House of Commons Library

Research Briefing

By Sarah Barber,
Georgina Hutton,
Adam Clark

25 October 2022

The Product Security and Telecommunications Infrastructure Bill

Summary

Image Credits

Adobe Stock 392757325 “Close up of hand touching smartwatch with health app on the screen, gadget for fitness active lifestyle” by sitthiphong (stock.adobe.com). Adobe Stock License / image cropped.

Disclaimer

Feedback

Every effort is made to ensure that the information contained in these publicly available briefings is correct at the time of publication. Readers should be aware however that briefings are not necessarily updated to reflect subsequent changes.

If you have any comments on our briefings please email papers@parliament.uk. Please note that authors are not always able to engage in discussions with members of the public who express opinions about the content of our research, although we will carefully consider and correct any factual errors.

You can read our feedback and complaints policy and our editorial policy at commonslibrary.parliament.uk. If you have general questions about the work of the House of Commons email hcenquiries@parliament.uk.

Contents

Summary

The Product Security and Telecommunications Infrastructure Bill would:

- Allow the Secretary of State to make regulations to introduce mandatory security requirements for consumer connectable products (also described as smart devices or internet of things (IoT) devices) sold in the UK; and
- Make changes to the electronic communications code which governs the rights of telecoms companies to install infrastructure on land.

Information about the Bill's stages and related publications is provided on the Parliamentary Bill page.

The Bill has had its Second Reading and Committee stage consideration. Following the agreement of a carry-over motion, the remaining Commons stages of the Bill are tabled for 25 May 2022.

Security requirements for consumer connectable products

Part One of the Bill relates to powers to introduce mandatory security requirements for consumer connectable products such as smart phones, smart TVs and connected speakers.

What are current safety and security requirements for smart devices?

Consumer connectable products are required to meet certain safety standards, but there are currently no mandatory security requirements. There is growing concern about the risks to consumers associated with some of these products, through breaches in safety and privacy and their potential for use in wider cyber-attacks.

The Government published a voluntary Code of Practice for Consumer IoT Security, in 2018. It provided manufacturers and others with guidance (13 principles) on good practice to ensure connectable products were secure.

In response to poor uptake of the Code of Practice and continued risks to consumers, the Government consulted in 2019 on introducing mandatory security requirements for connectable products. Legislative proposals were consulted on in 2020.

What would the Bill change?

The Bill would provide regulation-making powers for the Secretary of State to introduce security requirements for consumer connectable products sold in the UK.

The Government has said that it intends the following products to be affected by the Bill:

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

Some products would be excluded, such as smart meters, medical devices, vehicles and smart chargepoints (for electric vehicles).

The Government said it will use the powers under clause 1 of the Bill to introduce the top three guidelines from the Code of Practice:

- A ban on default passwords;
- A requirement for products to have a vulnerability disclosure policy whereby any security weakness in a product is identified and notified; and
- A requirement for transparency about the time period for which a manufacturer will provide security updates for the product.

It would also place duties on manufacturers, importers and distributers of these products to ensure compliance with the statutory requirements and to take action where a compliance failure has occurred.

The Bill sets out a number of enforcement measures that could be taken when there is a breach of compliance. For serious issues of non-compliance, the Bill sets the maximum penalty at £10 million or 4% of the company's worldwide revenue.

Changes to the electronic communications code (ECC)

Part Two of the Bill would make changes to the electronic communications code (ECC). The ECC is the main law that governs the rights of telecoms companies to install infrastructure on land, UK-wide.

Previous ECC reform

The ECC was significantly reformed in 2017. This included changes to rights to upgrade and share infrastructure and changes to dispute resolution processes. It also included changes to how land is valued when determining rent for hosting telecoms equipment under a court-imposed agreement.

Reforms to the ECC have always been highly contested, with often strongly opposing views between telecoms operators and site providers (landowners). The Government has to strike a difficult balance between ensuring digital connectivity is widely available while property rights are respected.

The land valuation reforms have been particularly controversial, with reports that rents for hosting telecoms equipment have reduced, in some cases dramatically. The ECC is said to be causing delays to infrastructure roll-out through lengthy negotiations and legal proceedings.

The Government's consultation that informed the Bill did not revisit the topic of land valuation.

What would the Bill change?

The Bill aims to encourage faster and more collaborative negotiations for the installation and maintenance of telecoms equipment on private land. The Government says this would help ensure the efficient roll-out of digital infrastructure such as gigabit-broadband and 5G.

The main changes the Bill would make include:

- New provisions to actively encourage alternative dispute resolution rather than legal proceedings where possible;
- Introducing a faster procedure to allow telecoms operators to get temporary rights to access and install infrastructure on land when an occupier is unresponsive;
- Giving telecoms operators rights to automatically upgrade and share equipment that was installed before 2017;
- Changes to the drafting of the ECC to clarify who can grant rights to host infrastructure on land in cases where infrastructure is already installed;
- Changes to the terms for renewing certain types of telecoms agreements that were in place before December 2017;

- Allowing a time period to be set for the court to resolve disputes on the renewal of code agreements; and
- Changes to what can be sought as temporary, interim orders while a telecoms infrastructure agreement is being renewed (for example, access rights in addition to rent payments).

Telecoms operators and site providers had opposing views on most of the above changes, with telecoms operators agreeing that changes should be made and most site providers disagreeing.

The Bill would apply to all of the UK.

Progress of the Bill

Commons stages

The Bill had its Second reading debate on 26 January 2022. The Secretary of State for Digital, Culture, Media and Sport, Nadine Dorries, introduced the Bill. She said that the Government had made significant progress to strengthen the UK's cyber security, but legislation was needed to protect from the harm posed by cyber criminals. There was cross party support for the provisions in Part One of the Bill, but some concerns raised that the Bill should have come sooner and could do more.

Nadine Dorries highlighted the importance of Part Two of the Bill to ensure that gigabit-broadband and 5G infrastructure can be rolled-out at pace. Many members highlighted issues with connectivity in their constituencies, and some raised concerns about rent reductions faced by landowners in their constituencies following the 2017 ECC reforms.

Part One of the Bill was not amended during Committee Stage. There was one proposed New Clause, and two Opposition amendments, one of which was moved to a division. Five Government amendments were made to Part Two of the Bill. They were all technical or consequential amendments to tidy the legislation and were passed without a vote. The Opposition tabled 5 amendments and two new clauses which did not pass.

Report stage took place on 25 May 2022. The Government moved a number of amendments, all of which were agreed without a vote. Of the opposition and backbench amendments that were moved at Report stage, one went to a division and was defeated. All of the amendments concerned Part Two of the Bill.

Lords stages

The Government made the following amendments to Part Two the Bill during its passage through the House of Lords.

- Clause 57 (definition of 'occupier') was removed from the Bill;

- New Clause 60 was added to the Bill. It would grant an automatic right to share and upgrade telecommunications equipment on telegraph poles;

- New Clause 66 was added to the Bill. It would grant the Secretary of State powers to prevent access rights under the ECC being granted to a telecoms operator if doing so would prejudice national security.

One opposition amendment was agreed on division:

- New Clause 76 was added to the Bill. It would require the Secretary of State to review the impact of the post-2017 reforms to the Electronic Communications Code.

The Government also introduced a series of amendments to Part One implementing some of the recommendations made by the Delegated Powers and Regulatory Reform Committee (DPRRC). They were agreed without a vote.

The changes to both parts of the Bill were all agreed at Report stage (section 4.2 below).

1 Part One: Safety requirements for connectable products

Part One of the Bill would provide regulation-making powers for the Secretary of State to introduce security requirements for certain consumer connectable products and places duties on manufacturers, importers and distributers with regards to these requirements.

An Impact Assessment of the product security half of the Bill was published on 24 November 2021.[1]

The Government has also published a factsheet on the product security elements of the Bill: The Product Security and Telecommunications Infrastructure (PSTI) Bill – product security factsheet.

1.1 Background: Concerns about security of connectable products

Consumer connectable products are any consumer products that can connect to a network or the internet and receive and transmit information. These products include smartphones, smart TVs and connected CCTV, alarm systems and baby monitors. These products may also be described as smart devices, or internet of things (IoT) devices. This briefing will refer to them as connectable products as this is the term used in the legislation.

While consumer connectable products must meet specific standards relating to product safety there are currently no minimum standards required for security.[2]

Insecure connectable products are vulnerable to a range of security threats. These include accessing personal information through a device, using a connectable product to access a wider network, and using a number of devices to undertake a larger cyber-attack. Examples of these are set out in the explanatory notes to the Bill, including a 2016 attack on Netflix and the BBC and 2017 and 2018 attacks that gained access to the information of around 1 million smart watch users:

1 DCMS, Impact Assessment: Regulation of consumer connectable product cyber security, 21 May 2021

2 For example, under the Consumer Protection Act 1987 and the General Product Safety Regulations 2005

> Insecure products can be used in ways not intended by the consumer, such as the case of security cameras being compromised in Singapore. In addition, insecure products can act as the 'point of entry' across a network, enabling attackers to access valuable information, such as the attackers who were able to access a US casino's customers' details via a connected thermometer in a fishtank.
>
> Devices can be compromised at scale as part of Distributed Denial of Service (DDOS) or 'botnet' attacks. For example, in 2016 cyber criminals compromised 300,000 products with the Mirai malware. The attackers utilised the collective computing power to successfully disrupt the service of many news and media websites including the BBC and Netflix. The Mirai malware was able to penetrate so many devices due to widespread weak security features (such as default passwords).
>
> In 2017 and 2018, a range of vulnerabilities were identified in the web service that connected to a smart watch brand that is marketed at children. The vulnerabilities allowed an attacker to access personally identifiable information including the linked mobile phone number and GPS coordinates for each watch. The penetration testers who had found the vulnerability were unable to contact the manufacturer to report their concerns meaning watch users - including children - continued to be exposed to harm. The total number of users of these smart watches was determined to be around 1 million globally.[3]

1.2 Measures to increase security

The increased use of these products and concerns about security were raised by the Government in the National Cyber Security Strategy in 2016. The strategy included an objective that most online products and services become "secure by default" by 2021:

> Consumers will be empowered to choose products and services that have built-in security as a default setting. Individuals can switch off these settings if they choose to do so but those consumers who wish to engage in cyberspace in the most secure way will be automatically protected.[4]

It said the Government would work with industry to ensure software and hardware is more "secure as default" and would explore ways of providing security information to consumers.[5]

Secure by Design report and the Code of Practice 2018

In March 2018, the Government published the Secure by Design report.[6] The report noted the opportunities offered by increased use of consumer

3 Product security and Telecommunications Infrastructure Bill: Explanatory notes
4 Cabinet Office, National Cyber Security Strategy 2016 to 2021, November 2016.
5 Cabinet Office, National Cyber Security Strategy 2016 to 2021, November 2016
6 DCMS, Secure by Design report, March 2018

connectable products but highlighted their lack of security provision. The report set out two risks associated with this:

- Risks to the privacy and safety of consumers; and
- the wider threat of large cyber attacks.

The report set out that the UK Government had "a duty of care to UK citizens to help ensure that they can access and use the internet safely." It called for greater action in the area and said there was "a need to move away from placing the burden on consumers to securely configure their devices and instead ensure that strong security is built in by design."[7]

A Code of Practice for Consumer IoT Security, developed through engagement with industry, was published alongside the report. It provided 13 guidelines for manufacturers and others, setting out good practice for ensuring that connectable products were secure. These guidelines included:

- Ensuring that consumer connectable products do not have universal default passwords when they are sold;
- Ensuring the period of time for which the security on products will be updated is made clear to the consumer; and that
- Manufacturers and others should implement a vulnerability disclosure policy to ensure that security vulnerabilities are monitored, identified, rectified and reported to stakeholders.[8]

At the time of the publication of the Secure by Design report, the Government said that its preference would be for "the market to solve this problem" but if this did not happen, it would look to introduce these measures through legislation.

In response to a parliamentary question in October 2018, the then Minister of State at the Department of Culture, Media and Sport, Margot James, set out that the Government's ambition was to achieve the best possible uptake of the Code, and that work had begun to place some parts of it on a regulatory footing:

> The guidelines within the Code of Practice bring together what is widely considered good practice in Internet of Things (IoT) security. As a voluntary document, it provides clarity to industry on the steps that are most important in protecting consumers' online security and privacy.
>
> We continue to welcome public pledges from manufacturers to implement the Code for their products, with two major companies having already made such a commitment. The Government's ambition is to achieve the best possible industry uptake of the Code and we will continue to monitor progress in this area. We remain in discussions with a number of manufacturers and are working towards securing additional industry pledges in the future.

