with another operator, the name of the other operator, and

(e) give the name of the main operator and an address in the United Kingdom at which the main operator may be contacted about the upgrading or sharing.

(8) Any person giving a notice at that address in respect of that electronic communications apparatus is to be treated as having been given that address for the purposes of paragraph 91(2).

(9) Any agreement under Part 2 of this code is void to the extent that—

(a) it prevents or limits the upgrading or sharing, in a case where the conditions mentioned in sub-paragraphs (3), (4) and (6) are met, of any electronic communications apparatus to which the agreement relates that is installed on, over or under land, or

(b) it makes upgrading or sharing of such electronic communications apparatus subject to conditions to be met by the operator (including a condition requiring the payment of money).

(10) Nothing in this paragraph is to be read as conferring a right on the main operator to enter the land which the main operator would not otherwise have, when upgrading or sharing the use of the electronic communications apparatus.

(11) References in this paragraph to sharing electronic communications apparatus include carrying out works to the electronic communications apparatus to enable such sharing to take place.

(12) In this paragraph—

"the relevant land" means—

(a) in a case where the main operator has a right to enter the land, that land;

(b) in any other case, the land on which works will be carried out to enable the upgrading or sharing to take place or, where there is more than one set of works, the land on which each set of works will be carried out;

"subsisting agreement" has the meaning given by paragraph 1(4) of Schedule 2 to the Digital Economy Act 2017.""—*(Chris Elmore.)*

This amendment, together with Amendments 9, 11 and 12, would apply a different regime under the Electronic Communications Code to private landlords, giving automatic upgrade rights for operators to properties owned by private landlords subject to the condition that the upgrading imposes no additional burden on the other party to the agreement.

Question put, That the amendment be made.

The Committee divided: Ayes 4, Noes 7.

Division No. 3]

AYES

Brennan, Kevin	Mishra, Navendu
Elmore, Chris	Osborne, Kate

NOES

Baynes, Simon	Lopez, Julia
Double, Steve	Randall, Tom
Edwards, Ruth	
Grundy, James	Vara, Shailesh

Question accordingly negatived.

Clause 59 ordered to stand part of the Bill.

Clause 60

UPGRADING AND SHARING OF APPARATUS INSTALLED BEFORE 29 DECEMBER 2003

Amendment proposed: 11, in clause 60, page 43, line 38, after "land" insert

"not owned by a private landlord".—*(Chris Elmore.)*

This amendment, together with Amendments 9, 10 and 12, would apply a different regime under the Electronic Communications Code to private landlords, giving automatic upgrade rights for operators to properties owned by private landlords subject to the condition that the upgrading imposes no additional burden on the other party to the agreement.

Question put, That the amendment be made.

The Committee divided: Ayes 4, Noes 7.

Division No. 4]

AYES

Brennan, Kevin	Mishra, Navendu
Elmore, Chris	Osborne, Kate

NOES

Baynes, Simon	Lopez, Julia
Double, Steve	Randall, Tom
Edwards, Ruth	
Grundy, James	Vara, Shailesh

Question accordingly negatived.

Amendment proposed: 12, in clause 60, page 44, line 47, at end insert—

"17B (1) This paragraph applies where—

(a) an operator ("the main operator") keeps electronic communications apparatus installed on, under or over land owned by a private landlord,

(b) the main operator is not a party to an agreement under Part 2 of this code in relation to the electronic communications apparatus, and

(c) the electronic communications apparatus was installed before 29 December 2003.

(2) If the conditions in sub-paragraphs (3), (4) and (6) are met, the main operator may—

(a) upgrade the electronic communications apparatus, or

(b) share the use of the electronic communications apparatus with another operator.

(3) The first condition is that any changes as a result of the upgrading or sharing to the electronic communications apparatus to which any existing agreement between the operator and the landlord relates have no adverse impact, or no more than a minimal adverse impact, on its appearance.

(4) The second condition is that the upgrading or sharing imposes no additional burden on the landlord.

(5) For the purposes of sub-paragraph (4) a burden includes anything that—

(a) has an adverse effect on the person's enjoyment of the land, or

(b) causes loss, damage or expense to the person.

(6) The third condition is that, before the beginning of the period of 21 days ending with the day on which the main operator begins to upgrade the electronic communications apparatus or (as the case may be) share its use, the main operator attaches a notice, in a secure and durable manner, to a conspicuous object on the relevant land.

(7) A notice attached for the purposes of sub-paragraph (6) must—

(a) be attached in a position where it is reasonably legible,

(b) state that the main operator intends to upgrade the electronic communications apparatus or (as the case may be) share its use with another operator,

(c) state the date on which the main operator intends to begin to upgrade the electronic communications apparatus or (as the case may be) share its use with another operator,

(d) state, in a case where the main operator intends to share the use of the electronic communications apparatus with another operator, the name of the other operator, and

(e) give the name of the main operator and an address in the United Kingdom at which the main operator may be contacted about the upgrading or sharing.

(8) Any person giving a notice at that address in respect of that electronic communications apparatus is to be treated as having been given that address for the purposes of paragraph 91(2).

(9) Nothing in this paragraph is to be read as conferring a right on the main operator to enter the land which the main operator would not otherwise have, when upgrading or sharing the use of the electronic communications apparatus.

(10) References in this paragraph to sharing electronic communications apparatus include carrying out works to the electronic communications apparatus to enable such sharing to take place.

(11) In this paragraph "the relevant land" means—

(a) in a case where the main operator has a right to enter the land, that land;

(b) in any other case, the land on which works will be carried out to enable the upgrading or sharing to take place or, where there is more than one set of works, the land on which each set of works will be carried out."—*(Chris Elmore.)*

This amendment, together with Amendments 9, 10 and 11, would apply a different regime under the Electronic Communications Code to private landlords, giving automatic upgrade rights for operators to properties owned by private landlords subject to the condition that the upgrading imposes no additional burden on the other party to the agreement.

Question put, That the amendment be made.

The Committee divided: Ayes 4, Noes 7.

Division No. 5]

AYES

Brennan, Kevin	Mishra, Navendu
Elmore, Chris	Osborne, Kate

NOES

Baynes, Simon	Lopez, Julia
Double, Steve	Randall, Tom
Edwards, Ruth	
Grundy, James	Vara, Shailesh

Question accordingly negatived.

Clause 60 ordered to stand part of the Bill.

Ordered, That further consideration be now adjourned. —*(Steve Double.)*

12.55 pm

Adjourned till this day at Two o'clock.

PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

PRODUCT SECURITY AND TELECOMMUNICATIONS INFRASTRUCTURE BILL

Fourth Sitting

Thursday 17 March 2022

(Afternoon)

CONTENTS

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

not later than

Monday 21 March 2022

The Committee consisted of the following Members:

Chairs: Caroline Nokes, † Graham Stringer

† Baynes, Simon *(Clwyd South)* (Con)
Bhatti, Saqib *(Meriden)* (Con)
† Brennan, Kevin *(Cardiff West)* (Lab)
† Double, Steve *(St Austell and Newquay)* (Con)
† Edwards, Ruth *(Rushcliffe)* (Con)
† Elmore, Chris *(Ogmore)* (Lab)
Grundy, James *(Leigh)* (Con)
† Hart, Sally-Ann *(Hastings and Rye)* (Con)
Hollern, Kate *(Blackburn)* (Lab)
Long Bailey, Rebecca *(Salford and Eccles)* (Lab)
† Lopez, Julia *(Minister for Media, Data and Digital Infrastructure)*
† Mishra, Navendu *(Stockport)* (Lab)
† Osborne, Kate *(Jarrow)* (Lab)
† Randall, Tom *(Gedling)* (Con)
† Vara, Shailesh *(North West Cambridgeshire)* (Con)
Warburton, David *(Somerton and Frome)* (Con)
Whitley, Mick *(Birkenhead)* (Lab)

Huw Yardley, Bethan Harding, *Committee Clerks*

† attended the Committee

Public Bill Committee

Thursday 17 March 2022

(Afternoon)

[Graham Stringer *in the Chair*]

Product Security and Telecommunications Infrastructure Bill

Clause 61

Rent under tenancies conferring code rights: England and Wales

2 pm

Chris Elmore (Ogmore) (Lab): I beg to move amendment 8, in clause 61, page 45, line 37, at end insert—

"(4A) Where the assumptions in subsection (4) cause the market value of a landlord's agreement to decline, the rent payable under a new tenancy granted by order of the court under this Part of this Act shall not decline by more than 40%."

