PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT

Second Delegated Legislation Committee

DRAFT PRODUCT SECURITY AND TELECOMMUNICATIONS INFRASTRUCTURE (SECURITY REQUIREMENTS FOR RELEVANT CONNECTABLE PRODUCTS) REGULATIONS 2023

Monday 11 September 2023

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

Friday 15 September 2023

The Committee consisted of the following Members:

Chair: Mr Philip Hollobone

† Afriyie, Adam *(Windsor)* (Con)
† Bruce, Fiona *(Congleton)* (Con)
† Byrne, Ian *(Liverpool, West Derby)* (Lab)
† Creasy, Stella *(Walthamstow)* (Lab/Co-op)
† Double, Steve *(Lord Commissioner of His Majesty's Treasury)*
† Fletcher, Mark *(Bolsover)* (Con)
† Freeman, George *(Minister for Science, Research and Innovation)*
† Kruger, Danny *(Devizes)* (Con)
† Mackinlay, Craig *(South Thanet)* (Con)
† McDonnell, John *(Hayes and Harlington)* (Lab)
† Morris, Anne Marie *(Newton Abbot)* (Con)
† Morton, Wendy *(Aldridge-Brownhills)* (Con)
† Onwurah, Chi *(Newcastle upon Tyne Central)* (Lab)
† Owatemi, Taiwo *(Coventry North West)* (Lab)
† Rimmer, Ms Marie *(St Helens South and Whiston)* (Lab)
Turner, Karl *(Kingston upon Hull East)* (Lab)
† Villiers, Theresa *(Chipping Barnet)* (Con)

Bethan Harding, *Committee Clerk*

† attended the Committee

Second Delegated Legislation Committee

Monday 11 September 2023

[Mr Philip Hollobone *in the Chair*]

Draft Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023

6 pm

The Minister for Science, Research and Innovation (George Freeman): I beg to move,

That the Committee has considered the draft Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023.

It is a great pleasure, Mr Hollobone, to serve under your direction and leadership this afternoon.

Consumers have a right to assume that if a product is for sale, it is safe and secure; too often, that is not always the case. Government must act to ensure that when UK consumers and business customers are purchasing consumer connectable products, they are not putting themselves at risk of cyber-attack, theft or even physical danger. Through the draft regulations, the Government are ensuring that protections are implemented for our commonly used items such as smart phones, smart watches and smart baby monitors, and for the UK citizens and businesses that use them.

Cyber-crime is thought to cost the UK billions of pounds—the total cost is estimated at about £27 billion a year—and it is on the rise, in particular cyber-crime that targets the internet of things. Vulnerable IOT products are a key attack vector for criminals, allowing them to compromise not only the device, but potentially the user's network and the broader connected technology ecosystem. This draft statutory instrument is an essential step in fighting the dangers of such cyber-risks.

The draft regulations are made under powers provided by the Product Security and Telecommunications Infrastructure Act 2022 and the European Union (Withdrawal Agreement) Act 2020. The regulations will mandate the manufacturers of consumer connectable products made available to customers in the UK to meet minimum security requirements, unless excepted. The instrument completes the introduction of the UK's world-first product security regime established by part 1 of the 2022 Act.

Subject to the approval of the Committee here gathered, the regime will afford UK citizens and businesses world-leading protections from the threats of cyber-crime. Research covering the first two months of this year shows that cyber-attacks targeting IOT devices have tripled since 2021, so the need for action has never been greater. The regime will also equip the Government with the tools to ensure the long-term security of a vital component of the broader UK technology ecosystem. That is especially important as frontier technologies, from artificial intelligence to quantum, allow technology to become more embedded in our economy and society than ever before.

Theresa Villiers (Chipping Barnet) (Con): I very much welcome the Government's efforts to make consumer goods in the so-called internet of things safer and more secure and resilient against cyber-attack, but how confident is the Minister that the regime will work against a determined attack by a hostile state? Recently, the Intelligence and Security Committee of Parliament produced a report saying that China targets UK industry and technology "prolifically and aggressively". Will the draft instrument be effective in protecting us from that kind of attack?