7 DCMS, Secure by Design report, March 2018
8 DCMS, Code of Practice for Consumer IoT Security, March 2018

> The Government has also begun work to place appropriate aspects of the Code on a regulatory footing with further details to be shared in due course [...].[9]

Consultation on regulating product security (2019-2020)

In May 2019, the Government published a consultation on introducing a regulatory approach to connectable products' security. It sought views from manufacturers, retailers, and others in the industry.[10]

The consultation noted that consumer connectable products were widely used in the UK and internationally, but there was a lack of information for consumers on the safety of these products and a lack of incentive for industry to provide this information to consumers. It said that self-regulation had "not worked" and that owners of smart device companies were disincentivised by costs relating to supply chains:

> Moreover, companies who try investing resource into ensuring their products are secure can end up losing competitive advantage over their rivals.[11]

The document said that regulation would "force out the very worst practice we are seeing in the market" and that it was the "best lever available to influence industry to meet these requirements."

The Government published its response to the consultation in February 2020. This said that the Government intended to create primary legislation to give the Secretary of State the powers to introduce security requirements for devices on sale in the UK. These requirements would be introduced through secondary legislation.

The consultation response explained that, following feedback on making all the elements of the Code of Practice mandatory, it recognised the heavy burden this would place on industry. It said that after assessing the balance between protecting consumers and minimising the burden on industry, it concluded the top three guidelines from the Code of Practice should be the focus.

These were that:

1. IoT device passwords must be unique and not resettable to any universal factory setting
2. Manufacturers of IoT devices need to provide a vulnerability disclosure policy on how concerns about security can be reported

---

9 Written Question: UIN 180309, 16 October 2018 [Internet: Security]

10 DCMS, Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security, February 2020

11 DCMS, Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security, February 2020

3. Manufacturers of IoT devices need to explicitly state the minimum length of time that the product will receive security updates.[12]

The response said that these requirements were easier to test from an enforcement perspective and that meeting these would give consumers protection.

Consultation on legislative proposals (2020-2021)

In 2020, the Government launched a consultation on the detail of legislation to require minimum security standards in connectable products.

The consultation explained that the intentions of the legislation would be to ensure that no connectable product was supplied to a consumer without meeting the three security requirements (based on the top three in the Code of Practice).

In April 2021, the Government published its response to the consultation.

In a ministerial statement, the then Secretary of State for Culture, Media and Sport, Matt Warman, said that the Government would introduce legislation to protect consumers from insecure products. He said it would apply "to all consumer connected products such as smart speakers, smart televisions, connected doorbells, connected toys and smartphones, with some specific exemptions due to the specific circumstances of how certain devices are constructed, secured, and regulated, or the impact that regulating these products would have."

Matt Warman said the legislation would align with the 2018 Code of Practice and international standards and would therefore be familiar to manufacturers and others in the industry.[13]

The factsheet produced alongside the Bill reports that businesses will be given an appropriate time to adjust their practices before enforcement action will be taken against them under the legislation. It says that following Royal Assent of the Bill, the Government will allow "at least 12 months' notice" before the legislation comes into force. [14]

Reaction to the Bill

The Bill has generally been welcomed by industry and other stakeholders. The Technical Director of the National Cyber Security Centre, Dr Ian Levy said it

12 DCMS, Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security, February 2020

13 Statement UIN HCWS934, 21 April 2021 [Regulating Consumer Connected Product Cyber Security]

14 DCMS, The Product Security and Telecommunications Infrastructure (PSTI) Bill – product security factsheet, 24 November 2021

would "ensure the security of connected consumer devices and hold device manufacturers to account for upholding basic cyber security."[15]

Director of Policy and Advocacy at Which?, Rocio Concha, said the Bill needed to "be backed by strong enforcement to ensure people can get effective redress when they purchase devices that fail to meet security standards and leave them exposed to data breaches and scams."[16] Following a Which? investigation that "revealed just how easily hackers could access popular smart tech," the consumer organisation called for the Bill to be strengthened in three ways:

- **Online marketplaces:** previous Which? research has shown that many insecure products are sold via marketplaces, listing sites and auction sites, so the legislation must effectively cover everywhere that consumers buy smart products.

- **Update support minimums:** the legislation makes it law that manufacturers must tell consumers how long they will support a smart product when they buy it. However, we feel that it is necessary to go further and mandate how long different types of products should be supported as a minimum. Consumers should be able to use products for longer, and not dispose of them earlier than necessary.

- **Consumer rights:** If someone owns an insecure smart device, they should be able to argue that it is faulty and then get a refund or replacement as per their legal rights under the Consumer Rights Act 2015. This is currently not defined clearly enough, in our view, under the PSTI legislation as drafted.[17]

Others have also said the Bill does not go far enough and must be only the beginning of action in this area. Amanda Finch, CEO of the Chartered Institute of Information Security, said that attackers will find ways to circumvent the measures in the Bill, and that it "has to be seen as one step in an endless process of review and refinement, rather than an end in itself."[18]

Professor George Loukas, professor of cyber security at the University of Greenwich, noted in evidence to the DCMS Committee that the Bill, and the security requirements the Government is proposing to introduce through secondary legislation, focus on devices rather than the human element. The vast majority of cyber security breaches, he said, involve "an element of human deception." He argued that manufacturers could do more to inform customers about the types of security risk their devices are secure against,

15 DCMS, Press release: New cyber laws to protect people's personal tech from hackers, 24 November 2021

16 Which? Which? response to Product Security and Telecommunications Infrastructure Bill unveiled in Queen's Speech, 11 May 2021

17 Which?, Smart products from the biggest tech brands easily hacked in Which? tests, 1 June 2022.

18 Is the UK government's new IoT cybersecurity bill fit for purpose? | TechCrunch

and about how to safely dispose of a connected product that is no longer supported.[19]

However, there are also worries about the added burden of the regulation for manufacturers of these products.

Martin Tyley, head of Cyber at KPMG said the Bill added extra regulations which could "overwhelm" manufacturers and noted that most impact may be on smaller companies. He said that all cyber security regulation should be accompanied by guidance and support for the industry.[20]

1.3 The Bill

This section provides a brief overview of the contents of Part One of the Bill. A more detailed description of the Clauses in the Bill is provided in the Explanatory Notes produced by the Government.

The clause numbers in this section refer to the Bill as amended on Report in the House of Lords.

Clauses 1-3: Security requirements

Clause 1 would provide regulation-making powers for the Secretary of State to introduce requirements to improve the security of connectable products sold in the UK. It states that a security requirement is one that relates to a relevant connectable product and applies to 'relevant' people, meaning a manufacturer, importer or distributor of a product.

The Clause does not specify the security requirements that will be included in the regulations. The Government has said that it will use the powers under Clause 1 to introduce the top three guidelines from the Code of Practice for consumer IoT products:

- A ban on default passwords;
- A requirement for products to have a vulnerability disclosure policy whereby any security weakness in a product is identified and notified; and
- A requirement for transparency about the time period for which a manufacturer will provide security updates for the product.[21]

Clause 2 would make further provisions about the regulations that may be made under Clause 1. Specifically, it provides that:

---

19 DCMS Committee, Oral evidence: Connected tech: smart or sinister?, HC 157, 11 October 2022, Q87-90.

20 UK introduces PSTI bill to protect IoT devices (iottechnews.com)

21 DCMS, The Product Security and Telecommunications Infrastructure (PSTI) Bill – product security factsheet, 24 November 2021

- a requirement may relate to 'all' the relevant products of a relevant person;
- a security requirement made in regulations may be ongoing and require action in respect of a product that is already on the market in the UK; and
- clarifies that regulations made under Clause 1 would be subject to the affirmative resolution, unless they only make very limited changes, such as altering a term used without altering the meaning of the security requirement.

Clause 3 would provide that regulations may be made to establish that a person who meets certain conditions (such as an international standard) would be treated as meeting the security requirements made under Clause 1. The Explanatory notes explain that the security requirements set out in regulations will be the minimum mandatory standards. However, some people may wish to exceed these and meet international standards for security, such as the EN 303 645. In these cases, the Secretary of State may specify that those meeting specific standards would be deemed to have met the security requirements.

Regulations made under Clause 3 would be subject to the affirmative resolution procedure.

Clause 4-6: Relevant products

Relevant products that may be subject to security requirements are defined in Clauses 4-6.

Clause 4 would provide that a relevant product is an "an internet-connectable product" or a "network-connectable product," and is not an excepted product as set out in the Bill.

Clause 5 defines an "internet-connectable product" as one that can connect to the internet. It defines a "network-connectable product" as a product that is capable of sending and receiving data, is not connected to the internet but meets one of two connectability conditions which relate to the products' ability to connect to other products that may connect to the internet.

More detail on the connectability conditions is provided in the Explanatory notes to the Bill:

> Subsection (4) establishes the first connectability condition where a product is capable of connecting directly to an internet-connectable product by means of a communication protocol that forms part of the Internet Protocol suite. To meet this condition, these products must be capable of using a communication protocol that forms part of the Internet Protocol suite, but itself unable to connect directly to the internet.
>
> Subsection (5) establishes the second connectability condition which covers the capability of a product connecting directly to two or more products at the same time by a communication protocol that does not form part of the Internet Protocol suite; and it being capable of connecting directly to an internet-

> connectable product by means of a communication protocol which does not form part of the Internet Protocol suite, whether or not at the same time as it connects to any other product.[22]

The Government has said that it intends the following products to be relevant products under the Bill:

- smartphones
- connected cameras, TVs and speakers
- connected children's toys and baby monitors
- connected safety-relevant products such as smoke detectors and door locks
- Internet of Things base stations and hubs to which multiple devices connect
- wearable connected fitness trackers
- outdoor leisure products, such as handheld connected GPS devices that are not wearables
- connected home automation and alarm systems
- connected appliances, such as washing machines and fridges
- smart home assistants.[23]

Some products would be excluded, such as smart meters, medical devices, vehicles and smart chargepoints.[24]

Clause 6 would establish regulation-making powers for the Secretary of State to set out which products are not considered relevant products for regulations made under Clause 1. Regulations made under Clause 6 are subject to the affirmative resolution procedure unless they make minor variations.

Clause 7: Relevant persons

Clause 7 would define the "relevant persons" to which the regulations made under Clause 1 would apply, as manufacturers, importers and distributers of a product. Under Clause 7(6), a person would not be a relevant person for the purposes of the Bill if they simply install the product as part of building works. The explanatory notes provide examples of excepted persons, such as an electrician installing a "smart" sound system in a home where they are only

22 Product security and Telecommunications Infrastructure Bill: Explanatory notes

23 DCMS, The Product Security and Telecommunications Infrastructure (PSTI) Bill – product security factsheet, 24 November 2021

24 Product security and Telecommunications Infrastructure Bill: Explanatory notes

responsible for the installation and have not been involved with purchase or supply of the product.

Clauses 8-25: Duties of relevant persons

Clause 8 would establish a duty for a manufacturer to comply with security requirements relating to a product, where that product is available on the market in the UK, and the manufacturer is or should be aware of this. This duty continues to apply when a product is on the market and is being used by consumers.

Clause 9 would establish that a manufacturer must make a certificate of compliance available with the connectable product and sets out what information must be provided on this certificate. It would also provide regulation-making powers for the Secretary of State to set out further details on certificates of compliance.

Clause 10 and 11 would place a duty on manufacturers of products to investigate potential compliance failures and act where this is identified. The manufacturer must take all reasonable action to prevent the product being available for sale and remedy the compliance failure.

In addition, the manufacturer must notify the enforcement authority about any compliance failure and any other manufacturers, distributers and importers of the product. Where specified conditions are met, they must also inform any customer to which the product was supplied about the compliance failure. Clause 11 provides powers for the Secretary of State to make regulations to specify these conditions. These regulations would be made under the negative resolution procedure.