This amendment would provide a legal guarantee that site providers' rents fall by no more than 40% under any new agreement.

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

Clause stand part.

Clauses 62 to 65 stand part.

Chris Elmore: The Government introduced the electronic communications code in 2017 and promised at the time that reductions in rent would, in reality, be no more than 40%. However, as we heard from Protect and Connect during Tuesday's evidence session, there have been thousands of cases in which small tenant farmers, sports clubs and community organisations that host masts have seen their rents fall by vastly more than that, with many facing reductions of more than 90%. That was confirmed during the evidence session, when a question was asked about the average, followed by questions from other Members, including me. That clearly showed that there had been far higher reductions for some organisations and owners. One such case is James, a 71-year-old sheep farmer who has maintained a mast on his farm for 15 years, normally receiving £2,900 a year in rent. In 2020, James received a letter informing him that he was now being offered £200 a year under a new agreement. That was a reduction of 93% and a huge overnight shock to his personal and professional finances.

The average reduction for contracts negotiated by Cellnex UK, as Mark Bartlett informed us on Tuesday, has been 63%—a decrease that would cause a huge dent in the finances of all the kinds of organisation I have referred to and a figure well above what the Government promised in 2017. I am sure that members of this Committee would not be best pleased if a significant stream of their income fell by 63%.

I know that the Minister said at Second Reading that valuations pre 2017 were much too high, but surely she must recognise, after the oral evidence we heard on Tuesday, that the race to the bottom that we are seeing is not sustainable and that the level of reduction in rent that is occurring will deter other landowners from agreeing to host infrastructure in the first place, thus slowing the roll-out that this very legislation is designed to speed up.

Rather than leaving reductions to chance, the Opposition have tabled amendment 8, which would enshrine in law that rents under any new agreement fall by no more than 40%. That would strike a much fairer balance between operators and site providers by ensuring that what is a significant income stream for many individuals and community groups is not wiped out overnight. It would also contribute significantly to a faster roll-out of telecommunications infrastructure, as site owners would be more willing to engage. Speeding up the roll-out of new telecommunications infrastructure is the express desire of the Bill. I hope that Members from across the Committee will stand squarely behind their constituents by supporting this amendment.

Kevin Brennan (Cardiff West) (Lab): I rise briefly to support my hon. Friend in pushing the amendment, in order to hear what the Minister has to say in response. The amendment goes to the heart of what a lot of the Bill is about: balancing the rights of private property owners and the policy requirement to speed up the roll-out of digital infrastructure.

This morning we debated an instance in which there would be no real financial cost to the private property owners from doing the right thing. In that instance, the state was ensuring that their properties could be accessed to put in the necessary infrastructure to roll out digital infrastructure in an urban setting—big blocks of flats, where lots of people might not have very good access to the internet and so on. In that instance, the Government were not prepared to accept our amendment, even though it would not have had any significant detrimental impact on the private property owners. In other words, they took the view that in that instance the private property owners, even if they would be only marginally inconvenienced, had to have their property rights protected, because this was a retrospective imposition and they would not have given permission.

In this instance—in fairness, I think this was not intended in 2017—private property owners have suffered, or might suffer, significant detriment to the income they can acquire through somebody else's use of their land with the state's assistance. In those circumstances, it is not unreasonable to say that the balance should be to ensure that they are not affected in a way that causes a massive reduction in the income they can earn from the use of their land.

If that was not a strong enough argument in itself, which perhaps it is not, the way the market has reacted to what happened after 2017 and the problems that there have undoubtedly been, with people reluctant to get involved with rolling out the infrastructure we need for the future, which we all want to achieve through the Bill and by other means, is further evidence that an adjustment perhaps needs to be made. The Minister could discuss with the Committee whether that adjustment is exactly what is contained in the amendment, but whether something should be done to address the arguments

and concerns that have been expressed to us by those who own land on which such infrastructure is sited is certainly worth further consideration.

The Minister for Media, Data and Digital Infrastructure (Julia Lopez): I thank the hon. Members for Ogmore and for Cardiff West for their contributions and for the amendment. I acknowledge that this is a tricky issue. There have been problems between both parties since the 2017 reforms, but we maintain that the 2017 valuation provisions created the right balance between the public need for digital communications and landowner rights. I think there is agreement that the prices being paid for rights to install communications apparatus before that date were simply too high. With digital communications becoming an increasingly critical part of our daily lives, that needed to be addressed.

The new pricing regime is more closely aligned to those for utilities such as water, electricity and gas. We think that that is the correct position. As I said earlier today, we are not seeking to take sides. We are on the side of good digital connectivity for our constituents, and we firmly believe that landowners should still receive fair payments that, among other things, take into account any alternative uses that the land may have and any losses or damages that may be incurred. I was alive to the concerns expressed to me by the Protect and Connect campaign, but also to those raised by individual Members about tricky constituency cases. When I came into my role in September, I met individual Members to discuss those cases. I also met Protect and Connect.

I tested the cases that were brought to my attention and asked for further details, which often were not forthcoming. There was a catch-all excuse that a lot of them were under non-disclosure agreements and the precise amount of rents settled at could not be disclosed. My broad view is that there were initial concerns and difficult cases where the mobile network operators were too aggressive in their negotiations—I think that was effectively acknowledged in the panel discussions earlier in the week—but we seem to have found an equilibrium now, helped partly by some of the cases that have gone through the courts.

We now have a body of case law that can be referred to in some of these tricky negotiations. We are also trying to deter people from going to the courts in the first place, by introducing more alternative dispute resolution mechanisms. I say that to reassure Members. There were problems initially. As far as I can tell from my case load, the correspondence coming in, the discussions that I have had with Members and the lack of additional noise on the subject in the Chamber, a better equilibrium has now been found between the mobile network operators and the landowners. If that is not the case, I am happy to look at those cases again, and we are introducing mechanisms to provide better negotiations between parties via the legislation.

Turning to the amendment, I am not sure why the hon. Member for Ogmore thinks that a specific limit should be imposed on the percentage by which rent can be reduced when the rental payment is determined by a court. Further, it is unclear why he has chosen arbitrarily to apply a figure of 40%. We have strongly resisted specifically regulating the amount of rent payable under a code agreement. Our preference has been to allow the parties to freely negotiate the amount payable under an agreement, based on a statutory framework either in the code, the Landlord and Tenant Act 1954 or the Business Tenancies (Northern Ireland) Order 1996. Even where the parties cannot reach an agreement and the court has to impose its terms, including the rent to be paid, the court has the freedom to reach its own conclusions using that framework, rather than having its discretion restricted by statutory rent controls. As I said, my understanding is that we now have a much better equilibrium, in that we have amounts of rent that both parties are much more content with.

I understand the concerns about whether this has stymied roll-out. If operators cannot get their infrastructure on to land, I imagine that they would start paying more to try to incentivise landowners to take it on. I think we have also seen cases where it has been in the landowner's interests to try to drag the process out so that they are on the old rents, rather than the reduced, new rents. I think that has also contributed to some of the delays.

If the amount of rent is controlled in the way suggested in this amendment, we will be heading closer to a regime that will apply reductions on a blanket basis, rather than take into account the broader range of relevant circumstances, as permitted by the legal framework. I suspect that that is something that both site providers and operators would be keen to avoid.

I am aware that it has been alleged that the Government expected rents to fall by in the region of 40% following the 2017 reforms. It is unclear whether it is on that basis that the hon. Member for Ogmore chose the statutory cap of 40% in his amendment. At the time of the 2017 reforms, which I confess predate me, the fact is that the Government were unsure what the level of rent reductions would be. We were clear that that was the case. Independent analysis contained in the impact assessment that accompanied those reforms predicted that reductions could be 40%, but that was never a Government prediction nor a target.