George Freeman: My right hon. Friend makes an important point. Perhaps I can come back to it in a bit more detail at the end of my comments, but I will make this point now: as I described, the measures will give a minimum level of security assurance to customers. This draft instrument is not the frontline, the arrowhead, of UK international counter-espionage; this is about ensuring that when people buy an iPhone or some such device, they can be confident that basic minimum standards have been met. It is not the basis on which we can all go to bed at night safe and secure, with the whole of UK critical national infrastructure secure. That work is being led by my right hon. Friend the Chancellor of the Duchy of Lancaster and Deputy Prime Minister.

I turn briefly to the basics of the draft instrument. First, on security requirements, the regulations mandate that manufacturers comply with the security arrangements that Parliament has set out in schedule 1. The security requirements are backed by security experts and have been consulted on extensively. In the view of the National Cyber Security Centre, which has been very involved, they will make the most fundamental difference to the vulnerability of consumer connectable products through the guidelines in the UK's code of practice for consumer IOT security.

The first requirement bans businesses from selling to UK customers consumer smart products with universal defaults or easily guessable default passwords. Such passwords expose users to unacceptable risk of cyber-attack and allow malicious actors to compromise products at scale, equipping them with the computing power to launch significantly disruptive cyber-attacks.

Secondly, manufacturers will be required to publish, in an accessible, clear and transparent manner, the details of a point of contact for the reporting of security vulnerabilities. Despite previous Government interventions and the increasing threat of cyber-crime targeted at these products, less than a third of global manufacturers had any policy for how they can be made aware of vulnerabilities as of 2022.

The final security requirement will ensure that the minimum length of time for which a product will receive security updates is not just published, but published in an accessible, clear and transparent manner. Consumers value security and consider it when purchasing products. Equipped with the vital information mandated by this requirement, UK customers and their intermediaries will be able to drive manufacturers to improve the security protections that they offer through market forces.

I will turn to the conditions for deemed compliance. Where the security outcomes that we are seeking to achieve are entirely or partially delivered through broader international standards, the regime allows manufacturers compliant with those standards to more readily demonstrate their compliance with our security requirements. That is the intent of regulation 4, and schedule 2 sets out conditions based on analogous provisions in two leading international standards. Where those conditions are met, a manufacturer is to be treated as having complied with a particular security requirement. Colleagues will be pleased to know that we have tried to take the opportunity to reduce process-driven bureaucracy and make it easy for proper compliance to be demonstrated in the interest of consumer protection.

The excepted products protocol in the instrument sets out a list of products that we have exempted from the scope of the product security regime. First, select product categories made available for supply in Northern Ireland are exempted. That exemption ensures that the regime upholds the UK's international commitments under the EU withdrawal agreement while extending the protections and benefits offered by the regime to consumers and businesses across the UK. Additionally, smart charge points, medical devices and smart metering devices are exempted to avoid double regulation and to ensure that those products are secured with the measures most appropriate to the particulars of their functions. To answer the point raised by my right hon. Friend the Member for Chipping Barnet, we would not want to rely on these regulations alone for the safety of medical devices; they are covered, quite rightly, by far more extensive regulations through the Medicines and Healthcare products Regulatory Agency.

Adam Afriyie (Windsor) (Con): I welcome the instrument in general terms, but I have a couple of quick questions. The Minister mentioned that Northern Ireland is outwith the scope of this regime because of its interaction with the European Union as it stands today. In effect, that treats Northern Ireland as not part of the United Kingdom for these purposes. Am I correct in thinking that?

Secondly, I completely agree with the cut-outs for medical devices, smart meters and so on. The Minister may need some inspiration on this, but are vehicles included in the minimum standards, given that lots of them now have autopilot systems and software updates to undertake week in, week out, and passcodes included in the software?

George Freeman: Those are two excellent questions. On Northern Ireland, basically the answer is no. This goes with the grain of the Windsor framework that the Prime Minister has negotiated, and it recognises that for the purposes of consumer standards, Northern Ireland is governed by the EU proposals in this space. I am delighted to say that the UK proposals are a little quicker, more agile and fleet of foot, and to some extent that might give Northern Ireland manufacturers an advantage. Perhaps I could come back to the point about vehicles; it is an important point to which the internet of things is very relevant.

The instrument also exempts laptops, desktop computers and tablets without a cellular connection from the regime scope. Engagement with industry highlighted that the manufacturers of those products would face completely unique challenges in complying with the regime. On many occasions where those products are in use, they are already subject to extensive cyber-protection standards. It is therefore not clear at this stage that including those products in the regime scope would be proportionate. However, as with so many of these things, I am happy and keen to keep a watching eye on that to ensure that we are keeping up with technology.