Clause 11 also sets out what information must be provided by the manufacturer about the compliance failure, Specifically:

- Details of the compliance failure;
- Any risks posed by the failures; and
- Action taken to remedy the compliance failure and whether these have been successful

Clause 12 would impose a duty on manufacturers to maintain records of any investigations into a compliance failure of a product, and any compliance failures. Clause 12 includes more detail on what these records must include.

Clause 13 would mean that a manufacturer that is not based in the UK may nominate an authorised person to perform its duties under the legislation.

Clauses 14-19 would place duties on importers of a connectable product that are equivalent to those on a manufacturer. It would require importers to comply with security requirements as they apply to them. Clause 19 would require that if an importer becomes aware of a manufacturer's compliance failure, they must contact the manufacturer about this as soon as possible. If it appears that action is not being taken to remedy the compliance failure,

the importer must take action to prevent the product being sold to consumers in the UK.

Clauses 21-25 would place duties on a distributer that are equivalent to those on an importer.

Clauses 26-52: Enforcement

Under Clause 26, the Secretary of State would be responsible for enforcing the measures contained in Part One of the Bill, and, Schedule 5 of the Consumer Rights Act 2015 would be amended to make available powers of investigation. However, under Clause 27 the Secretary of State may, by regulations, delegate these enforcement powers. In the Bill as introduced, the Secretary of State would have been able to delegate the enforcement function by agreement rather than by regulations. This was amended during the Lords report stage. Regulations under Clause 27 would be made under the affirmative procedure.

Lord Kamall (Parliamentary Under-Secretary of State, Department for Digital, Culture, Media and Sport) confirmed during the Lords Report stage debate that the Government intended to appoint the Office of Product Safety and Standards, part of BEIS, as the enforcement authority. He said that due to the Carltona principle (which permits civil servants to act as the Secretary of State) the Government would not be required to introduce regulations under Clause 27.[25]

Clauses 28 to 47 set out the following enforcement powers:

- Clause 28 would establish that the Secretary of State may issue a compliance notice where there are reasonable grounds to believe that a person has not complied with a requirement.

- Clause 29 would provide that the Secretary of State may issue a stop notice where there are reasonable grounds to believe that a person is carrying on an activity that is in breach of a relevant duty.

- Clause 30 would provide that the Secretary of State may issue a recall notice to a manufacturer, where the Secretary of State has reasonable grounds to believe that there is a compliance failure, any action to address it is inadequate, and they consider that a compliance notice, stop notice, or forfeiture of the product would be sufficient to deal with the compliance failure.

- Clause 31 would provide that a person who fails to comply with an enforcement notice would be liable for a fine. These fines are different in different nations of the UK.

[25] HL Deb 12 October 2022 vol 824 c796

- Causes 36 would make provision for the issuing of a penalty notice by the Secretary of State where, on the balance of probabilities, it is believed that a person has failed to comply with a duty.

- Clause 38 sets out that the maximum penalty is £10 million or 4% of a person's qualifying worldwide revenue. Powers under this clause allow the Secretary of State to set out how the revenue would be assessed.

- Clauses 45 and 46 would give the Secretary of State powers to inform the public about compliance failures and the power to publish details of any enforcement action against relevant persons.

- Clause 47 would give the Secretary of State powers to recall products where a recall notice has not been complied with.

As a safeguard, Clauses 33-35 make provision for appeals against enforcement notices and compensation for those to whom an enforcement notice has been wrongly issued.

In addition, Clause 42-45 would set out the conditions under which the Secretary of State may apply to the Courts for forfeiture of products. Clause 43 would clarify the process for applying for an order of forfeiture, and Clause 44 would provide an appeals process.

Finally, the Secretary of State would have the power under Clause 53 to issue guidance on new statutory security requirements for relevant products.

2 Part Two: Telecommunications infrastructure

Part Two of the Bill would make changes to the electronic communications code (ECC or the Code). The ECC is the main law that governs the rights of telecoms companies to install infrastructure on land. The ECC is contained in Schedule 3A to the Communications Act 2003 (as amended) and applies UK wide.

The Government has published a factsheet, Explanatory Notes and a De Minimis Impact Assessment for this part of the Bill.

The changes in Part Two of the Bill would come into force on a date set out by the Secretary of State in Regulations.[26]

2.1 Background: Digital infrastructure roll-out

Ensuring the wide availability of high-speed broadband and mobile infrastructure is a central part of the Government's National Infrastructure Strategy and levelling up agenda.

The UK Government has set the following targets for gigabit-capable broadband and mobile network coverage:

- a minimum of 85% of UK premises to have gigabit-capable broadband coverage by 2025;[27]
- 95% of the UK's geographic landmass to have 4G coverage from at least one mobile network operator by 2025; and
- a majority of the population to have 5G signal by 2027.[28]

The Library briefings on Gigabit-broadband in the UK: Government policy and targets and 5G provide more information on these targets, including a glossary of technical terms.[29]

[26] Clause 80 of the Bill (as amended on Report in the House of Lords).

[27] HM Treasury, National Infrastructure Strategy, 25 November 2020

[28] DCMS, Future Telecoms Infrastructure Review, 23 July 2018; DCMS, Shared Rural Network, 9 March 2020.

[29] Gigabit-broadband in the UK: Government policy and targets (CBP 8392, 21 December 2021) and 5G (CBP 7783, 6 November 2019)

As of January 2022: 66% of UK homes had access to gigabit-capable broadband according to telecoms regulator, Ofcom.[30] The Library's broadband data dashboard allows users to explore where these premises are by Parliamentary constituency.[31]

Telecommunications networks in the UK are rolled-out by private companies, referred to as "operators". Enabling the fast and cost-effective roll-out of new infrastructure by industry operators is an important policy objective for the Government to achieve the above targets.

The changes brought in this part of the Bill aim to address one area where telecoms operators say they face barriers to building infrastructure: delays getting access rights to land.

2.2 Electronic Communications Code (ECC)

What is the ECC?

In short, the ECC gives designated network operators rights, called 'code rights' to install, operate, maintain and/or upgrade electronic communications infrastructure (such as mobile masts or fibre broadband cables) on private and public land.[32]

Operators can only receive code rights through a written agreement between the occupier of the land (usually the landowner, also called the 'site provider') and the telecoms operator. These agreements – called a code agreement – are usually entered into consensually by negotiation. Ofcom has published a Code of Practice to provide guidance on what the parties should expect from each other when negotiating agreements.[33]

If an agreement cannot be agreed consensually, the operator can apply to the court for an order to impose an agreement. Part 4 of the ECC sets out the circumstances in which a court can make a code rights order, and how compensation for site providers should be determined.

30 Ofcom, Connected Nations: Spring Update, 20 May 2022.

31 Commons Library data dashboard, Constituency data: broadband coverage and speeds.

32 Designated operators are those that have been granted Code Powers (called Code Operators) by Ofcom, following a public consultation. Ofcom publishes a Register of operators with powers under the ECC which can be consulted for specific companies.

33 Ofcom is required to publish the Code of Practice and example standard terms of agreement under paragraph 103 of the ECC, however the Code of Practice is not binding on the parties to a negotiation.

2017 reforms

The ECC was significantly reformed in 2017.[34] One important reform was the way that rent for hosting telecoms equipment on land is calculated when the court is imposing an agreement under the ECC.

Rent is now determined based on the value of the land to the site provider, that is, without taking account of its value as a telecoms site (this is called the "no network assumption" or "no scheme" valuation approach).

Other changes to the ECC in 2017 included reforms intended to allow telecoms companies to automatically upgrade existing infrastructure and changes to dispute resolution procedures.

The 2017 reforms to land valuation has, in some cases, led to a dramatic reduction in rents for hosting infrastructure.[35] Commentators have noted one consequence of reduced rents is that site providers are less willing to engage with operators, resulting in delays to rolling out infrastructure.[36] This is particularly the case for rents for hosting mobile masts on land. The Centre for Policy Studies, following a survey of the telecoms industry, estimated 80% of negotiations were taking over six months to complete, and that the average time for negotiations was 11 months.[37]

There have been several court cases on the interpretation of parts of the reformed ECC. These have looked at the right to upgrade and share apparatus and the renewal of code rights following an expired agreement, amongst other issues. [38] Lawyers have said the drafting has created "frustration and confusion" among stakeholders.[39]

The issue is highly polarised between the mobile industry and property owner stakeholder groups, with accusations of aggressive or vexatious behaviour on both sides.[40] Both groups have highlighted the benefits of digital connectivity to the economy and society and the need for reforms to the Code to avoid delays to infrastructure roll-out.

---

34 The reforms were implemented by the Digital Economy Act 2017.

35 Phone masts: Landowners call for rethink on rents, BBC News, 22 June 2021; Telecoms Disputes Over Wayleaves, Rents Threaten to Become Toxic, Mark Jackson, ISP Review, 17 December 2018, accessed 17 January 2022.

36 Centre for Cities, Delivering change How cities can make the most of digital connections, Simon Jeffrey and Lahari Ramuni, July 2018.

37 Upwardly Mobile: How the UK can gain the full benefits of the 5G revolution, 1 October 2021.

38 Ashurst, The Electronic Communications Code - Are changes afoot?, 4 February 2021.

39 Shoosmiths, Consultation announced on changes to the Electronic Communications Code, 4 February 2021; Property Litigation Association, Andrew Walker QC – Code operators as occupiers under the Electronic Communications Code – Solving the conundrum of Compton Beauchamp, 24 August 2020.

40 Phone masts: Landowners call for rethink on rents, BBC News, 22 June 2021; Centre for Policy Studies, Upwardly Mobile: How the UK can gain the full benefits of the 5G revolution, 1 October 2021

More information about the ECC and the 2017 reforms can be found in the Library briefing, Building broadband and mobile infrastructure (section 3).

2.3 ECC reforms: 2021

Government consultation

In January 2021, the Government opened a consultation on potential reforms to the ECC.[41]

The Government identified three main areas it sought to address in the ECC reforms:

- Obtaining and using code agreements.
- Rights to upgrade and share equipment.
- Renewing expired agreements.[42]

The consultation **did not revisit** the issue of land valuation and compensation for site providers which was reformed in 2017.

The Government said it recognised that the valuation reforms had affected the willingness of site providers to agree or renew agreements. However, it said it did not think disagreements about financial terms were the "only reason that negotiations were not progressing as smoothly as they could be". Instead, the Government said the options put forward in the consultation aimed to "help foster more collaborative relationships between parties".[43]

Stakeholder comment on proposed ECC reforms

Reforms to the ECC have always been highly contested.[44] The Government has to strike a difficult balance between ensuring digital connectivity is widely available while property rights are respected.

Both the telecoms industry and property owner organisations have campaigned on the new proposals for reform. For example:

- Speed Up Britain is a "cross-industry, non-partisan organisation campaigning for better mobile connectivity in every part of the UK". It says that the 2017 ECC reforms have "encouraged disagreements" and

41 DCMS, Consultation on changes to the Electronic Communications Code 27 January 2021; press release: Government reviews law on access to land for digital infrastructure.

42 DCMS, Consultation on changes to the Electronic Communications Code, 27 January 2021, paragraph 1.18.

43 DCMS, Consultation on changes to the Electronic Communications Code, 27 January 2021, paragraph 2.14.

44 The 2017 reforms followed several years of consultation and review, including several previous unsuccessful attempts at reform. For background information, see the Library briefing paper: Reforming the Electronic Communications Code,CBP-7203, 1 June 2016.

led to "lengthy legal proceedings" causing delays to the roll-out and upgrades of existing telecoms sites. It calls on the Government to make changes to the ECC including to allow enable upgrading and sharing of sites and to allow an efficient renewal process for expired pre-code agreements. It argues that although rents have fallen, in most cases the telecoms industry offered more in rental payments than the valuation framework required.[45]

- Protect and Connect is a campaign group led by land and property owners who lease their land to telecoms companies, including small farmers, churches and community groups. It is funded by AP Wireless (a large telecoms lease management firm).[46] Protect and Connect argues that telecoms operators are using the reformed ECC to push down rents such that small businesses property owners are not getting a "fair deal". It is calling for the Government to reconsider the 'no scheme' valuation approach, which they say is balanced too heavily in favour of operators.