Chris Elmore: I did say in my opening remarks where the 40% comes from. Just to help the Minister, it does relate to the 2017 change, but also the Government's own analysis from the time. I do of course accept that she was not the Minister, but her party was in government, and those are her own Government's figures.

Julia Lopez: That certainly is a fair point to make, and I apologise for not picking that up in the hon. Member's comments.

A cap is likely to be even more detrimental to constituents in rural communities, who will benefit from the increased connectivity and reliability that we hope the Bill will bring.

As I have explained, agreements to which the code applies can currently be renewed in various ways, depending on the type of agreement and where in the UK it was entered into. The intention of clause 61, along with clause 62, is to create a clearer and more consistent legislative framework under which agreements are renewed. Central to that is ensuring that, no matter where in the UK an agreement is renewed, the financial terms are calculated in the same way. That will help to ensure that there is not a digital divide across the UK, with one country receiving additional investment at the expense of others because operating costs are cheaper.

[Julia Lopez]

The amendment suggests limiting any reduction in rent that may be imposed by the court when agreements are renewed under the 1954 Act. While that proposal is well intentioned, we do not believe that it should be allowed to proceed. It is vital that there is fairness throughout the UK. The Bill as drafted provides a clear framework, which will not only result in all payments being calculated in the same way, but in the ability to renew agreements quickly and cost-effectively. We think that will expand the digital network.

Kevin Brennan: I take what the Minister said about the figure of 40%, but it was contained, as my hon. Friend the Member for Ogmore said, in a previous Government's impact assessment. I remind her that, when Ministers issue impact assessments, they sign them, as she did with this one, saying:

"I have read the Impact Assessment and I am satisfied that, given the available evidence, it represents a reasonable view of the likely costs, benefits and impact of the leading options."

When her predecessor signed the impact assessment on behalf of the Government to say, "This is the Government's official view of what is likely to happen," their official view was that rents would drop, probably by 40%.

Julia Lopez: I accept the point that the hon. Gentleman is making. I also accept that in some cases rent reductions were much greater than expected. As we discussed earlier in the week, some of those were the result of overly aggressive behaviour by mobile network operators. We need to address some of the challenges that were raised by some of the changes that were made. In the body of case law, we now have a better equilibrium between landowners and operators, which should help to address some of those cases.

On some of the more emotive cases that have been raised with me over my tenure, I have sought to understand the details. Those cases are not always as has been presented, and I am led to believe that, in terms of a lot of the initially very difficult cases that came after the 2017 reforms were initially introduced, we are now in a very different place.

It is vital that there is fairness throughout the UK. As drafted, the Bill provides a clear framework that will not only result in all rental payments being calculated in the same way, but in the ability to renew agreements quickly and cost-effectively. We hope that will help us expand the digital network across the whole of our country. In those circumstances, I ask the hon. Member for Ogmore to withdraw his amendment.

I will now turn to clauses 61 to 65, which deal with the renewal of agreements to which the code applies that have expired or are about to expire. There are several ways in which such agreements can be renewed, depending on the type of agreement and where in the UK it was entered into. The aim of the clauses is to make all the routes to renewal as clear and consistent as possible, so that the process is the same across the UK.

2.15 pm

When agreements to which the code applies come to an end, it is important that there is a clear legislative framework in which their renewal can be negotiated and any disagreements dealt with. Making sure that renewal can be completed quickly and consistently not only provides certainty for all parties, but may deliver real benefits for consumers. Renewing such agreements ensures that operators can optimise their use of existing sites to provide greater network capacity and increase access to 5G services.

In England and Wales, there are two statutory routes to renewing the agreements. The first is in part 5 of the code and applies, for example, to most new agreements entered into since the code came into force on 28 December 2017; the other is set out in part II of the Landlord and Tenant Act 1954. Clause 61 applies specifically to agreements that are to be renewed under the second statutory route—that is, under part II of the 1954 Act.

Importantly, the two statutory routes contain different provisions relating to the financial terms of any renewal agreement imposed by a court. Under part 5 of the code, the amount that an operator is required to pay for rights to use private land is calculated on a no-network basis and the fact that the land will be used to host telecoms apparatus cannot be taken into account in assessing the amount to be paid by the operator. In effect, telecoms operators cannot be charged more than anyone else wishing to use the land would be. We think that that is the correct approach and should apply to all agreements to which the code applies.

That valuation framework is not currently available under the 1954 Act, so the no-network assumption does not apply and operators renewing agreements under that statutory route may be required to pay more than they would had part 5 of the code applied. We think the different outcomes are unfair, so the provisions in clause 61 extend the statutory valuation framework in the code to renewal of agreements under part II of the 1954 Act. We think that will result in fairer outcomes and ensure that the financial terms of all agreements to which the code applies that are completed or renewed after the Bill comes into force reflect the same valuation principles.

Clause 62 makes equivalent provision for agreements in Northern Ireland that were entered into before 28 December 2017 and are to be renewed under the Business Tenancies (Northern Ireland) Order 1996, not under part 5 of the code. That will ensure that the same valuation principles underpin the renewal of all agreements to which the code applies across the UK.

The statutory valuation regimes under the 1954 Act and the 1996 order deal solely with the assessment of the rent or the price that an operator is required to pay to keep its apparatus on the land. That is not the only sum a landowner can claim where an agreement is instead renewed under the code, as the code also makes provision for a landowner to recover compensation for any loss or damage that may result from the code agreement. This ensures that landowners are not left out of pocket and can recoup the costs they incur as a result of having telecoms apparatus on their land. There is no equivalent right to compensation in either the 1954 Act or the 1996 order. Clauses 63 and 64 therefore extend the rights of landowners to claim compensation under those provisions.

I hope the Committee will agree to these clauses standing part of the Bill.

Chris Elmore: I listened to the Minister's remarks, and she acknowledges some of the historical cases, but I refer her to this Committee's first sitting, where I asked Eleanor Griggs of the National Farmers Union about reductions in recent cases. Ms Griggs said that in in recent times, the NFU had made representations in cases in which farmers had received 90% decreases. Later, she referred to a farm in the constituency of the hon. Member for St Austell and Newquay where there was a significant reduction, from £3,500 to £17.50 a year.

We have to acknowledge the impact on many organisations, including farmers, churches, and particularly community groups. I have examples in my constituency of community groups that run scout halls or guide huts losing 60%, 70%, 80% or 90% of the income they use to balance their budgets and ensure that they can run services for children and young people throughout the year. The Minister has committed to review even more of the cases that come through for her personal intervention, but I think there should be a minimum threshold of 40%, which the Government committed to previously in their impact assessment, as my hon. Friend the Member for Cardiff West pointed out. I am therefore not minded to withdraw the amendment. I also hope that their lordships will consider it as part of any future scrutiny in the other place.

Question put, That the amendment be made.

The Committee divided: Ayes 4, Noes 7.

Division No. 6]

AYES

Brennan, Kevin	Mishra, Navendu
Elmore, Chris	Osborne, Kate

NOES

Baynes, Simon	Lopez, Julia
Double, Steve	Randall, Tom
Edwards, Ruth	
Hart, Sally-Ann	Vara, Shailesh

Question accordingly negatived.

Clause 61 ordered to stand part of the Bill.

Clauses 62 to 65 ordered to stand part of the Bill.

Clause 66

UNRESPONSIVE OCCUPIERS

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

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

Government amendments 2 to 4.

That the schedule be the schedule to the Bill.

Julia Lopez: I am afraid I have to tell the Committee that this does not get any more inspiring.