The administrative provisions in the SI, including those relating to statements of compliance, are uncontroversial. The regime will require that those documents are company products serving as an audit trail to enable compliance across the supply chain and to facilitate effective enforcement. We do not expect every single consumer to read all of that every time they buy a pair of speakers or any digital device, but the active intermediaries on behalf of consumers will be able to access it, and we foresee an active enforcement culture, not least online.

The product security regime, including these regulations, is the first in the world to recognise that the public has a right to expect that the products available for them to purchase are secure, and that the Government have a duty to enforce that. The measures will cement the UK as a world leader in responsibly embracing the enormous potential of emerging technology. They are a first step in the development of a framework that will keep pace with technology. I commend the regulations to the Committee.

The Chair: The Committee will be delighted to know that the debate can continue until half past seven.

6.10 pm

Chi Onwurah (Newcastle upon Tyne Central) (Lab): It is a delight to serve under your chairmanship, Mr Hollobone, in this important debate. I thank the Minister for setting out the context for the regulations and their intended effect. I declare an interest: as the Minister is aware—I certainly talk about it enough—before I entered Parliament I worked in tech for 23 years, with the last six at Ofcom as head of telecoms technology, which included internet security.

My experiences at Ofcom and as a chartered electrical engineer gave me a strong awareness of the immense value of new technologies, such as IOT, but also of their potential harms. In 2011, I was the first Member of Parliament to mention the internet of things in this place, in a Westminster Hall debate I secured on machine-to-machine communications. Since then, the market for connected devices has grown exponentially; with smart phones in so many pockets, smart appliances in so many homes and wearables on so many wrists, there is a clear need for robust consumer protections. Let me be clear that the Labour party welcomes the introduction of the regulations, which will provide long overdue protection for users of consumer connectable products.

Although a step in the right direction, it has been a long while coming. According to Cisco, in 2010 there were 12.5 billion devices connected to the internet. Strategy Analytics found that in 2018 that had risen to 22 billion, with much of that growth driven by smart phones and IOT devices. It was only in 2016, when the Government published their national cyber-security strategy,

[Chi Onwurah]

that they set an ambition for the majority of online products and services coming into use to be secure by default by 2021.

Responding to a question I tabled in December 2016, I was told that cyber-security was a top priority for the Government. It was a top priority, however, that inspired almost no action—a little like online harms, where legislation is still to be passed. By the time 2020 came around, the Government had acknowledged the failure of their voluntary code of practice, and were instead proposing a new regulatory regime. As the Minister said, having legislated on the issue in 2022, we now stand to see regulations finally coming into effect in 2024.

It is clearly a case of better late than never. I understand the challenges involved in delivering a set of tech regulations on a complex and technical subject. It is right that there has been an extensive consultation on the subject, which no doubt created a wealth of information that required careful analysis. The reason I bring up the delay is that while the Government were asleep at the wheel, criminals were not. In 2016, hackers used domestic IOT devices, including televisions and baby monitors, to bring down major websites such as Twitter and Spotify. That style of attack poses huge risks to businesses and critical national infrastructure, such as our electricity grid.

Individual consumers have also been left vulnerable. Whether it is smart toys, which enable hackers to target our children, or smart alarm systems that leave people's properties vulnerable to break-in without forced entry, these are massive and hugely damaging threats for individuals, families, businesses and our national security. In delaying action on the matter, the Government have effectively given hackers the head start.

Recent years have seen a surge in the popularity of smart devices in the home, such as smart speakers and doorbells. In 2016, Ofcom estimated that there were 13.3 million IOT connections in the UK, including 5.7 million categorised as consumer electronics. It is estimated that by 2024, that figure will have increased to 40 million. Globally, we expect that there were 14 billion connections in 2022.

There was an opportunity for the UK to get a consumer protection regime in place ahead of this recent acceleration in the uptake of smart devices. Doing so could have meant that millions of devices being bought by British consumers in the intervening period were sold securely, and it could have given a boost to our innovative businesses in that area by giving clarity of regulation. Instead, consumers and businesses have been left relatively exposed to risks. I ask the Minister, could the Government have delivered this regime more quickly?