The British Property Federation published a briefing note setting out reforms its members would like to see aside from changes to the valuation framework, including 'lift and shift' provisions to allow for the relocation of equipment, and an industry standard on the likely type and levels of compensation.[47]

The All-Party Parliamentary Group for Broadband and Digital Connectivity ran an inquiry in the summer of 2021 looking at how reforms to the Code could facilitate fixed-line broadband infrastructure (as opposed to mobile infrastructure).[48] It recommended that the ECC should distinguish between mobile and broadband infrastructure and that standardised template agreements and fee structures for fixed-broadband could speed up negotiations with site providers.[49]

The Law Society said the Government's proposals for ECC reform focus more on "symptoms" of the problems encountered, rather than addressing the "root causes". It said this stemmed from the balance of rights in the ECC being "too heavily in favour of operators".[50] The Society said changes to dispute resolution procedures and adjustments to some code provisions would only provide "part of the answer".

Government's response

The Government's response to the consultation was published in November 2021.

---

45 PBC Deb 15 March 2022, c46.

46 PBC Deb 15 March 2022, c11.

47 BPF, Property owner perspectives on the Electronic Communications Code (ECC), June 2021, accessed 15 December 2021.

48 APPG for Broadband and Digital Connectivity, #BetterBroadband inquiry [accessed 19 January 2021]

49 Letter from Selaine Saxby MP (Chair of APPG for Broadband and Digital Connectivity) to Secretary of State for DCMS on #BetterBroadband inquiry findings.

50 The Law Society, Changes to the Electronic Communications Code – Law Society response, 20 April 2021.

The Government said many stakeholders raised compensation as a major issue affecting negotiations on code rights. The Government reiterated that it did not intend to revisit the valuation framework contained in the Code and that its policy position remained the same:

> ...that the statutory valuation framework which underpins negotiations ... remains appropriate for the installation and maintenance of digital communications infrastructure systems.[51]

The Government pointed to the importance of good digital networks to be widely available and noted the valuation framework is in line with the situation for other utilities.

Following the consultation, the main changes which would be implemented by the Bill include:

- New provisions to actively encourage **alternative dispute resolution** rather than legal proceedings where possible;
- Introducing a new procedure to allow operators to get **temporary rights to access land** in circumstances where an occupier is unresponsive;
- Changes to drafting regarding the **renewal of expired agreements**;
- Changes to rights to **automatically upgrade and share apparatus** for infrastructure installed before 2017;
- Changes to allow a **timescale for court proceedings** for disputes on code agreement renewals; and Changes to what can be sought as temporary, interim orders while a code agreement is being renewed (for example, access rights in addition to rent payments).

The Government says its proposed reforms aim to strike an "appropriate balance" between facilitating the delivery of digital networks in the wider public interest and the private property rights of landowners.[52]

Stakeholder comment on the Bill

The Government's response to its consultation on proposed changes said that property owners and telecoms operators had opposing views on almost all the proposed changes, including those made in the Bill.

Mobile industry stakeholders have welcomed the proposed changes in the Bill, saying it will allow operators to speed-up roll-out of digital infrastructure.[53] Property owner campaign group, Protect and Connect, were disappointed the Government had not changed its position on valuation,

51 DCMS, Consultation on changes to the Electronic Communications Code - government response, 24 November 2021, paragraph 1.14.

52 DCMS, Consultation on changes to the Electronic Communications Code - government response, 24 November 2021, paragraph 2.5.

53 Speed Up Britain - Electronic Communications Code Progress, Mobile UK, 13 January 2021.

arguing that sticking to this approach would continue to delay infrastructure roll-out.[54]

A lawyer at Pinsent Masons, Michael Smith, commented that although telecoms operators and site providers may have opposing views, the Bill should:

> ...provide the legal certainty and improved mechanisms sorely needed to encourage greater collaboration over the delivery of the digital infrastructure UK businesses need to thrive in a global economy.[55]

2.4 The Bill

This section provides a brief overview of the contents of Part Two of the Bill. A more detailed description of the Clauses in the Bill is provided in the Explanatory Notes produced by the Government.

The clause numbers in this section refer to the Bill as amended on Report in the House of Lords.

Clauses 57–60 – Rights to upgrade and share

Clauses 57 to 60 concern sharing of telecoms equipment installed under a code agreement.

Two examples of where the automatic right to upgrade equipment is important for operators are:

- For the roll-out of 5G networks, which are largely installed on-top of existing masts.
- For fixed-line broadband, upgrading and sharing rights are often needed to utilise the existing underground tunnels (ducts) and poles that already host cables, to replace these with upgraded fibre-optic cables. Many of these ducts and poles were installed for the purpose of telephone landlines, and it can be difficult to trace access agreements over such a long time.[56]

Currently, under paragraph 17 of the ECC, operators with code rights can automatically upgrade their equipment and share it with other operators, provided the upgrading and sharing has no more than a "minimal adverse impact" on the appearance of the apparatus and imposes "no additional burden" on the site provider.

---

54 Campaigners outraged as government rejects mobile phone mast overhaul, CityAM, 25 November 2021.

55 Code reforms can bolster UK digital connectivity, Michael Smith, Pinsent Masons, 5 January 2022.

56 DCMS, Consultation on changes to the Electronic Communications Code - government response, 24 November 2021, para 4.25.

Clause 57 in the Bill as introduced would have amended the definition of 'occupier' in the ECC. The Clause was removed at the Lords Report stage following a Supreme Court judgement. See section 4.2 for more information.

This automatic right to upgrade and share in paragraph 17 was introduced as part of the 2017 ECC reforms and currently only applies to agreements entered into after this date. The Government's response to its consultation said an estimated 80% of the UK's telecommunications networks were installed prior to the 2017 ECC reforms.[57]

The Government's consultation on the ECC reforms heard that it was unclear whether the court could impose conditions exceeding those in paragraph 17, particularly in relation to sharing.[58] Rights to upgrade can already be imposed as a separate code right (paragraph 3) but sharing is not listed as a separate right.

Clause 57 would add the right to share as a separate code right that could be agreed or imposed by a court. It would also amend various parts of the Code to reflect this change.

Clauses 58–59 would extend automatic rights to upgrade and share contained in paragraph 17 to apply retrospectively to code agreements entered into before 2017.

The retrospective change would apply in the following limited circumstances:

- For apparatus installed underground.
- Where the upgrading and sharing would have no adverse impact on the land.
- Where the upgrading and sharing would impose no burden on any person with an interest in the land.
- Where the activity required to upgrade or share can be carried out without accessing private land, unless such an access agreement is already in place. This condition applies because the right to share does not include a right of access – that right would require a new separate code agreement.

Clause 59 would enable the automatic right to upgrade and share to also apply to apparatus installed prior to 2003 (before the Code came into force) for which there may not be documentation evidencing a code agreement.

In response to the Government's consultation, some site providers, including responses from emergency services, raised concerns about possible implications for health and safety requirements at their sites due to the potential for telecoms equipment to interfere with services' own equipment.[59] Some professional bodies raised concerns about implications for contract law

57 DCMS, Consultation on changes to the Electronic Communications Code - government response, 24 November 2021, para 4.23.

58 DCMS, Consultation on changes to the Electronic Communications Code - government response, 24 November 2021, para 4.15.

59 DCMS, Consultation on changes to the Electronic Communications Code - government response, 24 November 2021, para 4.29.

and believed the commercial relationship was better served by negotiations between operators and site providers.[60]

Clause 60, added by the Government at Lords Report stage, would extend operators' rights with regards to equipment on and between telegraph poles on private land.

Currently the Part 11 of the Code grants operators rights to "fly lines" between telegraph poles. However, it does not permit operators to upgrade equipment on the pole (for example running a fibre optic cable from the base to the top). Nor does it permit operators to share poles with other operators. In evidence to the Public Bill Committee, industry figures said these restrictions limited their ability to roll out gigabit broadband infrastructure, especially in rural areas and Scotland where overheard cables are more common.[61]

Clause 60 would grant both rights. In order to protect the interests of landowners and occupiers, exercise of the new rights must not have more than a minimal adverse impact on the appearance of the pole or on the land. Any works involved must not cause loss, damage, or expense to any person with an interest in the land.

Clause 61–65 – Renewal of expired agreements

These clauses apply to England and Wales or Northern Ireland only.

In short, clauses 61-65 would make changes such that all code agreements, including those made before the 2017 Code came into force, when renewed by a court order would be renewed on land valuation terms consistent with the 2017 Code.

Background

One issue arising out of the 2017 reforms has been the treatment of certain expired code agreements that are up for renewal. When a code agreement expires, the rights contained in that agreement normally remain in place until the agreement is formally terminated or is renewed by the parties by entering into a new agreement (either consensually or imposed by the court).[62]

In general, the ECC reforms introduced in 2017 did not apply retrospectively. For example, new rights contained in the 2017 Code, such as the automatic right to upgrade and share, would only apply to code agreements entered into after 2017. However, whether the 2017 Code (such as the new land valuation framework) can apply when renewing agreements that were made

60 DCMS, Consultation on changes to the Electronic Communications Code - government response, 24 November 2021, para 4.27.

61 PBC Deb 15 March 2022 (second sitting), c40-41. See also techUK, The FTIR: Fit to deliver for 5G and full fibre four years on?, October 2022, p12.

62 DCMS, Consultation on changes to the Electronic Communications Code - government response, 24 November 2021, para 5.1

before the Code came into force (28 December 2017) and continued after (called a "**subsisting agreement**"), is more complicated.[63]

The 2017 Code introduced provisions regarding the termination and renewal of code agreements. Part 5 provides in cases where a renewal agreement is imposed by a court order, the land valuation framework contained in Part 4 of the Code applies.[64] However, Part 5 does not cover all code agreements. In particular, subsisting agreements protected by security of tenure provisions under the Landlord and Tenant Act 1954 in England and Wales (the 1954 Act) and equivalent legislation in Northern Ireland, are excluded.[65] There is no equivalent legislation in Scotland: all expired code agreements are subject to Part 5.

Since the 2017 reforms there have been several court cases on the interaction between the 1954 Act and the Code, and in particular, how agreements not covered by Part 5 should be treated on expiry.[66] The Government's consultation response said there continues to be uncertainty about how operators can renew these agreements and/or obtain new code rights.[67]

The Government said this uncertainty "does not reflect the policy aims of the 2017 reforms". The Government believes all code agreements – including all new and renewal agreements – should reflect the new Code. The Government's consultation response explained the current procedure for renewing agreements was creating particular problems for mobile networks:

> For instance, one operator is preparing to add 5G equipment to almost half of their 14,000 sites with others preparing to upgrade existing 4G sites to make them 5G ready. It is important that, when Code agreements for existing sites expire, or are about to expire, operators are able to renew those agreements quickly and in accordance with the reformed Code framework (including paragraph 17 rights to upgrade and share apparatus) in order to optimise the use of existing sites and adapt 4G networks to 5G.[68]

---

63 Transitional provisions for agreements entered into before 2017 are set out in Schedule 2 of the Digital Economy Act 2017; a "subsisting agreement" is defined in paragraph 1(4).

64 Explanatory Notes (PDF), para 250.

65 The 1954 Act provides business tenants with the right to 'security of tenure'. This means that once a lease has expired, the tenant has the right to remain in occupation and a right to renew the lease (subject to statutory grounds for refusal). It is possible to 'contract out' of these provisions, by an agreement under section 38A of the 1954 Act. Only subsisting code agreements that are leases under the 1954 Act and which are protected by security of tenure (that is, there has been no agreement under section 38A to contract out) are excluded from Part 5 of the 2017 Code on renewal. The equivalent legislation in Northern Ireland is the Business Tenancies Order (Northern Ireland) 1996 (BTO 1996).

66 For example, *Cornerstone Telecommunications Infrastructure Ltd v Ashloch Ltd and another* [2021] EWCA Civ 90 and *Arqiva Services Ltd v AP Wireless II (UK) Ltd* [2020] UKUT 0195 (LC). See for commentary:

67 DCMS, Consultation on changes to the Electronic Communications Code - government response, 24 November 2021, para 5.3.

68 DCMS, Consultation on changes to the Electronic Communications Code - government response, 24 November 2021, para 5.6.

Clauses 61–65

Clauses 61–65 would make changes such that the procedure and terms for the renewal of code agreements not covered by Part 5 would be "more closely aligned" to Part 5, where the main aim of that agreement is to confer code rights.[69] This means all code agreements renewed by a court order would be renewed under terms that mirror the 2017 land valuation framework.