The clause creates a bespoke process for telecoms operators to seek access to certain types of land where a person repeatedly fails to respond to requests for access to install apparatus under or over land for the purposes of providing an electronic communications service. The clause sets out that process by inserting into the electronic communications code new part 4ZA, which makes provision for a court to impose an agreement where the operator needs that person, "the landowner", to confer or be bound by code rights. Part 4ZA will apply in situations where an operator intends to provide an electronic communications service and to achieve that must install electronic communications apparatus under or over, but not on, relevant land. "Relevant land" is defined as land that is not covered by buildings, and that is neither a garden, a park nor a recreational area. The provision also takes a power for the Secretary of State to specify through regulations further types of land that may be "relevant land", but may only do so following consultation.

The provisions will require an operator to have given two warning notices, followed by a final notice. Those three notices all follow an initial request notice, giving a total of four. The Bill sets out that there must be a period of 14 days between the giving of each notice. For the landowner to fall out of scope of proposed new part 4ZA, all that is required of them is to respond to any of these notices in writing, before the operator applies to the court under part 4ZA. If any response is received, the operator will no longer be able to apply for a part 4ZA order and must either negotiate for a code agreement or apply for rights to be imposed by the courts in the normal way.

If granted, a part 4ZA order will impose an agreement between a landowner and an operator, conferring the rights requested in the initial notice. The terms of that agreement are to be specified in regulations. It may reassure the Committee that those regulations will be subject to the affirmative procedure. Furthermore, before the regulations are made, the Bill expressly obliges the Secretary of State to consult with a range of parties.

Importantly, the provisions impose a six-year maximum time limit on the period for which rights conferred under a part 4ZA order may last. I emphasise that detail, because it forms an important part of the Bill's safeguards for landowners' property rights. This clause provides a much needed process that will play a large part in ensuring that homes and businesses benefit from the national gigabit broadband upgrade and are not left behind.

I will now turn to the amendments tabled in relation to clause 66, all of which are technical amendments. Amendments 2 and 3 have been tabled in order to make a minor clarification to the text of the electronic communications code, to avoid any possible unintended interpretation of the legislation. Amendments 2 and 3 clarify that the right mentioned in paragraph 26(8) and paragraph 27G(4) of the electronic communications code to require the removal of apparatus applies in relation to apparatus placed under or over land. By inserting the words "under or over" into paragraph 26(8) and paragraph 27G(4) of the code, these amendments clarify that part 6 of the code may be used by a landowner to require the operator to remove apparatus installed "under or over", as well as on, the land.

Without amendments 2 and 3, paragraph 26(8) and 27G(4) as currently worded may be interpreted to mean that while equipment installed on land under the "interim rights" or "unresponsive occupier" process could be removed via the part 6 process, equipment

[Julia Lopez]

installed under or over land under these processes might not. That is not the policy intention, and as such this amendment is being introduced to clarify the policy position.

Amendment 4 makes a minor amendment to remove a provision which has been found to have no effect. The provision in question—paragraph 3(9) of the schedule to clause 66 in the Bill—was intended to ensure that part 5 of the code does not apply to the process created by clause 66 in the Bill. Part 5 of the code sets out that code rights may persist even after the agreement which underpins them expires. It was never intended that part 5 should apply to rights gained through part 4ZA, due to the importance of the time limits I have mentioned. The Bill provision that this amendment removes was intended to ensure that part 5 did not apply to rights gained through part 4ZA. However, we are satisfied a different part in the code already ensures this. As such, paragraph 3(9) in the schedule of the Bill has no real effect and ought to be removed.

In practical terms, there is no legal or policy change effected through this amendment, beyond increasing the clarity of legislation. This amendment simply removes a provision which had no effect in the first place, and thus tidies the legislation. I hope that everyone will accept that that is beneficial.

Chris Elmore: I want to make clear the Opposition's support for clause 66. From all my conversations with industry, it is quite clear that where there is an unresponsive landowner, it is extremely complicated to then meet the public's demands. If the Bill is about improving digital activity for all our constituents, particularly in some of the most rural and hard to reach communities—I find it hard to believe that includes my own constituency, but it does—then this is an important and welcome change.

Kevin Brennan: Despite the very thorough explanation that the Minister gave of what is a technical clause, I understand what the difference is between something being placed over or under land, but I am not sure what the difference is between something placed over or on land. There must be a technical reason why it is there; does she know the answer to that?

Julia Lopez: I think it being on land is a much more intrusive process. For instance, we could be talking about a cable that happens to be going over somebody's land, and therefore to do something to it would not require a great deal of intrusion. Similarly, if it was the matter of being able to dig at the side of a road, it is technically access land, but only underneath the surface of the land—I hope this makes sense. It is much less intrusive process. I think it is a process that could be objected to far less by a landowner; they are not being asked if somebody can drive over their land, put something unattractive on it or inconvenience them in any way. We are talking about underground works and cabling works that objectively would have no real impact on their land.

Question put and agreed to.

Clause 66 accordingly ordered to stand part of the Bill.

Schedule

UNRESPONSIVE OCCUPIERS: CONSEQUENTIAL AMENDMENTS

Amendments made: 2, in the schedule, page 66, line 17, at end insert—

"(c) in sub-paragraph (8), after "placed on" insert ", under or over"."

This amendment clarifies that the right mentioned in paragraph 26(8) of the electronic communications code to require the removal of apparatus applies in relation to apparatus placed under or over land.

Amendment 3, in schedule, page 66, line 18, after "sub-paragraph (4)" insert—

"(a) after "placed on" insert ", under or over";

(b) "

This amendment clarifies that the right mentioned in paragraph 27G(4) of the electronic communications code to require the removal of apparatus applies in relation to apparatus placed under or over land.

Amendment 4, in the schedule, page 66, line 20, leave out sub-paragraph (9).—*(Julia Lopez.)*

This amendment removes the amendment to paragraph 30(3) of the electronic communications code. The amendment to paragraph 30(3) is unnecessary because paragraph 30(2) would not in any event apply to a code right conferred by virtue of an order under new paragraph 27ZE of the code.

Schedule, as amended, agreed to.

Clause 67

ARRANGEMENTS PENDING DETERMINATION OF CERTAIN APPLICATIONS UNDER CODE

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

2.30 pm

Julia Lopez: The clause deals with situations where once an agreement to which part 5 of the code applies has run its initially agreed course, one of the parties wants it to be terminated, modified or replaced by an agreement with different terms. In those circumstances, the matter can be referred to a tribunal if the parties cannot resolve matters themselves. It can take time for such disputes to be dealt with, and paragraph 35 of the code deals with the circumstances in which an interim order can be requested, which will apply until the full dispute is heard.

Our policy intention for interim orders is to allow any specific priority aspect of a dispute to be looked at, so that temporary arrangements can be imposed where appropriate. At present, however, paragraph 35 of the code is restricted, so that only a site provider can ask for an interim order, and they can do so only in relation to the consideration paid by an operator. The clause widens that provision so that either party can ask for an interim order and can do so in relation to any term of the former agreement. That will enable specific issues to be dealt with at a much earlier stage of the dispute. In particular, it will mean that operators are given the same opportunity as site providers have to ask for the financial terms of an agreement to be reviewed on an interim basis. This will help ensure that once an agreement to which part 5 of the code applies has run its initially

agreed course, there are no unnecessary delays to the valuation framework of the code being applied to new financial arrangements.

It will also provide the courts with greater flexibility to look at situations where a party needs an urgent change to any term of their agreement. We think that will be particularly helpful where an operator needs urgent changes to terms so that they can upgrade or continue using an existing site. There are likely to be situations where this will also benefit site providers. However, the clause is not to be used as a way of circumventing the usual negotiation process. Parties will be expected to negotiate in the usual way before making an application to the court, and to comply with the ADR requirements that the Bill introduces.

We think the clause will help many operators benefit from the full code framework at a much earlier stage, which will allow them to take advantage of provisions to upgrade and share apparatus and the code valuation framework as introduced in 2017. That will result in more investment in the expansion and upgrading of digital networks, ensuring that consumers receive the best coverage and connectivity possible.

Question put and agreed to.

Clause 67 accordingly ordered to stand part of the Bill.

Clause 68

Use of alternative dispute resolution

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

The Chair: With this it will be convenient to discuss clause 69 stand part.