Acting faster would have carried significant upsides for British businesses, as I have said, in adapting to the new requirements. These regulations translate the three most critical measures from the voluntary code of practice into the statute book, and, as I have said, we welcome them. However, given that mandating these recommendations seems to have remained the Government's intention from 2020 onwards, it is more confusing as to why that was not legislated for in primary legislation, as Labour called for during the debates on the Bill in 2022. I fear that in pursuit of maintaining the Bill's flexibility, despite expert consensus on the importance of the requirements, the Government have kicked the can down the road on providing certainty, which our businesses need in order to drive the economic growth that we all hope to see.

As the impact assessment for the SI notes, the proposals will have significant consequences for thousands of businesses, including around 170 manufacturers and thousands of retailers and charities involved in the sale of these products. In many cases, the cost of compliance would have been hard to avoid, but businesses would have benefited from earlier clarity about the scope of the regulations. That is particularly true when non-compliant equipment will need to be disposed of.

Now that the scope of the regime is finally confirmed, businesses will need guidance to ensure that the benefits of the new requirements are felt by consumers and that the detrimental business impact is minimised. The explanatory memorandum accompanying the SI promises non-statutory guidance for industry. Will the Minister commit to a timeframe for delivering that guidance, or give businesses any sign about when that might become available? As we know, small businesses do not have chief technology officers, and they need the support and help of Government.

I would also like to query some of the inconsistencies that I see in the regulations. As the Minister said, computers, laptops and non-cellular tablets, except those designed for children under 14, have been exempted. The reason seems to be that the situation, particularly the supply chain, is complicated. Could he say a little more about that?

I would also like clarity on the relationship between these measures and cellular internet of things modules or SIMs , which I think is what the hon. Member for Windsor was referring to when he spoke about vehicles. SIMs power much of the consumer connected device landscape by enabling internet access, and are often embedded. China is currently attempting to corner the global market in SIMs, which could have immense national security implications. For example, when it comes to cars, they can transmit location, the route and even videos of the driver and passenger. Will the Minister say clearly whether this legislation is applicable to SIMs? If not, why not, and what protection is to be brought forward in that regard?

Further, while the Product Security and Telecommunications Infrastructure Act gave the Government the power to create requirements on manufacturers, importers and retailers, those seem unevenly applied by this SI. To give just one example, there is no requirement for distributers of these products to publicise the defined support period, but there is such a requirement for manufacturers to do so, even though it is the distributers who often provide the direct interface with the consumer. Will the Minister explain why the Government are taking that approach, and whether they are considering further regulations applicable to distributers?

There is also very little in the SI about enforcement, but the parent Act allows for recall notices, stop notices, penalty fines and forfeiture of products, and the impact assessment says that the Office for Product Safety and Standards will be the enforcing agency and will need to buy devices to test. Will the Minister assure us that the office will have the resources it needs to do this, given the global and, as he said, complicated nature of the market for these products and the embedded nature of the connectivity modules?

I have the greatest respect for the Minister. He knows, and I am sure that he wishes it were otherwise, that his Government's record on digital inclusion is not the best. There has been no digital inclusion target since 2014, and that has resulted in 10% of our population being excluded. Is he certain that consumers will be adequately protected by the three basic measures—as he himself referred to them—that the SI brings in? He says they will give a minimum level of security, but he also implies that they will keep our citizens safe from cyber-attacks. Does he really think that that is the case?

Regardless, we want to see consumers empowered to understand and assert their rights in this area. My final question to the Minister is whether, in addition to guidance for industry, the Government will issue guidance to consumers on digital inclusion and literacy. To conclude, we support the introduction of the regulations, which will establish much-needed protections for users of connected devices and address significant gaps in our national cyber-security. However, the Government must act fast to communicate the new requirements to businesses and consumers well in advance of commencement, and I hope the Minister will address my questions in his remarks. It is important that these regulations are a success, and I urge him to do all he can to ensure that that is the case in the build-up to April next year.

6.22 pm

Craig Mackinlay (South Thanet) (Con): It is always a pleasure to serve on one of your Committees, Mr Hollobone. Usually, pieces of delegated legislation do not create a great deal of interest, but this is one that I am most excited about, as the Minister will be pleased to hear, because this is a topic that I have been discussing in various quarters for some years.