The Government's consultation response said stakeholders were divided on these changes.[70] Most telecoms operators thought Part 5 should be available to all expired code agreements, whereas most site providers disagreed, particularly given the impact this would have on rent payments for renewed agreements. See Section 1.2 above for background on the valuation framework under the 2017 Code.

These changes are introduced through the addition of new sections to the Landlord and Tenant Act 1954 (1954 Act) and the Business Tenancies Order (Northern Ireland) 1996 (BTO 1996) to provide where:

- a tenancy is renewed under the 1954 Act or BTO 1996; and
- that lease is a subsisting code agreement; and
- the primary purpose of that agreement is to grant code rights,

Any financial terms of the renewal would be determined by reference to provisions mirroring paragraph 24 of the 2017 Code (which sets out the valuation framework for all new code agreements entered into after 2017).

Clauses 63 and 64 would amend the 1954 Act and BTO 1996 to add provisions mirroring the Code regarding the rights of a site provider to claim for loss or damage caused by an operator exercising code rights (paragraph 25 of the Code).

Clause 65 would transfer jurisdiction for the resolution of disputes regarding telecoms renewal agreements under the 1954 Act from the County Court to the First-tier and Upper Tribunal, which are the courts that deal with all other code disputes. This change is not needed for Northern Ireland as disputes under the BTO 1996 are already heard in the Lands Tribunal, the same court as for code disputes.

Clause 66 – national security

Clause 66, added by the Government at Lords Report stage, would grant the Secretary of State powers to require courts to refuse an application for Code Rights in circumstances where imposing an agreement would be likely to prejudice national security, defence, or law enforcement. The Government

69 DCMS, Consultation on changes to the Electronic Communications Code - government response, 24 November 2021, para 5.10.

70 DCMS, Consultation on changes to the Electronic Communications Code - government response, 24 November 2021, para 5.7–5.7.

explained that this power is needed to prevent telecoms operators being granted access to sensitive sites without the landowner's consent.

The Government said that use of the power will be considered only when all consensual options have been exhausted:

> It is worth emphasising that it will not provide public sector landowners with national security law enforcement and defence equities with a blanket exemption. It is anticipated that it would be employed only rarely, on a case-by-case basis and in extremis, and that only a small number of sites would be eligible. Nevertheless, we will consider how Parliament can be updated on the use of this power so that it can carry out its scrutiny role effectively.[71]

Clause 67 – Unresponsive operators

Clause 67 would introduce a new Part 4AZ into the Code, setting out a new procedure for operators to gain temporary code rights to access land in circumstances where a site provider (called the 'required grantor') does not respond to repeated requests for access.

The Government explained that it important for operators to have timely access to land as delays can lead to premises being 'de scoped' from an operator's roll-out and left without a connection:

> Non-responsive occupiers and landowners can slow down the operators' deployment of a network to a community. In the worst cases, delays may mean that an operator either has to re-route their network at substantial cost, or remove the premises that it is unable to reach from its overall network build altogether. This latter outcome is referred to as 'descoping'.
>
> Once an operator has left the area, it is unlikely that it will return to connect any premises that have been left behind as a result of the need to reroute or descope, due to the large additional costs involved. Should they choose to do so, these costs may be passed on to the consumer in the form of higher fees. Given the increasing reliance on connectivity, there is clearly an imperative to avoid this happening.[72]

The Code does already offer a route via the courts to get access rights in circumstances where an operator is non-responsive, but operators argue that it is costly and lengthy. The Government's consultation heard estimates that process can take 7–12 months per property, which is an unattractive option for operators and can lead to properties being left behind as described above.[73]

Clause 67 aims to reduce the number of connectivity gaps that arise due to a failure by the landowner/occupier to respond, by creating a faster process for

---

71 HL Deb 12 October 2022 vol 824 c822.

72 DCMS, Consultation on changes to the Electronic Communications Code - government response, 24 November 2021, para 3.33-3.34

73 DCMS, Consultation on changes to the Electronic Communications Code - government response, 24 November 2021, para 3.35.

operators to gain access in these circumstances. This new process would be set out in a new Part 4ZA.

The new Part 4ZA is similar to Part 4A of the Code, introduced recently for gaining access to tenanted properties, through the Telecommunications Infrastructure (Leasehold Property) Act 2021. The Library briefing on that Act provides further information.

The Government's consultation response stated there was a "mixed response" to the proposals for non-responsive occupiers. The "vast majority" of operators thought that there should be a streamlined process whereas the "vast majority" of site providers disagreed.[74]

New Part 4ZA

The new Part 4ZA would only apply in circumstances where, in order to connect certain premises, the operator needs to install equipment either above or below (but not on top of) other third-party land. It would only apply to 'relevant land', defined as land that is **not** covered by buildings or used as a garden, park or other recreational area. For example, to connect a property with full-fibre broadband, an operator needs access rights to install a cable underneath a vacant lot or field.

Part 4ZA would set out the procedure that operators must follow, including providing at least three written notices (in addition to the initial request) with set minimum time periods between each notice. If the operator follows this procedure and the landowner/occupier still does not respond, the operator can apply to the First-tier Tribunal for code rights to be imposed.

The code rights could be imposed for a time-limited period, specified by the Secretary of State in regulations, being no more than 6 years. The rights could also expire if an agreement is formed between the parties.

The Part includes powers for the Secretary of State to modify the definition of what land can be included and the terms that must be included in a code agreement obtained under this part.

Clause 67 would give effect to the Schedule to the Bill, which would enact consequential changes following from Clause 66.

Clause 68 – Interim orders

If parties are unable to agree the terms of a renewal agreement then either party can seek an order from the court on whether a renewal should be imposed, and if so, what the terms should be.

Currently the Code allows only site providers (not operators) to apply for an interim order regarding the amount of rent the operator should pay them

[74] DCMS, Consultation on changes to the Electronic Communications Code - government response, 24 November 2021, para 3.43.

while the full case is determined.[75] There is no provision for seeking an interim order regarding non-financial aspects of the agreement.

Clause 68 would make changes to allow either party to apply to the court for an interim order in the case of renewal agreements, including for non-financial terms. Clause 68(4) sets out the factors the court must consider when making an interim order, including the operators' business and technical needs.

Clause 69 – Alternative dispute resolution

Clause 69 would add to the Code provisions to encourage using Alternative Dispute Resolution (ADR) rather than the courts to resolve disputes.

It would add a requirement for operators to provide information about ADR to side providers (the landowner/occupier) when serving a paragraph 20 notice. A paragraph 20 notice is the notice served by operators on the landowner/occupier to request code rights. Operators would be required to inform site providers of the consequences of refusing to engage in ADR. For example, that it could be taken into account by the courts when imposing an agreement. Operators would also have a new obligation to consider the use of ADR before applying to the courts.

Similar provisions would be inserted into Part 5 of the Code, regarding the termination and renewal of code agreements. In this case either party (not just the operator) would be required to consider whether the use of ADR would be appropriate before applying to the court to resolve a dispute.

Clause 70 – Complaints about operators' conduct

Clause 70 would place an obligation on Ofcom to include guidance on how operators handle complaints about their conduct in its non-binding Code of Practice published under paragraph 103 of the ECC.

Ofcom is required to publish a Code of Practice under paragraph 103 of the ECC. The Code of Practice is non-binding on parties to the negotiation. It sets out guidance for what parties should expect from each other when negotiating agreements.

The Government's consultation considered whether a statutory complaints/compliance process should be introduced. Most site providers and professional bodies were in favour of this but most operators were not.[76] Following feedback, including that the Code of Practice was not suitable for

[75] DCMS, Consultation on changes to the Electronic Communications Code - government response, 24 November 2021, para 35.

[76] DCMS, Consultation on changes to the Electronic Communications Code - government response, 24 November 2021, para 3.16-3.17.

statutory enforcement in its current form, the Government decided not to pursue a mandatory complaints and compliance process.[77]

The Government also highlighted that there were "ongoing discussions" between the telecoms industry and site providers about potential reforms to Ofcom's Code of Practice.[78]

Clause 71 – Jurisdiction of First-tier Tribunal in Wales

Clause 71 was added by the Government at the Commons Report stage. It would allow the Secretary of State to make regulations conferring jurisdiction for hearing Code disputes in Wales on the First-tier Tribunal. Currently, under paragraph 95 of the ECC, disputes must commence in the Upper Tribunal. Allowing cases to be handed down to the First-tier Tribunal would bring Wales into line with England.

Clause 72 – Time limits on code proceedings

Clause 72 would introduce a new section 119A into the Communications Act 2003. It would allow the Secretary of State to set out in regulations, a time period within which proceedings on applications made under the Code must be determined.

Currently Regulation 3 of the Electronic Communications and Wireless Telegraphy Regulations 2011 requires the court to decide an application for a new code agreement within six months of the application being received.[79] There is no such requirement for disputes regarding the termination or renewal of agreements.

Clause 73 – rights of network providers in relation to infrastructure of other utilities

Clause 73 does not amend the Electronic Communications Code.

Clause 73 would give the Secretary of State powers to make regulations about conferring rights on telecoms networks operators in relation to the infrastructure of other public utilities ('relevant infrastructure').

The clause specifies that this power would include amending or revoking any provision of the Communications (Access to Infrastructure) Regulations 2016 (SI 2016/200) – known as the ATI Regulations. The Government has said that it will hold a further consultation on minor changes it intends to bring to the ATI

77 DCMS, Consultation on changes to the Electronic Communications Code - government response, 24 November 2021, para 3.28-3.29.

78 DCMS, Consultation on changes to the Electronic Communications Code - government response, 24 November 2021, para 3.29.

79 DCMS, Consultation on changes to the Electronic Communications Code - government response, 24 November 2021, para 5.14.

Regulations to ensure they can be used to their full potential (see Box 1 below).

The Clause is broadly drafted. It would allow the Secretary of State to make regulations about requiring access to infrastructure to be granted to telecoms operators, about requests by network operators for access and the procedures that would apply including for dispute resolution.

Before making regulations the Secretary of State must consult Ofcom and "other such persons the Secretary of State considers appropriate".

The regulations would be made by the affirmative procedure.

1 The ATI Regulations

The Communications (Access to Infrastructure) Regulations 2016 (the ATI regulations) were introduced in 2016 to implement certain requirements of the EU Broadband Cost Reduction Directive and apply UK-wide.[80]

The regulations include a requirement for operators of utilities (gas, electricity, water, and telecoms) to share physical infrastructure with competing network operators.[81] Physical infrastructure sharing can lower the cost of telecoms network builds.

The Government has noted that the ATI regulations have so far had limited success in increasing infrastructure sharing.[82] In June 2020 the Government launched a Call for Evidence as part of a review of the regulations to assess whether further improvements could be made to encourage infrastructure sharing and boost network investment.[83]

The Government's response to the call for evidence, published in November 2021, found that the regulations were "broadly appropriate" and that it was not necessary to make major changes at this point. [84]

However, the Government did consider that the regulations were not being used to their full potential and that clarifications to the scope of the regulations would be helpful. It also identified some changes that could speed up processes and strengthen Ofcom's enforcement powers. Clause 73 of the Bill woud give the Government powers to make changes through secondary legislation.

80 Directive 2014/61/EU on measures to reduce the cost of deploying high-speed electronic communications networks (the Broadband Cost Reduction Directive).

81 DCMS, Broadband rollout trial to target hard-to-reach homes through UK's water pipes, 9 August 2021; DCMS Guidance, Fibre in Water: Improving access to advanced broadband and mobile services via drinking water mains, 9 August 2021.

82 DCMS, Future Telecoms Infrastructure Review, 23 July 2018, para 69.

83 DCMS, Review of the Access to Infrastructure Regulations - call for evidence, June 2020.

84 DCMS, Review of the Access to Infrastructure Regulations call for evidence - government response, 24 November 2021.

Clause 76 – independent review of the ECC

Clause 76, added following a successful Opposition amendment at Lords Report stage, would require the Secretary of State to appoint an independent person to review the impact of the Electronic Communications Code and the Telecommunications Infrastructure (Leasehold Property) Act 2021 on the deployment of gigabit broadband and other telecoms infrastructure. The Secretary of State would be required to do so within three months of the passage of the PSTI Act.