Julia Lopez: I will now speak to clauses 68 and 69, which introduce measures on alternative dispute resolution and complaints relating to the conduct of operators. The purpose is to encourage more collaborative discussions between landowners and telecoms operators, and to ensure that litigation is used only as a last resort where an agreement cannot be reached.

Clause 68 sets out two new requirements for operators and one new requirement for courts. Together, they will encourage the greater use of alternative dispute resolution processes. The requirements are as follows. First, when a request notice is sent for access to land or other rights under the electronic communications code, all operators must inform the landowner of the availability of ADR processes if the landowner is unhappy with the offer made. Secondly, in cases where an agreement cannot be reached operators must consider using ADR processes before applying to the courts. If the matter relates to modification of an expired agreement, either party must consider ADR before applying to the court. Finally, when awarding costs, the courts will be required to take into account any unreasonable refusal to engage in ADR by either party.

Some landowners and their representatives have told us that they find negotiations for code rights difficult. In some cases, landowners have felt pressured to accept any terms offered, to avoid the risk of being taken to court—this relates to the David and Goliath situation that we discussed earlier in the week. The measures in clause 68 address this issue by encouraging the use of ADR in order to minimise the risk of landowners feeling such pressure, and to facilitate co-operative discussions between landowners and telecoms.

Clause 69 inserts new subsection (ca) into paragraph 103 of the electronic communications code, which lists the issues that Ofcom's code of practice must deal with. Subsection (ca) adds to the list

"the handling by operators of complaints relating to the failure of operators to comply with the code of practice".

Landowners and their representatives have reported to the Government that, in some cases, they are reluctant to enter into code agreements because they are concerned about how the operator or their contractors will behave when they access the relevant land. The clause works to address the issue by requiring Ofcom to prepare guidance, following consultation, regarding operators' handling of conduct. To complement that, we will bring forward secondary legislation to introduce a new statutory requirement for operators to have a complaints process for code matters, enforced by Ofcom.

Question put and agreed to.

Clause 68 accordingly ordered to stand part of the Bill.

Clause 69 ordered to stand part of the Bill.

Clause 70

Power to impose time limits on the determination of code proceedings

Julia Lopez: I beg to move amendment 5, in clause 70, page 60, line 15, at end insert—

", and

(b) amend or repeal any of the following provisions (which provide signposts to those regulations)—

(i) paragraph 2A of Schedule 3 to the New Roads and Street Works Act 1991;

(ii) section 107(1A) of this Act;

(iii) paragraph 97 of Schedule 3A to this Act;

(iv) section 69(5A) of the Marine and Coastal Access Act 2009;

(v) section 27(6A) of the Marine (Scotland) Act 2010.".

This amendment ensures that the power conferred by the new section 119A of the 2003 Act includes power to amend or revoke certain signposts in primary legislation which might otherwise be rendered otiose by the exercise of that power.

The Chair: With this it will be convenient to discuss clause stand part.

Julia Lopez: It is clearly desirable that legal disputes relating to code rights be dealt with as quickly as possible; that will minimise delays to network deployment and expansion in a number of ways.

Fast dispute resolution will make sure that, where the public interest test is satisfied, operators can get the rights they need for network deployment and expansion as soon as possible. It also means that where that test is not satisfied, that is identified promptly, so that operators know they have to explore different options. Finally, fast dispute resolution is in the best interests of all parties. Protracted legal proceedings take time, cost money and harm ongoing stakeholder relationships.

[Julia Lopez]

However, while we recognise that fast dispute resolution has a lot of benefit, it is important that there be no undue interference with the judicial process and the ability of courts to deal with cases justly. Time limits should not, for example, interfere with a court's ability to provide the parties with sufficient opportunities to identify, locate or produce evidence. Any statutory provisions relating to the time within which disputes must be determined therefore require careful consideration and close scrutiny.

Legislation already makes limited provision for certain applications relating to new code rights to be heard within six months, but this provision sits outside the code; it is in the Electronic Communications and Wireless Telegraphy Regulations 2011. It was introduced in the course of our transposing European legislation, rather than as a specific element of the domestic code framework.

The new power in clause 70 will enable the Secretary of State to make regulations that are broader in scope, and can specify a period within which a full range of code-related disputes must be determined. As the clause makes clear, regulations made under it may amend or revoke provisions made under the 2011 regulations. That gives the Secretary of State flexibility to consider a full range of approaches, including having no time-limited period at all, if appropriate.

Other, wider measures that we are introducing in the Bill, and potentially in subsequent secondary legislation, will affect court resources. In many cases, the changes will ensure that caseloads are more evenly distributed, particularly between the first-tier and upper-tier tribunals. Rather than seeking to make changes relating to dispute time limits now, we are therefore putting in clause 70 a power permitting the Secretary of State to make regulations on this issue in future. That will enable the Government to revisit the measures as a whole, once the other measures in the Bill come into force, so that their overall impact can be assessed when considering whether changes are appropriate. We will, of course, work closely with the Ministry of Justice and the Northern Ireland and Scotland Governments before making any further proposals on this issue.

Amendment 5 provides a very limited power for the Secretary of State to amend a specified list of provisions in primary legislation. The provisions signpost to regulations about time limits for disputes on code rights. It is clearly desirable that legal disputes relating to code rights be dealt with very quickly. Any statutory provision relating to the time within which disputes must be determined requires careful consideration. The amendment ensures that, if changes are made to the existing regulations, corresponding amendments can be made to legislation that signposts those regulations.

Chris Elmore: This point also relates to previous clauses, but I think links best to clause 70. The Minister mentioned that the Secretary of State would review dispute resolution at a later date. Throughout the oral evidence sessions, there were calls from the NFU, Protect and Connect and other organisations for the dispute resolution to become compulsory. If resolutions were slowing down, and decisions were not being reached, would the Minister consider introducing, through secondary legislation, a compulsory element, so that we can avoid some of the concerns raised by the witnesses, particularly those representing landowner and club groups and so on?

Julia Lopez: I think it is implicit in what I said that we will keep all of this under close review, because we do not want any of the changes we make to slow the roll-out. We hope that the changes have their intended effect, which is ultimately not about any particular group's interests, beyond their getting better digital connectivity. We are always happy to keep this under close review. We do not think a mandatory ADR would serve our overall goal. If problems come up over the next few years, these powers will enable us to make changes.

Amendment 5 agreed to.

Clause 70, as amended, ordered to stand part of the Bill.

Clause 71

RIGHTS OF NETWORK PROVIDERS IN RELATION TO INFRASTRUCTURE

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

Julia Lopez: Sharing infrastructure in the roll-out of gigabit-capable networks can greatly reduce the cost of deploying networks, increase the pace of roll-out and reduce the frustrating need to dig up streets, preventing unnecessary disruption to the local populations we represent and reducing carbon emissions. The Communications (Access to Infrastructure) Regulations 2016 enable sharing of information about access to physical infrastructure across the utility, transport and communications sectors. They include the right to access that infrastructure on fair and reasonable commercial terms and conditions. The 2016 regulations were implemented in the UK, following the European broadband cost reduction directive, to reduce the cost of deploying high-speed electronic communications networks.

We recently published our response to a call for evidence on a review of those regulations. We set out that there may be areas where the 2016 regulations could be made easier to understand and use. We said we would legislate to allow future changes to the 2016 regulations via secondary legislation, rather than having to rely on primary legislation. This legislation would be subject to a further consultation with Ofcom and such other persons the Secretary of State considers appropriate. It would also be scrutinised in the Parliament through the affirmative procedure.

Clause 71 grants the Secretary of State the power to make provisions, through regulations, conferring rights on network providers in relation to infrastructure for the purpose of developing communications networks. These provisions include the power to amend, revoke or replace the 2016 regulations. The clause details the areas in which provisions may be made by the Secretary of State through regulations. These areas include: provisions relating to grants of access to relevant infrastructure; the carrying out of work as specified; procedures and forms of request by network providers for rights conferred by the regulations; and disputes under the regulations.

Question put and agreed to.

