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