The review would consider:

- the extent to which revisions to the electronic communications code have secured progress towards His Majesty's Government's targets relating to telecommunications infrastructure;
- the balance of rights and responsibilities of land- owners and telecommunications operators;
- the impact of the PSTI Act on the level of competition in the telecommunications sector.

It would be able to make recommendations on matters including but not limited to:

- potential further revisions to the electronic communications code;
- potential amendments to legislation or guidance relating to the valuation of land used to host telecommunications infrastructure;
- the potential benefits of imposing a requirement for telecommunications operators to report annually to Ofcom on their investment in new infrastructure.

3 Progress of the Bill

3.1 Second Reading

Part One

At Second Reading debate, the Secretary of State for Digital, Culture, Media and Sport, Nadine Dorries, introduced the Bill.

She said that the Government had made significant progress to strengthen the UK's cyber security but legislation was needed to protect from the harm posed by cyber criminals. [85]

There was cross party support for the provisions in Part One of the Bill. Shadow Secretary of State Lucy Powell said that the opposition supported the measures in Part One but raised concerns that "these measures have not come sooner and do not go further."[86]

The SNP DCMS Spokesperson, John Nicolson, sought clarity on the enforcement mechanisms in Scotland and asked for the Minister to consider including a duty in the Bill to consult the Scottish government when developing the enforcement mechanism to account for the requirements of the Scottish legal system.[87]

Part Two

Regarding Part Two of the Bill, the Secretary of State highlighted the importance of digital infrastructure to everyday life and the need to roll-out gigabit broadband and 5G at pace. She said that Part Two of the Bill aimed to update the electronic communications code to help meet the Government's ambitions for digital connectivity.[88]

There was cross-party support for the aims and general purpose of Part Two of the Bill. Several members from both sides of the House highlighted broadband and mobile connectivity problems in their constituencies. Some Members raised questions about land valuation, pointing to accounts of small

85 HC Deb 26 January 2022 vol 707 c1026.
86 HC Deb 26 January 2022 vol 707 c1032.
87 HC Deb 26 January 2022 vol 707 c1036.
88 HC Deb 26 January 2022 vol 707 c1028.

landowners in their constituencies that had seen significant drops in rent, in some cases as high as 90%.[89]

Shadow Secretary of State Lucy Powell said that the Government's broadband and 5G roll-out had been "piecemeal, short-term thinking".[90] Regarding Part Two she said that the Opposition's main concern was that the Bill "is likely to slow down, rather than speed up, the broadband and 5G roll-out".[91] The Opposition's concern was that without a change in the valuation principles, some landowners would be resistant to negotiating code agreements when offered large rent reductions and delay agreements being reached. The Opposition asked the Government to review the effect of the 2017 changes to the ECC and its impact on the speed of roll-out.[92]

When asked why the land valuation framework was not being addressed in the Bill, the Secretary of State said that the Government had listened and engaged with landowners but believed that the 2017 land valuation framework was fair and in line with other utilities.[93] She said that the Bill includes measures to make dispute resolution easier and encourage greater collaboration that should hopefully lead to fair and reasonable prices being agreed.[94]

3.2 Public Bill Committee

The Public Bill Committee stage began on 17 March 2022. The Committee held five sittings and concluded on 22 March 2022.

The membership of the committee was as follows:

Chairs: Caroline Nokes, Graham Stringer

Members:

- Simon Baynes (Clwyd South) (Con)
- Saqib Bhatti (Meriden) (Con)
- Kevin Brennan (Cardiff West) (Lab)
- Steve Double (St Austell and Newquay) (Con)
- Ruth Edwards (Rushcliffe) (Con)

89 HC Deb 26 January 2022 vol c1028.
90 HC Deb 26 January 2022 vol 707 c1033.
91 HC Deb 26 January 2022 vol 707 c1033.
92 HC Deb 26 January 2022 vol 707 c1033 and 1051.
93 HC Deb 26 January 2022 vol 707 c1029.
94 HC Deb 26 January 2022 vol 707 c1029.

- Chris Elmore (Ogmore) (Lab)
- James Grundy (Leigh) (Con)
- Sally-Ann Hart (Hastings and Rye) (Con)
- Kate Hollern (Blackburn) (Lab)
- Rebecca Long Bailey (Salford and Eccles) (Lab)
- Julia Lopez (Minister for Media, Data and Digital Infrastructure)
- Navendu Mishra (Stockport) (Lab)
- Kate Osborne (Jarrow) (Lab)
- Tom Randall (Gedling) (Con)
- Shailesh Vara (North West Cambridgeshire) (Con)
- David Warburton (Somerton and Frome) (Con)
- Mick Whitley (Birkenhead) (Lab)

The Public Bill Committee (PBC) received written submissions and took evidence at its first two sittings before going on to conduct its clause by clause examination of the Bill. The written evidence and transcripts of the Committee's sittings are available on the Product Security and Telecommunications Infrastructure Bill pages of the Parliament website.

This section will only discuss clauses of the Bill subject to debate or proposed amendment.

Committee stage consideration of Part One of the Bill

Part One of the Bill was not amended during Committee Stage. There was one proposed new clause, and two Opposition amendments, one of which was moved to a division.

Security requirements

Shadow DCMS Minister Chris Elmore moved amendment 6 which aimed to ensure that the security requirements for consumer connectable products be set out in the Bill, rather than being introduced through regulations.[95] He said that this would strengthen the protection for consumers and would give industry a better understanding of the requirements and speed up the process. The Minister for Media, Data and Digital infrastructure, Julia Lopez, said that the Government had been clear about the three requirements that would be introduced.[96] She said that amendment 6 was unnecessary and may

[95] PBC Deb 17 March 2022 c68
[96] PBC Deb 17 March 2022 c69

also be dangerous, as it did not allow for flexibility in response to changing threats. The amendment was withdrawn.

New Clause 3

Chris Elmore explained that New Clause 3 would require the Secretary of State to report to parliament on security risks from consumer connectable devices.[97] He said it was "imperative" that the security of these products was monitored and regularly reported on. Julia Lopez responded to the amendment and said that the Government already published regular reports on this subject and that this would continue.[98] The amendment was withdrawn.

Online marketplaces

Chris Elmore moved amendment 7 which aimed to ensure that online marketplaces, such as Ebay and Amazon, would be considered distributers under the measures in the Bill.[99] He noted evidence the Committee had heard from Which? about the sale of insecure consumer connectable products through these websites and said that as currently drafted, the Bill "would do nothing to increase the legal responsibility online marketplaces have for the safety and security of products sold through them".[100]

Julia Lopez said that where online marketplaces are the retailer of a product, rather than offering a product on behalf of a third party, they would be liable under the Bill. She also said that the amendment would have unintended consequences placing liability on businesses that could not comply.[101]

Chris Elmore pushed the amendment to a division, where it was defeated by 8 votes to 4.[102]

Committee stage consideration of Part Two of the Bill

Five Government amendments were made to Part Two (amendments 1-5). They were all technical or consequential amendments to tidy the legislation that were made without division.[103]

The Opposition tabled two new clauses. New Clause 1, regarding a requirement to give written notice to emergency services about equipment upgrades, was withdrawn. New Clause 2, which sought to require the Secretary of State to conduct a full economic review of the effect of the Electronic Communications Code was defeated on division.

---

97 PBC Deb 17 March 2022 c68

98 PBC Deb 17 March 2022 c70

99 PBC Deb 17 March 2022 c75

100 PBC Deb 17 March 2022 c75

101 PBC Deb 17 March 2022 c76

102 PBC Deb 17 March 2022 c78

103 Amendment 1: PBC Deb 17 March 2022 (third sitting), c83. Amendments 2-4: PBC Deb 17 March 2022 (fourth sitting), c108 and 112.

The Opposition tabled 5 amendments to Part Two which were all defeated on division.[104] One group of amendments concerned the automatic upgrade and sharing rights.[105] The other concerned the rental payments for renewal agreements.[106]

Automatic upgrading and sharing rights

Opposition amendments 9-12 sought to expand the retrospective upgrading and sharing rights in Clauses 59 and 60 to also apply to equipment on telegraph poles and in blocks of flats for property owned by private landlords.[107]

This followed evidence from Openreach on the challenges of connecting blocks of flats and rural properties (which rely more on poles rather than underground cabling).[108] The Bill as currently drafted only allows retrospective automatic upgrades for infrastructure underground. Openreach argued this could see flats in urban areas and rural properties left behind in roll-out plans.[109]

Julia Lopez, Minister for Media, Data and Digital Infrastructure, said that the amendment would tip the balance too far in favour of operators and the Bill was intentionally drafted restrictively.[110] The Minister also highlighted that the industry didn't have consensus on what rights were required.[111] Other telecoms operators argued in evidence that expanding the automatic upgrade rights too far could entrench the existing operator (usually Openreach) and be harmful to competition.[112]

Land valuation

Opposition amendment 8 sought to place a limit of 40% on rent reductions for renewal agreements. This amendment was aimed at claims that some landowners were seeing very significant rent reductions for renewal agreements.

The Minister argued that the Bill created a fair framework that would apply consistently to all code agreements and that it did not want to put statutory limits on rent.[113] The Minister said that the Government believed that a lot of extreme cases of rent reduction were shortly after the 2017 changes and that the case law and industry had reached more of an equilibrium, which would also be helped by other provisions in the Bill.[114]

---

104 Amendments were moved by Chris Elmore and were defeated by 7 votes to 4.
105 Amendments 9-12; PBC Deb 17 March 2022 (third sitting), c92-96.
106 Amendment 8; PBC Deb 17 March 2022 (fourth sitting), c105.
107 PBC Deb 17 March 2022 (third sitting), c84-96.
108 PBC Deb 15 March 2022 (second sitting), c52.
109 PBC Deb 15 March 2022 (second sitting), c52.
110 PBC Deb 17 March 2022 (third sitting), c88.
111 PBC Deb 17 March 2022 (third sitting), c88.
112 PBC Deb 15 March 2022 (second sitting), c45.
113 PBC Deb 17 March 2022 (fourth sitting), c102-103.
114 PBC Deb 17 March 2022 (fourth sitting), c103.

Oral evidence

On 15 March 2022 the Committee took evidence from landowner organisations and from telecommunications companies. There were opposing views regarding rent payments heard during the evidence sessions.

Landowner organisations highlighted disappointment that land valuation was not addressed in the Bill, describing this issue as the "root cause" of problems with the ECC.[115] Landowner organisations stressed there was an imbalance of power between small landowners and telecoms operators. When asked about comparisons to other utilities, Anna Turley of Protect and Connect argued that other utilities were more tightly regulated that telecoms companies. She called for the Bill to include penalties for poor negotiating behaviour and for more requirements for transparency and accountability about whether savings made on rent were being reinvested into infrastructure.[116] Landowner organisations also called for Alternative Dispute Resolution be made mandatory.

Telecoms industry operators argued that the ECC is "working quite well" for new sites but the main challenge was for renewing existing agreements.[117] Juilette Wallace, representing mobile industry group Speed Up Britain, accepted that some telecoms operators may have been "a little too over-enthusiastic" in their interpretation of the new ECC in early 2018. She argued that most of the alleged "David and Goliath" examples (referring to a situation where a small landowner must negotiate with a large financially-resourced telecoms company) are from these early days and that the industry had "moved on a lot".[118] She disputed the "David and Goliath" analogy arguing that most disputes were "industry arguing with industry" (referring to large telecoms site providers and operators).[119] Mark Barlett argued that in most cases the telecoms industry offered more in rental payments than the valuation framework required. He said that on average, rent reductions were around 63% lower for renewal agreements.[120]

3.3 Report stage

Report stage took place on 25 May 2022. The Government moved a number of amendments, all of which were agreed without a vote. Of the opposition and backbench amendments that were moved at Report stage, one went to a division and was defeated. All of the amendments concerned Part Two of the Bill.

115 PBC Deb 15 March 2022 (first sitting), c5.
116 PBC Deb 15 March 2022 (first sitting), c14.
117 PBC Deb 15 March 2022 (second sitting), c43.
118 PBC Deb 15 March 2022 (second sitting), c43.
119 PBC Deb 15 March 2022 (second sitting), c43.
120 PBC Deb 15 March 2022 (second sitting), c47

For a more detail discussion of the Report stage and Third Reading debates, please see sections 3.3 and 3.4 of the House of Lords Library briefing on the Bill.