I am concerned about the internet of things—what is actually happening within the clever software and products? Frankly, they go beyond my full understanding and, I am sure, beyond that of many in the room. If I understand it correctly, the whole concept of the statutory instrument is for consumers to have some certainty that the products they are buying are safe as regards their data security and that they will not be hacked through cyber-activity.

The regulations will apply to a multitude of goods. Those goods are expanding exponentially, whether that is the clever fridge that—if one is lucky enough to buy one—says when more milk is needed, or the Ring door camera telling the owner by text message or some app on their telephone that someone is at the door. If I put my hand in the air—I might even be able to make it happen—Siri starts talking to me. What is happening there? What is Siri listening to, and what is Siri listening to that it should not be listening to? One hopes that software from a known, big global brand has more security, surety and safety associated with it, and I hope our trust in some of these bigger organisations, such as Apple, is duly found.

One need only look on Amazon these days—I am not pointing out Amazon for any great reason—to see that the number of internet of things products available is truly vast. I would not even like to go through the whole gamut of what is available. There are speakers, baby cameras and even lightbulbs—I purchased one not too long ago. Obviously, a variety of watches from big brands is available—or smaller brands from China, available at a fraction of the price of the bigger brands but seemingly to the user doing all the same clever things. One wonders at times whether that cheapness is meant to encourage us to buy a product for good or ill.

I raised that very issue with National Trading Standards in the European Scrutiny Committee. Members might think, "Why on earth is the European Scrutiny Committee thinking about these things?" The hearing was on product standards related to Northern Ireland and border issues. Generally, National Trading Standards is interested in whether something will catch fire when we plug it in. Will it be physically safe and not burn the house down, scald someone or catch light? When I raised my concerns about the in-built software, National Trading Standards said it was a very interesting point, but had no great idea about what to do about it, so a few questions arise.

I note that in the SI there is a required statement of compliance by the manufacturer. The Minister referred to the National Cyber Security Centre. When a product arrives from China or elsewhere into the UK via our purchase from Amazon—not necessarily off the Amazon shelf but perhaps through one of the facilitating agents that it allows—I doubt that the National Cyber Security Centre or National Trading Standards entrench themselves in what it does behind the scenes. That is to say, in the clever software that drives it. Even if they did, it would be at a moment in time.

How often do we buy these products—even a phone? I note that my watch OS is on 9.6.2. It upgraded only last week it is already prodding me that it needs 9.6.3. One wonders, "Why couldn't they get it right in the first place?" That happens regularly. It could be an innocuous product, such as the baby monitor that we can look at on a clever app on our phone. We merrily download those apps, but after a month or two they scurry off to the internet with all sorts of "agree here" boxes and 15 pages of terms and conditions. I am sure not one person in the room reads them before ticking the box and saying, "I accept all that—just give me the thing". That item might have been safe when it crossed the border, if it was even tested to that point, which I doubt, but we have very little surety about what happens in the software upgrades. It just scurries off and does its software upgrades; we are all very familiar with that.

Last week, I entered the brave new world of lightbulbs. I had some lighting done and decided on an app that lets me put the lightbulb on from this room should I so wish. Amazing—really consumer friendly. Why did I decide on that app? The electrician who did some work in my home said, "I use this one and I rather like it. It has all the features and does all the bits that one wants it to do." But do I know what is really happening? Do I know what data is being collected?

There was a report just last week that even something as basic as the Ring camera that tells us when someone is at the front door is scurrying off and sending out all sorts of data—our email address and whatever else we have provided to get it working. Sometimes there is an intrusiveness in the questions asked by some of these apps, and one wonders why they need that sort of information. Often, there is also the question, "Will you allow this app to track you across other websites?" One wonders whether this is just becoming a very grand data capture exercise. I have no concept of where the data goes—for whom, why or anything else. Have any Members in the room had an experience like this? I was discussing

[Craig Mackinlay]

a colour of paint with my wife and, lo and behold, I picked up my iPad and Farrow and Ball and Dulux seemed to come up almost before I started writing in the search engine. One wonders what is going on in the background. I ask the Minister: are we likely to test the underlying software when it comes across the border, or simply to rely on self-certification and certificates of compliance?