Clause 71 accordingly ordered to stand part of the Bill.

Clause 72

POWER TO MAKE CONSEQUENTIAL AMENDMENTS

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

The Chair: With this it will be convenient to discuss clause 73 stand part.

Julia Lopez: Clause 72 confers on the Secretary of State a power to make any changes to other legislation that are required as a consequence of part 2 of the Bill coming into force. By way of example, changes may be needed to ensure that legislation that references the electronic communications code continues to work correctly after the Bill is passed. The power can be used to amend any legislation. In the case of primary legislation, it is limited to legislation passed or made before the end of the parliamentary Session in which the Bill is passed.

Clause 72 requires that any regulations made using this power that amend or repeal primary legislation be subject to the affirmative procedure. The negative procedure will apply to any other regulations made using this power. Where any changes are required to devolved legislation, the UK Government will work with the devolved Administrations to ensure that the wider legislative framework operates as intended. Clause 73 provides a straightforward explanation regarding references in this Bill to the electronic communications code.

Kevin Brennan: As the clause impacts the devolved Administrations and gives Ministers the right to interfere with primary legislation that is being passed by the devolved Governments, what consultation there has been with the Senedd, Scottish Parliament and Northern Ireland Assembly about this power of the UK Government?

Julia Lopez: We have official-level contact frequently, in case something has to be changed. I would like to reassure the hon. Gentleman that I have met my counterparts in the Scottish and Welsh Administrations, including one of his colleagues in the Labour Administration. I will continue to have those meetings, in case changes that would have any meaningful impact are required as a result of the legislation.

Question put and agreed to.

Clause 72 accordingly ordered to stand part of the Bill.

Clause 73 ordered to stand part of the Bill.

Clause 74

POWER TO MAKE TRANSITIONAL OR SAVING PROVISION

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

2.45 pm

The Chair: With this it will be convenient to discuss clauses 75 to 78 stand part.

Julia Lopez: Clause 74 allows the Secretary of State to make transitional or saving provisions. This is required to provide for a smooth introduction of the new legal framework by, for example, specifying grace periods before the legislation comes into force. Clause 75 makes provision about a number of technical matters that regulations made under the Bill address, and enables such regulations to be exercisable by statutory instrument.

Clause 76 sets out the extent of the provisions of the Bill. Both cyber-security and telecommunications are reserved matters, and, for the most part, the Bill extends across the UK. Clause 77 sets out the commencement. Clause 27, on matters of enforcement, comes into force on Royal Assent, and the remaining clauses come into force via commencement regulations made by the Secretary of State. Clause 78 is the short title of the Bill.

Question put and agreed to.

Clause 74 accordingly ordered to stand part of the Bill.

Clauses 75 to 78 ordered to stand part of the Bill.

Ordered, that further consideration be now adjourned.—*(Steve Double.)*

2.47 pm

Adjourned till Tuesday 22 March at twenty-five minutes past Nine o'clock.

Written evidence reported to the House

PSTIB10 BT Group

PSTIB11 Central Association of Agricultural Valuers (CAAV)

PSTIB12 British Property Federation (BPF)

PSTIB13 Blacks solicitors LLP

PSTIB14 Notcutts Ltd

PSTIB15 Charles Anderson

PSTIB16 Sandra Parkinson

PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

PRODUCT SECURITY AND TELECOMMUNICATIONS INFRASTRUCTURE BILL

Fifth Sitting

Tuesday 22 March 2022

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 26 March 2022

The Committee consisted of the following Members:

Chairs: † Caroline Nokes, Graham Stringer

† Baynes, Simon *(Clwyd South)* (Con)
† Bhatti, Saqib *(Meriden)* (Con)
Brennan, Kevin *(Cardiff West)* (Lab)
† Double, Steve *(St Austell and Newquay)* (Con)
† Edwards, Ruth *(Rushcliffe)* (Con)
† Elmore, Chris *(Ogmore)* (Lab)
† Grundy, James *(Leigh)* (Con)
† Hart, Sally-Ann *(Hastings and Rye)* (Con)
Hollern, Kate *(Blackburn)* (Lab)
† Long Bailey, Rebecca *(Salford and Eccles)* (Lab)
† Lopez, Julia *(Minister for Media, Data and Digital Infrastructure)*
† Mishra, Navendu *(Stockport)* (Lab)
† Osborne, Kate *(Jarrow)* (Lab)
† Randall, Tom *(Gedling)* (Con)
† Vara, Shailesh *(North West Cambridgeshire)* (Con)
† Warburton, David *(Somerton and Frome)* (Con)
Whitley, Mick *(Birkenhead)* (Lab)

Huw Yardley, Bethan Harding, *Committee Clerks*

† attended the Committee

Public Bill Committee

Tuesday 22 March 2022

[Caroline Nokes *in the Chair*]

Product Security and Telecommunications Infrastructure Bill

9.25 am

The Chair: We are now sitting in public and proceedings are being broadcast. Before we begin, I have a few preliminary announcements. *Hansard* colleagues would be grateful if Members could email their speaking notes to hansardnotes@parliament.uk. Please switch electronic devices to silent. As you all know, teas and coffees are not allowed during sittings.

New Clause 1

Power for operator to upgrade or share apparatus

"(1) The electronic communications code is amended as follows.

(2) In paragraph 17, in sub-paragraph (1), for the words 'sub-paragraphs (2) and (3)' substitute 'sub-paragraphs (2), (3) and (4A)'.

(3) After sub-paragraph (4) insert—

'(4A) The third condition is that, where a site is provided by an emergency service, before the beginning of the period of 21 days, ending with the day on which the main operator begins to upgrade the electronic communications apparatus or (as the case may be) share its use, the main operator provides written notice to the site provider.'"—*(Chris Elmore.)*

This new clause would require operators with agreements under the code that are not subsisting agreements to provide written notice to site providers that are an emergency service before the beginning of the period of 21 days (with the 21 days ending the day the operator begins upgrading the apparatus).

Brought up, and read the First time.

Chris Elmore (Ogmore) (Lab): I beg to move, That the clause be read a Second time.

Good morning to you, Ms Nokes, and to all members of the Committee.

The new clause is self-explanatory, but I will speak to it in the hope of persuading colleagues of its considerable merits. It would require operators with agreements under the code that are not subsisting agreements—agreements that came into force before the code was agreed—to provide written notice to site providers that are an emergency service before the beginning of the period of 21 days, ending on the day that the operator begins upgrading the apparatus.

This uncontroversial new clause would simply mandate operators to give advance notice to sites that provide and deliver emergency services, such as hospitals, for example. Due to the sensitive and life-saving nature of the work that is carried out daily in those buildings, it would make sense for providers of emergency services to be given advance notice of when work is going to be undertaken, in the hope that work will then be able to go ahead as smoothly as possible. The new clause would reduce the delay and interference for both the site owner and the operator.

Under this Government, broadband roll-out targets have been reduced time and again—from full fibre to full gigabit, and now down to 85% gigabit. The new clause would speed up the roll-out of telecommunications infrastructure, which the country needs. We hope that this constructive new clause will have cross-party support, and I urge Members on both sides of the Committee, including the Minister, to support it.

The Minister for Media, Data and Digital Infrastructure (Julia Lopez): I thank the hon. Gentleman for tabling the new clause, which relates to the automatic rights for operators to upgrade and share existing apparatus. To be clear, those rights are already contained in the code, and apply only to agreements completed after the 2017 reforms to the code came into force. The new clause suggests the introduction of a 21-day notice requirement for operators that want to exercise these rights where apparatus is situated on land owned by an emergency service provider.

I very much appreciate the intention behind the new clause, and am grateful to the hon. Gentleman for briefly sharing with me last week some of the instances that he has in mind. Of course, it is important that emergency service providers are aware of work on their sites that may have an impact on their daily activities; I am sympathetic and alive to that. I have tested the issue with officials in the last week, and they suggest that in that context, it is crucial to look at the scope of the paragraph 17 rights, which authorise only activity that will have no more than a minimal adverse impact on the appearance of the apparatus and will impose no additional burden on the other party to the agreement. Clearly, the rights are therefore available only in very limited circumstances.