Government amendments

Julia Lopez, minister of state at DCMS, moved **new clause 1** that would replace Clause 57. In the Bill as introduced, Clause 57 was intended to address situations where telecoms operators are, for the purpose of the ECC, the occupier of the land on which they have installed communications equipment. Operators in that situation may be unable to renew or renegotiate existing agreements because, under the ECC, agreements must be between the operator and the occupier. The Government redrafted Clause 57 based on feedback from operators that the original wording would not cover all scenarios.

Chris Elmore, responding for Labour, said that while the new wording was an improvement he remained concerned that operators could use the Clause to break existing agreements and seek a new one based on the 2017 ECC (with lower rents.

Clause 57 would be removed by the Government at the Lords Report stage (see section 4.2 below).

New clause 2 adds Clause 71 to the Bill. It would allow the Secretary of State to confer jurisdiction of Code disputes in Wales to the First-tier Tribunal as well as the Upper Tribunal. This would bring Wales into line with England.

Chris Elmore said that his party had "no issue" with the new clause.

Amendments 4-7 were introduced to clarify the Bill's provisions on alternative dispute resolution (ADR). They make clear that either the operator or the site owner can tell the other party that they wish to engage in ADR.

Backbench and opposition amendments

Amendments 9 and 11 were moved by Conservative MP Sir Desmond Swayne. They would make it mandatory for operators to engage in ADR. This, he said, would address examples of "egregious bullying" where operators "overawe and frighten landowners with the threat of legal action."[121]

The Minister said that while she was sympathetic to the amendments' aim of promoting collaborative negotiations, the Government's view was that ADR should not be mandatory as it may not be appropriate in all situations.

For Labour, Chris Elmore said he hoped that the Lords would continue the debate on mandatory ADR.

[121] HC Deb 25 May 2022 vol 715 c331.

Sir Desmond also moved **amendments 12 and 13**. They would remove the clauses in the Bill that would allow operators to renew agreements based on the land valuation regime introduced in the 2017 ECC reforms. The 2017 reforms, he said, had caused the market for mast sites to dry up. As one of the aims of the Bill is to speed up the process of reaching agreements, Sir Desmond argued that "the obvious remedy" is to return to the pre-2017 valuation regime.[122] Chis Elmore welcomed the amendments.

Julia Lopez acknowledged the "discontent" about the new valuation framework, but argued that it "creates the right balance between the public need for fantastic digital infrastructure and making sure that landowners receive a fair payment for allowing their land to be used."[123]

Amendments 14-17 were moved by Chris Elmore. Similarly to amendments 9-12 tabled at Committee stage, they would introduce retrospective upgrade rights to equipment in properties owned by private landlords. He argued that the amendments were needed to tackle "broadband blackspots" in urban areas caused by operators struggling to gain landlords' consent to access to multi-dwelling units (MDUs), such as blocks of flats. He said that the rights would be subject to the condition that their exercise can have no adverse affect on a person's enjoyment of the land and cause no loss, damage, or expense.[124]

Responding for the Government, Julia Lopez reiterated the view expressed at Committee stage regarding the need to balance public benefit and private rights. She argued that works in a building would almost always have an impact on the landlord, and noted that there was no consensus in the industry that the proposed rights would be beneficial.

Amendment 14 was pressed to a division and defeated by 280 votes to 163.

3.4 Third Reading

Third Reading also took place on 25 May 2022. The Bill was sent to the House of Lords without a division.

Chris Elmore, speaking for Labour, and Owen Thompson, for the SNP, both said that their parties supported the principles of the Bill. Chris Elmore said in particular that he would like to see the core security requirements (such as the ban on default passwords) in the Bill itself rather than in future regulations, and that the Bill could do more to deliver support the gigabit broadband rollout. Owen Thompson reiterated calls made at Second Reading that the Secretary of State should have a duty to consult Scottish Ministers when developing an enforcement mechanism for Scotland.

---

122 HC Deb 25 May 2022 vol 715 c331.

123 HC Deb 25 May 2022 vol 715 c326.

124 HC Deb 25 May 2022 vol 715 c329-330.

4 Lords stages

The Government made the following amendments to Part Two of the Bill during its passage through the House of Lords.

- Clause 57 (definition of 'occupier') was removed from the Bill;
- New Clause 60 was added to the Bill. It would grant an automatic right to share and upgrade telecommunications equipment on telegraph poles;
- New Clause 66 was added to the Bill. It would grant the Secretary of State powers to prevent Code Rights being granted to a telecoms operator if doing so would prejudice national security.

One opposition amendment was agreed on division:

- New Clause 76 was added to the Bill. It would require the Secretary of State to review the impact of the post-2017 reforms to the Electronic Communications Code.

The Government also introduced a series of amendments to Part One implementing recommendations made by the Delegated Powers and Regulatory Reform Committee (DPRRC). They were agreed without a vote.

The amendments were all agreed at Report stage (section 4.2 below).

4.1 Second reading and Committee stage

The Bill was read a second time in the House of Lords on 6 June 2022. Opening the debate, Lord Parkinson (Parliamentary Under-Secretary of State for the Department of Digital, Culture, Media and Sport) said that the Bill would

> facilitate the extension of futureproofed gigabit-capable broadband and 5G networks, and improve the protection of people, networks and infrastructure from the harms caused by insecure consumer-connectable products.[125]

Lord Bassam, the shadow spokesperson for DCMS, said that while the Opposition supported the Bill, it required "practical changes and improvements" to support the rollout of digital infrastructure.

[125] HL Deb 6 June 2022 vol 822 c1031.

Committee stage was held over two sittings, on 21 and 29 June 2022. The Bill was not amended. The Government did not table any amendments and no other amendments were put to a vote.

Part One of the Bill

The provisions in the first Part of the Bill, on product security, were broadly welcomed. However, Liberal Democrat peers Lord Fox and Lord Clement-Jones criticised the Government for leaving too much of the detail to secondary legislation. A number of amendments were tabled that would specify the Government's obligations with regards to regulations introduced under the Bill. Peers also sought clarification on the relationship between the Bill and existing consumer protection legislation and the extent to which online marketplaces are within the Bill's scope.

Security requirements

During the Second Reading debate, Liberal Democrat peers Lord Fox and Lord Clement-Jones criticised the Bill for leaving the detail of the security requirements that will be set for connected consumer products to secondary legislation. Consequently, argued Lord Fox, it is unclear from the text of the Bill

> what a consumer might reasonably expect from consumer-connectible products in their house. What might they be able to expect through the life of that product in terms of security and hacking? Assuming that there is no such thing as absolute security, following the implementation of the Bill and all its, as yet, unseen statutory instruments, what level of security should the UK consumer reasonably expect for their household, and what is their recourse in the event that that is not met?[126]

At Committee, peers tabled a series of amendments intended to address this perceived deficiency.

Amendment 1 was tabled by Lord Clement-Jones. It would add to the Bill a set of general principles relating to product security and require the Secretary of State to have regard to those principles when making regulations. Lord Fox, speaking to the amendment, explained that the principles were based on the Government's Code of Practice for Consumer IoT Security:

- Manufacturers, importers, and distributers have a duty of care towards their customers with regards to privacy and safety;
- Consumer are entitled to expect connectable products on the UK market to meet minimum cyber security standards;
- Manufacturers, importers, and distributors should be able to demonstrate an understanding of and support programme for emerging security threats, and ensure their products are safe by design.[127]

[126] HL Deb 6 June 2022 vol 822 c1035.

[127] HL Deb 21 June 2022 (first sitting) vol 823 c173-176.

The Government's position was that product security is best served by standards-based regulation rather than principles:

> If one sets standards, one can send a device to a laboratory and assure oneself that those standards have been met. If one sets principles, that does not apply. That is why the Bill is designed to give force to standards. Those standards, developed here in the UK and now adopted by Governments and jurisdictions across the globe as well as by international standards bodies, are widely recognised significantly to lower risk for consumers.

Lord Fox questioned whether a standards-based regime could keep up with innovation by technology companies and cyber criminals. In his speech, for example, he referred to an article predicting the end of the password, rendering the proposed ban on default passwords 'obsolete.'[128]

Amendments 4 and 5, tabled by Labour and the Liberal Democrats respectively, both sought to require regulations made under Clause 1 to include certain specified security requirements. This would, for example, add the proposed ban on default passwords to the Bill itself. Amendment 5 also sought to mandate a minimum period that manufacturers of smart products should provide security updates. Consumer group Which? had called for the Bill to be strengthened in this way.[129] **Amendment 3** proposed to add a specific reference to children's toys and baby monitors.

Lord Parkinson responded to these attempts to put certain security requirement in primary legislation by stressing the Government's desire for flexibility. The Bill, he said, aimed to introduce a regulatory framework capable of responding to changes in cyber threat and technology:

> Our requirements need to be able to respond and adapt to those changes. Obliging the Government to set out requirements framed using terminology that may seem appropriate today could limit the security benefits of such a requirement in future, impose impractical obligations on businesses, create new security threats or introduce barriers to innovation. Further, if we put some security requirements in the Bill now and additional requirements in secondary legislation in future, we would risk confusion.[130]

Consumer protection

Lord Fox spoke to **amendments 14 and 14A**, tabled by Lord Clement-Jones. These were probing amendments that sought to clarify the relationship between the security requirements in the Bill and existing consumer protection legislation. This was another point raised by Which?:

> If someone owns an insecure smart device, they should be able to argue that it is faulty and then get a refund or replacement as per their legal rights under the Consumer Rights Act 2015. This is currently not defined clearly enough, in our view, under the PSTI legislation as drafted.[131]

---

128 Wired, Apple Just Killed the Password—for Real This Time, 7 June 2022.

129 Which?, Smart products from the biggest tech brands easily hacked in Which? tests, 1 June 2022.

130 HL Deb 21 June 2022 (first sitting) vol 823 c184.

131 Which?, Smart products from the biggest tech brands easily hacked in Which? tests, 1 June 2022.

The amendments would define security issues as a fault under the Consumer Rights Act 2015 and allow individual consumers to seek redress for defective connected products. Baroness Merron (Lab) and the Earl of Errol (CB) also spoke of the need for clarity on this issue.[132]

The Minister suggested in his response that the Government drew a distinction between 'product safety,' where unsafe product may cause physical harm, and 'product security.' The Earl of Errol noted that insecure products could

> render serious physical harm to someone because having all their money removed from their bank account could affect their mental state and result in the breakdown of their marriage, suicide, failure of business, all sorts of things. Therefore, it may have just as damaging physical effects on someone, though not immediately apparent. Although they are different they are equally unsafe, so this has more merit than he is suggesting.[133]

In a letter to peers sent after the debate, Lord Parkinson acknowledged the Earl's point but argued that the regulatory framework should nevertheless be different:

> Product safety requirements can generally be complied with before a product is made available. In contrast, some of the security requirements in this regime compel businesses in the supply chain to take continuous actions, ensuring that vulnerabilities can be reported and remedied.
>
> Cyber threats are constantly changing and will require different approaches to resolve. A blanket alignment with the product safety regime could punish businesses dealing with these live issues and potentially make them liable to pay compensation for matters beyond their control. Of course, where security requirement breaches do meet the criteria set out in legislation, consumers will be entitles to the protections provided by that legislation.[134]

Online marketplaces

Lord Bassam moved **amendment 7** which sought to bring online marketplaces which sell connected consumer products into the scope of the Bill. **Amendment 8**, moved by Lord Fox, had the same intent.[135]

Lord Parkinson reiterated the Government's view – as also expressed during the Commons Committee stage – that online marketplaces would be covered by the Bill where they act as a manufacturer, importer, or distributer of connected products. If the online marketplace does not fall into one of these categories, the organisation that does (such as a third-party seller using the marketplace platform) could be held responsible under the Bill.

Lord Fox and Lord Lucas pressed the Minister on consumer protections with regards to products sold on online marketplaces by overseas retailers and

---

132 HL Deb 21 June 2022 (second sitting) vol 823 c203-205.

133 HL Deb 21 June 2022 (second sitting) vol 823 c206.

134 DCMS, Letter from Lord Parkinsonto Peers regarding issues raised during the Committee stage (first day) of the Bill: App security and privacy interventions consultation, online marketplaces, consumer protections and redress, 28 June 2022.