I am pleased that my hon. Friend the Member for Windsor raised the point about Northern Ireland, because I want us to have very safe and good legislation so that consumers can be sure about the products that they buy. Perhaps the regulations will represent a greater degree of consumer safety than we currently have or had under the old EU legislation. I think that that was the Minister's intent—for the measures to be world leading and fleet of foot. I think those were the words that he used. But where does that leave us? Products that can enter the EU or are in the EU market—in the Republic of Ireland, for instance—have free access into Northern Ireland. They then have pretty much free access—because we are a United Kingdom, and we should not forget that—into GB. Could we have a situation in which the safety of goods sourced or provided for the consumer in GB, and potentially NI if they can tick the boxes required under single market rules, is degraded when that route from the EU, through the Republic, into NI and into GB, which is allowed, occurs? Or are we going to accept, as we seem to have done, that if CE markings are acceptable in the EU, they are acceptable here?

I will close—I am sure to the great pleasure of many in the room—by saying that this is an expansive debate about serious things, as we connect ourselves to the internet. One wonders: when we buy cheap, are we buying dangerous?

6.31 pm

Stella Creasy (Walthamstow) (Lab/Co-op): It is a pleasure to serve under your chairmanship, Mr Hollobone. I do not wish to detain the Committee for long, but it strikes me that it would be useful to make a couple of observations, not least that I find myself in substantial agreement with the previous speaker about the importance of this issue.

Craig Mackinlay: First time for everything.

Stella Creasy: There are so many stopped clocks around this building at this point in time. I am also now fascinated to see what will come up on my Facebook adverts as a result of the hon. Gentleman's speech. I suspect I will be getting many about lightbulbs, and Farrow and Ball paints—people can make their own jokes out of that.

I have a few simple questions for the Minister. So far, we have talked about products and the regulation of them, but we have not talked about consumers and consumer experiences. The elephant in the room is Brexit. After all, we were signed up to regulations that were shared across a massive consumer group of 550 million consumers, which meant that we had weight when negotiating with manufacturers. Now we are not, and we are bringing in our own regulations. Whatever one thinks of that decision, it means that there will potentially be some anomalies for consumers, unless our consumers never leave this country, whether to go to Northern Ireland or to mainland Europe. Can the Minister say a little about whether the draft regulations will have an impact on guarantees on consumer standards?

In particular, a lot of people will look at the exchange rate and try to get a better deal by buying goods overseas. What will the measures mean for consumers who might want to use any of these items on their holidays? People might take a baby monitor with them, or if their watches break they might walk into an Apple store in a foreign country and ask for help. What will our having a different set of regulations mean? Should we buy an item overseas to use it here? Could the companies tell us that we have voided our guarantees because we have bought a good in a different territory, where there are different regulations and therefore potentially different software components?

Has the Minister had any conversations with his colleagues about the requirements under the Consumer Rights Act 2015? The consumer protection regulations were written at a time when we all abided by a common framework of regulations, which meant that consumers did not need to worry about these things. Now we are going it alone, so when we go overseas or bring things here from overseas, there will inevitably be conflict and confusion. The Minister said a lot about the companies and the regulations; he has not said as much about the actual consumers—our constituents—who might suddenly find that "Computer says no" repeatedly, and not know to whom they can turn to do anything about it.

6.34 pm

George Freeman: Tempted though I am to delay the Committee with long, exhaustive answers to all those points, which were well made, perhaps I could reassure colleagues on both sides of the House that we have thought about them. Some important points were made for the record, and I will try to keep my speech as short as possible. I thank you, Mr Hollobone, and the Committee: the feedback is incredibly helpful. I would value a chance to continue this discussion with those who have spoken today, many of whom have taken an interest in this subject for a long time.

Let me start with the hon. Member for Newcastle upon Tyne Central, speaking for the Opposition. I congratulate her on returning to the position that I like to think of as my shadow. It has been a pleasure working with her. I also congratulate her on being the first to mention the internet of things in this House if indeed that is verifiable—I am sure it is, digitally as well as in many other ways. On the accusation that the Government were a bit slow to move in 2021, I will just gently point out that there were some other things going on, not least the pandemic, and that we are in fact, with this, quicker than the EU that we have just left. This is an example of us being more agile and more forward-leaning.

I will also make this point. Many of us have sat through and nodded through European legislation, knowing that there is really nothing we can do to change it. This is a good example of Members of Parliament, from both sides of the House, raising important points and the Minister listening, to ensure that we get our own

legislation right. I think that if we had done that a bit more, we would not have had the frustrations that we did.