Of course, operators may need to upgrade and share apparatus that will have a greater impact on a site provider than paragraph 17 permits, and they should be able to do so, but in those circumstances they must obtain the site provider's agreement or seek to have the required rights imposed by the courts. In contrast, the automatic rights in paragraph 17 are available only in very limited circumstances. The conditions in paragraph 17 specifically exclude activities that would impose an additional burden on a site provider. Activities that disrupted a site provider's daily business, or created new health and safety risks, would be very unlikely to satisfy that requirement.

Operators that upgrade or share their apparatus in ways that go beyond the paragraph 17 rights, and which do not have a site provider's permission or court authorisation, will be acting outside the parameters of the code. As such, they may be liable to any legal remedies or sanctions that are applicable to their actions. If an operator is in doubt as to whether the paragraph 17 conditions are satisfied, it would be sensible for it to discuss the planned works with the site provider. I am not aware of any instances in which an operator has relied on its paragraph 17 rights to carry out upgrading and sharing activities that have gone beyond the scope of what that paragraph allows, but if the hon. Gentleman is aware of occasions when that has happened, I would welcome further details and information about them.

At present, we think that the scope of activities permitted by paragraph 17 is so narrow that a specific notice regime is not required. Putting one in place

would undermine the policy intention of the rights, which is to enable limited upgrading and sharing works to be carried out as quickly and efficiently as possible. I therefore hope that the hon. Gentleman will withdraw the new clause.

Chris Elmore: In the light of what the Minister has said and, crucially, her offer to hear the examples that I will provide her with, I beg to ask leave to withdraw the motion.

Clause, by leave, withdrawn.

New Clause 2

REVIEW OF THE CHANGES TO THE ELECTRONIC COMMUNICATIONS CODE

"(1) The Secretary of State must conduct a full economic review of the effect of Schedule 1 of the Digital Economy Act 2017 (The Electronic Communications Code).

(2) The Secretary of State must prepare and publish a report on this review within two months of the passage of this Act and must lay a copy of the report before Parliament."—*(Chris Elmore.)*

This new clause would require the Secretary of State to outline the economic impact of the 2017 introduction of the Electronic Communications Code.

Brought up, and read the First time.

Chris Elmore: I beg to move, That the clause be read a Second time.

This new clause would require the Secretary of State to conduct a full economic review of the effect of the electronic communications code since 2017, and to publish a report on that review's findings. When the code was introduced in 2017, the Government promised that they would publish a review of its impact by 2022, but I am afraid to say that we are still waiting. The Committee should note that this is not a new request; we are merely holding the Government to account on promises that were made in 2017.

The review should look into issues including, but not limited to, the impact of the legislation on investment into mobile networks, the number of new sites provided, the speed of infrastructure deployment, changes in rent to site providers, and the total legal costs that have been borne by the judiciary as a result of litigation. The Department's vague responses to parliamentary questions show that it is unsure of how much money has been saved by rent reductions since 2017. That suggests, in turn, that the Department is also unaware of how much of that money has been reinvested back into the development of telecommunications infrastructure, which was the express purpose of the legislation.

The impact assessment for the previous legislation is clearly overdue, and the testimonies that we heard on Tuesday last week suggested that a review needs to take place sooner rather than later. The Minister was keen to suggest that only a small number of rent reductions were of more than 90%, but testimonies from witnesses last Tuesday suggested otherwise. The Minister also said that the number of legal cases was decreasing, but there have been over 300 since the introduction of the code, compared with just a handful prior to its introduction. Once again, we are hearing mixed messages from the Government while the message from those on the ground who have been adversely affected by the rent reductions is crystal clear.

The simple truth is that we are currently unable to make a clear and objective assessment of the effectiveness of the electronic communications code because its impact has not been reviewed. A review was promised, as I will continue to reiterate, when the legislation was first introduced; I accept that it was not this Minister who made that commitment, but it was this Government. Such a review would give us a better understanding of where we were in 2017, of where we are now in 2022, and of what we need to do to improve the situation in the future, as we increase our reliance on digital connectivity.

Technological progress and innovation will define the success of the United Kingdom in the 21st century, and any progress will be underpinned by how quickly and effectively we are able to roll out digital infrastructure projects such as 5G and gigabit-capable broadband. It is firmly in the national interest to get a better understanding of whether the changes we have made so far have been effective, and what lessons can be learned to ensure that our country thrives in the technological and digital spheres in the years ahead.

For the reasons that I have outlined, I hope that colleagues on both sides of the Committee will support the new clause and ensure simply that the Government are held to account on commitments made when the 2017 code was published.

Julia Lopez: I thank the hon. Gentleman for tabling the new clause and, again, I appreciate the intention behind it. It would require the Government to carry out a review of the 2017 legislation that updated the electronic communications code, which is the overarching legislation that the Bill amends and that we have been discussing in Committee.

I appreciate that the intention behind the new clause is to better understand the impact of the 2017 changes to the code but, unfortunately, such a review clause would have unintended consequences. We are particularly concerned that there might be a chilling effect on the market while the review is carried out, which would lead to delays not just in implementing the measures in the Bill, but in wider deployment. When the 2017 code came into force with reduced rents, a lot of cases went through the courts because operators were still on higher rents as long as negotiations were ongoing. We do not want to see a similar challenge in this case.

If a review takes place, stakeholders will likely delay entering into agreements to enable the deployment of infrastructure. Only when the review has concluded and it is clear whether further changes are to be made to the code will parties be prepared to make investment or financial commitments. That will have a profound effect on our connectivity ambitions, despite our desire to move as quickly as possible to level up the country with world-leading connectivity. It will also have an adverse impact on consumers and businesses, many of whom want to access higher speeds and the latest technologies such as 5G.

The Bill focuses on a few issues that prevented the 2017 changes from having their full impact, such as speeding up deployment while protecting the rights of landowners and site providers. Wider changes to the code will halt all progress made and will risk bringing deployment to a standstill. That would leave many homes and communities without the upgrades to connectivity that they badly need, which I am sure the hon. Member will agree would not be the desired outcome.

[Julia Lopez]

Let me clarify what was said in 2017 about reviewing the changes to the code. In the impact assessment that accompanied the reforms, the Government said that they would review the policy by June 2022. They did not say that they would carry out a full economic review of the impact of the reforms on the rental agreements. We have reviewed the policy. Officials have held regular meetings with stakeholders since the 2017 reforms came into force, including facilitating workshops between stakeholders to encourage more collaborative working. My predecessor, my right hon. Friend the Member for Maldon (Mr Whittingdale), held a series of roundtable meetings with stakeholders from both the operator and the site provider communities so that he could understand the situation better.

Since I have been in post, I have been testing some of the concerns of the hon. Member for Ogmore in Parliament to ensure that we are beyond some of the initial challenges that we all accept existed when the code changes were made. Regular engagement and the issues highlighted directly informed last year's consultation, which preceded this Bill, and led to the provisions in the Bill that are needed to realise the benefits of the 2017 reforms. I hope that this gives the hon. Member reassurance that we have reviewed the policy as a whole, and I ask that he withdraw his amendment.

Chris Elmore: I have listened to the Minister and I accept that there are challenges with any review, but the only way in which we learn is by reviewing what we have done previously. There are some nicks in the system that are still not rectified. There is no reason why a Government review would mean that the industry would need to stop rolling out fibre broadband, improving broadband more generally, 5G roll-out or anything else. The process could be done with industry to ensure there is an efficient and effective way of reviewing, so that we can learn from what has happened and improve moving forward. I am keen to push the new clause to a vote.

Question put, That the clause be read a Second time.

The Committee divided: Ayes 4, Noes 9.

Division No. 7]

AYES

Elmore, Chris	Mishra, Navendu
Long Bailey, Rebecca	Osborne, Kate

NOES

Baynes, Simon	Lopez, Julia
Bhatti, Saqib	Randall, Tom
Double, Steve	Vara, Shailesh
Edwards, Ruth	Warburton, David
Hart, Sally-Ann	

Question accordingly negatived.