On the point about the hackers having a head start, I think the truth is that technology is moving at such a pace that of course those who want to harness technology for ill generally tend to move much more quickly than the Government. That would be true were the hon. Member for Newcastle upon Tyne Central in my position. What we are doing today is moving to shut down that head start. There are genuine questions about how quickly we move and how we get it right. I make the commitment to all colleagues that this is a start and we intend to have an annual process of listening to colleagues in the House, listening to the industry and asking whether we should not be going further faster to keep up with technology. The Opposition, I know, have the monopoly on hindsight, led as they are by the extremely able Leader of the Opposition, often referred to as Captain Hindsight. I will just point out that none of us quite foresaw the pace at which this would all move. I know that Government are often not the fastest mover, but we are, here, moving more quickly than partners in Europe.

Chi Onwurah: Will the Minister give way?

George Freeman: I am on a roll. I have to say that no one cheered more loudly than when I heard the hon. Member talk about business certainty. As the right hon. Member for Hayes and Harlington is a member of the Committee, I cannot help but point out that the biggest business certainty was making sure that he never became Chancellor, with his agenda of radical socialism and neo-communism. I notice—for the record—that he is no longer in his place, which is probably a good thing for business certainty.

Let me turn to the points that were raised. Perhaps, with your permission, Mr Hollobone, I can write to everyone with an update on our thinking about the timetable. We are looking to get the regulations in place as quickly as we possibly can. Perhaps I can come back to the point about the timetable, because it requires a detailed answer.

As I said, I will deal with the various points that were made. On the question of exemptions, this is a start. The Government are initially mandating security requirements that, in the opinion of the National Cyber Security Centre—this is not just my whim; it has been consulted on deeply—will have the most fundamental impact on the risks posed today by insecure consumer connectable products. We are confident that the requirements are robustly evidenced, are proportionate and are appropriate to mandate in law at this time. That is not a step we take lightly. The real key is to change the culture and to create a culture in which distributors and all those involved in the supply chains know that they are required by law to do this; they have a responsibility to consumers. However, should the Government deem it appropriate, the parent Act empowers Ministers to introduce further measures in the future, to keep pace with the changes in technology and the threat landscape. Those are powers that we intend to use, in consultation with the House.

Let me turn to the point about security updates, which a number of colleagues raised. The Government do not yet consider it appropriate to mandate and specify minimum security update periods for relevant connectable products, before the impact of the initial security requirements is known. Our mandating necessarily broad regulation across a sector as inherently complex as technology security will always run the risk of imposing obligations on businesses that are disproportionate to the associated security benefits, or leaving citizens exposed to cyber-threats. There is no consensus yet in the industry. One of the things that we hope this measure will do is trigger a broader conversation, on the timescale that we need—each year—to talk to industry about what is happening and ensure that we are keeping up to date.

Let me pick up the point about digital exclusions. A number of people asked, through the consultation, why conventional computers and non-cellular tablets were exempt. We do not have evidence at the moment that including them in the scope of the regime would significantly reduce risk. There is a mature anti-virus-software market that empowers customers to secure their own devices and, alongside this, mainstream operating system vendors already include security features in their services. As ever, we legislate in a way that we think is timely, appropriate and proportionate, trying to deal not with every single risk that one might envisage, but with those that are faced by consumers today. The result is that those devices are not subject to the same level of risk as others.

Let me turn to the point about Northern Ireland made by my hon. Friend the Member for Windsor and others. Customers across the UK will be able to benefit from the security protections that the regime aims to deliver. For selected product categories, honouring the UK's international commitments has necessitated that the regime will apply differently in Northern Ireland. I stress that, in practice, the exemption applies to limited types of products, such as lifts, pyrotechnic articles and personal watercraft, which are regulated already under legislation contained in the Windsor framework.

We are required to ensure the smooth flow of trade under the United Kingdom Internal Market Act 2020. The Prime Minister has also committed to ensuring smooth-flowing trade within the UK. The House should be reassured that the Government's position on that is unchanged. My hon. Friend the Member for South Thanet made another, equally important point that we need to ensure that that does not inadvertently allow in a flow of products that would not be compliant.