New Clause 4

REQUIREMENT TO CONSULT ON IMPOSITION OF MINIMUM PERIODS OF TIME FOR WHICH PRODUCTS WOULD NEED TO RECEIVE SECURITY UPDATES

"(1) Within three months of the date on which this Act receives Royal Assent, the Secretary of State must publish the text of draft regulations exercising the power in subsection (1) of section 1 (Power to specify security requirements) so as to provide for minimum periods of time for which relevant connectable products would need to receive security updates.

(2) The Secretary of State must consult—

(a) representatives of all relevant persons (as defined in section 7 (Relevant persons)), and

(b) any other person the Secretary of State thinks appropriate on the draft regulations.

(3) Within three months of the final date for receipt of responses to the consultation, the Secretary of State must lay before Parliament a report on the responses."—*(Chris Elmore.)*

Brought up, and read the First time.

Chris Elmore: I beg to move, That the clause be read a Second time.

During the oral evidence session last Tuesday, we heard a number of concerns about part 1 of the Bill, which were outlined particularly eloquently by Madeline Carr, professor of global politics and cyber-security at University College London, who tellingly stated that she does not currently own an Alexa due to a lack of trust, and that the Bill as it currently stands would not give her sufficient confidence to go out and purchase one. Her Majesty's Opposition value the contribution and knowledge of experts such as Professor Carr, and we have tabled new clause 4 on that basis.

The clause would require the Secretary of State to undertake a consultation on the imposition of a minimum period during which relevant connectable products would need to receive security updates. That would allow the Secretary of State to consult with academics such as Professor Carr, among others in the field, to establish the best way of making those connectable products, which have the potential to bring huge benefits to our lives, as safe as possible for as long as possible.

I presume the Minister might retort by saying that increased regulation of this sphere might stifle innovation, but that is exactly the opposite of what we heard last Tuesday. What we heard was that without strong, strategic Government intervention, there is not much desire for, or a market for, cyber-security. That is why introducing a minimum period for which connectable products would be subject to security requirements is so important: without Government intervention, increased security for British consumers will not come about.

Another reason that implementation of the new clause is so vital is that it relates to the digital divide and the ability of those who are the most financially vulnerable to have access to secure products. We do not want the less well off to be purchasing items that are subject to security updates for a much shorter period, thus making them more vulnerable to cyber-attacks than those who are more financially secure. I raised that issue on Second Reading and, dare I say it, there was some pushback from Members in the Chamber, but the issue was highlighted by Professor Carr and David Rogers, who was the lead editor during the process that is the basis for the Bill.

The party that I am deeply proud to represent was founded to represent the interests of working people, and it is ultimately my responsibility to ensure that working people across the country do not lose out with respect to the pace of technological change and as the threats facing that technology continue to increase. We acknowledge that no Bill can anticipate all threats that we will face in the future and the varying types of

product that will come to the market, but we do have control over ensuring that we do our utmost in legislation to best protect the citizens of the United Kingdom. As we heard from a number of industry experts, one of the best ways to do that is to introduce a minimum period for which these products should be subject to security updates. For that reason, I hope the Committee will support the new clause.

Julia Lopez: Again, I thank the hon. Member for his suggestions, and I always appreciate the intention behind what he is trying to do. On this matter, we have been consulting with experts throughout the development of the legislation. As he will be aware, a lot of the details about how we shall regulate these products will come in secondary legislation. Here, we are taking broad powers so that, as the technology develops, we can tweak them as things change. We are also considering a wide number of products that will be in scope.

We do not want to take specific powers at this stage, and, as I mentioned in relation to the hon. Gentleman's amendment 6, which we debated last week, it is important that the legislation retain the flexibility to adapt to and reflect the changing threat and technological landscapes. We have consulted widely on the legislation, and will continue to do so where new requirements are appropriate, but committing the Government to working on requirements framed using terminology that may seem appropriate today could limit the security benefits of such a requirement in the future.

As I reassured the hon. Member last Thursday, we are committed to introducing security requirements based on the first three guidelines of the internationally recognised code of practice for consumer internet of things security. Those will include a requirement for manufacturers to be transparent about the time for which products will be supported with security updates. At its core, that approach demonstrates a shift towards clear transparency that can inform the consumer when purchasing a relevant device. We know that many consumers are security conscious, but, as things stand, not enough manufacturers make that information readily available to them.

Data from Which?, which the Committee heard from last week, highlights that less than 2% of assessed products had clear information on the length of time for which they would receive security updates. We are using legislation to increase the availability of information to UK consumers, so that they can make their own purchasing choices with a clear understanding of security. As consumers learn more, they will expect more, and we hope that that will drive the market approach to embedding minimum periods for security updates. Last week, the Committee heard from Which? that some consumers might be continuing to pay for their devices even after security updates are available to them. That is exactly the kind of thing we want to avoid, and we think that transparency is the key to raising consumer awareness.

As manufacturers raise the bar to the appropriate level, we anticipate that more and more will do the same as a result of that shift to transparency. Should manufacturers fail to respond in that way, the Government may, in the future, consider that there is a case for setting out a requirement for certain products to be covered by minimum security periods. That is all part of the flexible approach we are keen to take to legislation to ensure that our requirements reflect the realities of technologies and the wider market.

Additionally, I have concerns that the new clause would commit the Government to unnecessary work that would only need to be repeated following the implementation of the initial requirements, before a substantiated case for this additional requirement could be made.

For those reasons, I am not able to accept the new clause. We are taking broad powers and a lot of details will be looked at when we consider secondary legislation. We will be looking at this issue as these products develop. If we think that a requirement for the hon. Member's minimum period comes about, we will look at the issue again. At this stage, though, I hope he will consider withdrawing his new clause.

9.45 am

Chris Elmore: I have listened carefully to what the Minister has said. For the record, I agree with her about increasing the availability of security information for consumers. I am concerned that the figures are so low regarding the public's understanding of the cyber-security arrangements when buying goods, whether that be a smart toothbrush—that was an education to me a few months ago when I was being lobbied on the Bill—or what data our smart fridges hold on us. Such information is a revelation, although I should probably know better as the shadow Minister.

The new clause is about a consultation for minimum periods and I accept that there is secondary legislation linked to that. However, as the Opposition, we have an obligation, particularly following the evidence from Professor Carr, to make clear what we think should happen regarding a simple consultation by the Secretary of State on the imposition of minimum periods for purchasing; and the Committee can make that clear in a separate decision.

Question put, That the clause be read a Second time.

The Committee divided: Ayes 4, Noes 10.

Division No. 8]

AYES

Elmore, Chris	Mishra, Navendu
Long Bailey, Rebecca	Osborne, Kate

NOES

Baynes, Simon	Hart, Sally-Ann
Bhatti, Saqib	Lopez, Julia
Double, Steve	Randall, Tom
Edwards, Ruth	Vara, Shailesh
Grundy, James	Warburton, David

Question accordingly negatived.

Question proposed, That the Chair do report the Bill, as amended, to the House.

Chris Elmore: On a point of order, Ms Nokes. I thank all Committee members for a constructive and cordial debate throughout, including in the evidence sessions. I thank the Clerks, particularly for answering my team's never-ending questions. As new members of staff for

[Chris Elmore]

me who have been flown into a new Bill, James Small-Edwards and Alex Williams have been superb. I thank you, Ms Nokes and Mr Stringer, for your chairpersonship across the sessions—and, of course, the Doorkeepers, who have spent all their time running through the room as I am calling for Divisions.

Question put and agreed to.

Bill, as amended, to be reported.

9.48 am

Committee rose.

Written evidence reported to the House

PSTIB17 Dan Patefield, Head of Programme, Cyber and National Security; and Sophie James, Head of Programme, Telecoms and Spectrum Policy, techUK (supplementary submission)

PSTIB18 Palo Alto Networks

PSTIB19 CyberUp Campaign

PSTIB20 Protect & Connect