My hon. Friend the Member for Windsor asked about how we are dealing with automotive vehicles and the internet of things in cars. As we indicated in the April 2021 call for views on the regime, the Government intend to introduce separate regulation to cover the cyber-security of connectable automotive vehicles. To minimise an unnecessarily duplicative regulatory burden on industry, our position remains that cars should be exempted from these draft regulations, because we will be introducing a different framework. Developments in the legislative landscape have precluded the Government from including an exemption for connectable automotive vehicles in this, but we intend to bring forward that legislation as quickly as possible.

Chi Onwurah: Will the Minister give way?

George Freeman: I will finish these points, if I may.

[George Freeman]

On enforcement, astute colleagues have observed that it falls under the Department for Business and Trade. The previous Parliamentary Under-Secretary of State, the Minister for Small Business Consumers and Labour Markets, approved the recommendation for the OPSS to adopt the enforcement role for part 1 of the 2022 Act. The OPSS is part of the DBT and will therefore simply be enforcing the product security regime as the Secretary of State. It will begin enforcement functions as soon as the draft regulations come into force. To the question, I am reassured that the OPSS is properly resourced.

I have some final points. On the international aspect of the IOT security measures, the proportionality of implementing a given cyber-security measure for a product depends on a huge range of factors, from the product's technical architecture to the settings in which it is ultimately deployed in. The Government are therefore mindful of the risk of imposing obligations on businesses that may in many cases be disproportionate. The Chancellor of the Duchy of Lancaster and Deputy Prime Minister, and the National Cyber Security Centre are keeping an active watch on the importance of updating that.

On SME information, I am absolutely delighted to undertake that we will provide tailored information and guidance to assist small and micro-businesses. As colleagues have observed, they do not always have the relevant bandwidth to keep abreast of technology.

My hon. Friend the Member for South Thanet asked whether the self-certification and compliance mechanism—the duty placed on manufacturers—is sufficient to cover the risk. My answer to that would be that the draft statutory instrument is in our judgment the right place to start, but it is a start. We did not want to introduce heavy-handed legislation on day one, which would undermine business confidence and trigger huge fears in the industry. We wanted to start with something that everyone could at least acknowledge—our very important basic standards—then develop that, through consultation with the House, in a proportionate and agile way. I reinforce my comments on how that is a rather different approach from the EU one.

The hon. Member for Walthamstow made an important point about consumers. On the point about SMEs, we are actively engaging with consumer groups and we will ensure that any of their concerns are also reflected in our ongoing updates.

Stella Creasy: Will the Minister clarify a simple point? Would a consumer's guarantee be voided were they to use one of the items overseas, or if they brought an item here and used it on their connection, because there are now two different regimes?

George Freeman: The hon. Member makes an important point. Perhaps I could clarify that in my written note to all Members to follow up. I think everyone would be interested in the enforceability of consumer rights.

Chi Onwurah: I am sure the Committee will be pleased to know that I will not take up the Minister's provocation as to whether waiting 14 years to address security on the internet of things is a question of hindsight. Can the Minister clarify two points that I may have misunderstood? I heard him say that distributors did have a requirement on them to publicise the information about software upgrades. I may have misunderstood that because I thought it was only manufacturers who did.

More importantly, on cars, I think the Minister is saying that autonomous vehicles are exempted. I may have missed exactly where autonomous vehicles are exempted—it was not in the list of exemptions that I had. I am happy to take a clarification on that. Obviously, not all cars are autonomous vehicles, but is the assumption that any car that has an internet connection is in some way an autonomous vehicle?

George Freeman: All distributors already have a duty to ensure that the goods they are selling and distributing are legal. What we are doing is placing the onus on manufacturers. Distributors take their responsibility to consumers very seriously, and the vast majority will be very concerned and actively move to ensure they are not distributing illegal goods. It is not that there is not an onus on distributors; it is that we are implementing it via the mechanism.

On the point about cars, I did not want to mislead the House—I say this as the previous Minister for the future of transport—but we are in the process of putting together legislation on the digital vehicle and the internet of things in not just autonomous vehicles but smart and intelligent vehicles generally. It is to that process that we are deferring; this SI is not focused on that.

With that, I think I have addressed the points raised. I will happily write to the Committee, and if there are any points that I have not raised, Members should feel free to collar me between now and the picking up of my pen.

The Chair: We await the Minister's letter with huge anticipation and great excitement.

Question put and agree to.

Resolved,

That the Committee has considered the draft Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023.

6.47 pm

Committee rose.