135 HL Deb 21 June 2022 (first sitting) vol 823 c193-195.

manufacturers.[136] In a letter sent after the debate, Lord Parkinson explained that the Bill empowers the Secretary of State to seize or recall non-compliant products sold in the UK, including products from overseas organisations. He also said that the Government was "collecting evidence" on how to ensure that online marketplaces have "proportionate responsibilities" for the safety and security of products sold on their platform.[137]

Computer Misuse Act 1990

Conservative peer Lord Arbuthnot moved **amendment 16** which proposed a statutory defence for "ethical hackers."[138] Currently, the Computer Misuse Act 1990 criminalises all unauthorised access to computers. The CyberUp campaign, which includes industry groups such as techUK and the CBI, has argued that this blanket ban criminalises some of the vulnerability and threat assessment work done by cyber security professionals.

For further information on this issue, see the Commons Library debate pack prepared for a Westminster Hall debate on the Computer Misuse Act 1990.[139]

The Government is in the process of reviewing the 1990 Act. Lord Parkinson asked for the amendment to be withdrawn pending the outcome of the review.

Part Two of the Bill

In the debates on the second Part of the Bill peers raised similar issues as had been discussed during the Commons stages, including upgrading and sharing rights, land valuation, and dispute resolution.

None of the proposed amendments covered in this section were added to the Bill.

Clause 57, intended to change the definition of 'occupier' in the Electronic Communications Code, was also debated. However, the Clause was removed during Report stage, as discussed in section 4.2 below.

Automatic upgrading and sharing rights

At Second Reading and Committee stage peers debated the merits of extending the automatic right to upgrade and share communications equipment. The Bill as introduced would add a retrospective right to upgrade and share equipment installed underground under a Code agreement entered into prior to the 2017 reforms. Peers discussed proposals to add similar rights

136 HL Deb 21 June 2022 (first sitting) vol 823 c196-197.

137 DCMS, Letter from Lord Parkinsonto Peers regarding issues raised during the Committee stage (first day) of the Bill: App security and privacy interventions consultation, online marketplaces, consumer protections and redress, 28 June 2022.

138 HL Deb 21 June 2022 (second sitting) vol 823 c207-208.

139 House of Commons Library, Westminster Hall debate on the Computer Misuse Act 1990, 17 April 2022.

for overground equipment (usually on telegraph poles) and equipment in blocks of flats, or multi-dwelling units (MDUs).

Amendment 18, tabled by Conservative peer Baroness Harding, sought to enable the sharing of poles built on private land before 2017. It had general support across the Chamber, and Baroness Harding noted that there was a "clear consensus across the industry that the Bill needs to make this possible."[140] The Commons Public Bill Committee heard evidence from the industry about the importance of access to poles. Openreach and CityFibre said that easier access to poles on private land would help speed up the rollout of gigabit broadband and reduce costs, especially in rural areas.[141]

Lord Parkinson acknowledged that the Government had been called on to use the Bill to facilitate the upgrading and sharing of poles, and said that it understood the potential benefits. However, the Government was not willing to accept Baroness Harding's amendment due in part to concerns about its impact on landowners. Lord Parkinson promised that the Government was looking closely at the issue and would return to it at Report stage.

There was a less agreement on whether to grant automatic rights to upgrade equipment in MDUs. Baroness Harding spoke of the importance of not exacerbating "existing non-digital inequalities in the digital world, which is exactly what happens when the fibre rollout goes past blocks of flats in many communities across London and other cities." However, she and other peers noted that a right to upgrade existing equipment would give a significant competitive advantage to Openreach given that it owns the existing copper wiring.

Lord Vaizey spoke in favour: "If you want as much connectivity as quickly as possible to as many homes as possible, you have to put Openreach at the centre of your strategy."[142] He tabled **amendments 17A and 17B** at Committee stage but neither was moved.

Land valuation

The 'no scheme' land valuation regime introduced in the 2017 reforms to the Electronic Communications Code (see sections 2.2 and 2.3 of this briefing) drew significant interest. Some peers argued that the 2017 reforms, by allowing telecoms to significantly decrease rents, had resulted in fewer sites being made available. The Earl of Devon (CB), for example, said that the "market for telecoms infrastructure has largely ground to halt" as the financial incentive for site providers to engage constructively with operators has been undermined. The Bill's proposals for achieving more collaborative negotiations through alternative dispute resolution (ADR) "entirely misses

140 HL Deb 29 June 2022 vol 823 c652.

141 PBC Deb 15 March 2022 (second sitting), c40-41.

142 HL Deb 6 June 2022 vol 822 c1042.

the point. If the financial underpinnings of those negotiations remain as one-sided as they are, no amount of ADR will help."[143]

Lord Clement-Jones similarly argued, with reference to a CEBR report for landowners' campaign group Protect and Connect, that the 2017 reforms had slowed down the rollout of communications infrastructure.

Speaking for the Government, Lord Parkinson argued that it was "too simplistic" to attribute changes in the market to the 2017 valuation regime. He pointed to other aspects of the 2017 reforms, notably rights to share equipment, and the Covid-19 pandemic as alternative explanations for lower demand for new mast sites.

Numerous amendments were tabled at Committee stage that sought, directly or indirectly, to address the issue of land valuation.

Amendments 20, 22, and 23 would amend or disapply the no-scheme valuation framework, particularly for agreements renewed under the Landlord and Tenant Act 1954. Lord Parkinson said that the Government could not accept these amendments as they would represent a "retrograde step" back to the high rents of the pre-2017 Code. There would also be an inconsistent approach to land valuation depending on whether an agreement was renewed under the Code or the 1954 Act.

Amendments 24, 25, 26, and 27 would set a limit on the maximum permitted reduction in rents and require rent reductions to be phased in over time. Lord Parkinson said that it would not be appropriate set national guidance in this area given the "hugely diverse range of circumstances" covered by Code agreements.

Amendments 45-49 would require the Government to undertake a review of the 2017 ECC reforms and recent legislation specifically with regards to the extent to which they have accelerated the rollout of digital infrastructure. The Government would also be required to publish a strategy for resolving issues around landowner rights and competition within the telecoms sector.[144]

Lord Parkinson argued that setting requirements to for the Government to undertake reviews at specific times would "fetter the Government's ability to judge when a meaningful review of progress can most sensibly be completed and what information it should include." He assured the Chamber that the impact of the Bill would be monitored.[145]

Amendment 50 would oblige telecoms companies to report information to Ofcom on their annual investment in mobile networks, the rent paid to site providers, and the number of mobile sites built or upgraded. This arose from

143 HL Deb 6 June 2022 vol 822 c1054.

144 HL Deb 29 June 2022 (second sitting) vol 823 c743-748.

145 HL Deb 29 June 2022 (second sitting) vol 823 c751.

claims made by the Government that reduced rents were justified in part because they enable greater investment in digital infrastructure.

The Minister questioned whether the imposing reporting obligations would be proportionate given that complying with the duty would divert resources away from rolling out network infrastructure. He also argued that requiring operators to publish average rents could undermine negotiations.

Alternative Dispute Resolution

One of the aims of Part Two of the Bill is to encourage "collaborative relationships between telecommunications operators and site providers" within the reformed Electronic Communications Code framework introduced in 2017.[146] During the debates, some peers argued that the Bill should do more to improve the balance of power between site owners and telecoms operators, particularly when disputes arise.

Amendment 35, moved by Lord Clement-Jones, would make the Bill's alternative dispute resolution (ADR) provisions mandatory rather than voluntary. Peers including Baroness McIntosh (Con), the Earl of Lytton (CB), Lord Northbrook (Con), and Baroness Merron (Lab) also spoke in favour of mandatory ADR.[147]

Lord Parkinson explained the Government had chosen to make ADR voluntary for two reasons. First, ADR is not appropriate where disagreements are based on different interpretations of the law. Second, mandatory ADR may force parties into a process they do not want to participate in. In both cases, the dispute would end up in court and the mandatory ADR process would have only served to add time and cost.

The Minister reported that a majority of landowner groups his Department had consulted were opposed to ADR. He also noted that a party's unreasonable refusal to engage in ADR would be considered by courts when awarding costs.

Amendments 39-42, also in the name of Lord Clement-Jones, aimed to give greater weight to Ofcom's code of practice on the Electronic Communications Code. The amendments would require courts to take non-compliance with the code of practice into account when awarding costs; make compliance with the code of practice mandatory; and, in cases of non-compliance, allow Ofcom to impose fines and require compensation to be paid. Obligations would apply to operators and site providers. The amendments would also set certain requirements with regards to operators' complaints procedures. Lord Clement-Jones argued that "having clear and enforceable guidance on the standards expected by the parties" would help achieve the Government's aim

146 HL Deb 6 June 2022 vol 822 c1032.

147 HL Deb 29 June 2022 (first sitting) vol 823 c704-708.

of "promoting consensus-based agreements and getting this market working again."[148]

In response, Lord Parkinson argued that because the code of practice was intended as guidance, determining whether a particular action constituted a breach would be "very subjective." The prospect of fines would, he believed, disincentivise both parties from seeking agreements.

Regarding complaints procedures, he said that the Government intended to bring forward secondary legislation to achieve three things:

> first, to create a requirement on operators to have a complaints procedure in place to handle complaints relating to their conduct; secondly, to set out minimum standards which this process must meet; and, thirdly, to oblige operators to have regard for the Ofcom code of practice when handling complaints.[149]

4.2 Report stage

Report stage was held on 12 October 2022. The Government introduced amendments to both parts of the Bill. One opposition amendment to Part Two was agreed on division.

Amendments to Part One of the Bill

The Government introduced a series of amendments implementing recommendations made by the Delegated Powers and Regulatory Reform Committee (DPRRC). All were agreed without votes.

Amendments 2, 4, and 5 – procedure

These amendments apply the affirmative resolution procedure to regulations made under Clause 3 and Clause 9(7). In the Bill as introduced they would have been subject to the negative procedure.

Clause 3 empowers the Secretary of State to provide that a connected product should be deemed to have complied with the security requirement if certain conditions, specified in regulations, are met. This would be the case, for example, where the product meets equivalent international standards.

Clause 9(7) provides a power to exempt manufacturers from the duty to provide a statement of compliance with the security requirements for connected products if certain conditions, specified in regulations, are met. This would be the case, for example, where an international certification regime provides an equivalent statement of compliance.

148 HL Deb 29 June 2022 (first sitting) vol 823 c704.
149 HL Deb 29 June 2022 (first sitting) vol 823 c709-711.

The DPRRC recommended that these powers should either be narrowed or made subject to the affirmative resolution procedure.[150] The Government argued in respect to both clauses that they were framed broadly in order to provide the flexibility required to adapt to changing international standards and regulatory regimes, but accepted that the affirmative procedure would be appropriate.[151]

The DPRRC also made recommendations in relation to powers in Clauses 11, 18, 19, 24, and 25. These concern duties to issue notifications and take action where manufacturers, importers, and distributors become aware of compliance failures in relation to connected products. Consumers must be notified if conditions set out in regulations are met. In the DPRRC's view, the Secretary of State should have a duty, rather than a discretionary power, to make such regulations.

The Government did not take this recommendation forward. The Minister, Lord Parkinson, said in response to the DPRRC's report that the power is intended to be "supplementary" to the enforcement body's powers to inform customers and that will be applicable only where "immediate action is necessary and suitable." He also argued that the power must "remain flexible to allow further nuance to be made in regulations with reference to specific security requirements and types of breaches."[152]

Amendments 6-12 and 14 – enforcement

When the Bill was introduced, Clause 27 permitted the Secretary of State to delegate the Bill's enforcement functions to any person by entering into an agreement with them. This arrangement was strongly criticised by the DPRRC:

> The enforcement functions which may be delegated by an agreement under clause 27 are very significant, and how they are exercised will no doubt have an important impact on the effectiveness of the regulatory regime. Also, there are no limitations on the persons to whom the functions may be delegated. As things stand, there is no requirement for parliamentary scrutiny of the delegation by the Secretary of State of the power to exercise enforcement functions under clause 27, and there are no limitations on the persons to whom the functions may be delegated. There is not even any requirement on the Secretary of State to publish information about delegations made under clause 27.[153]

The DPRRC's view was that the power to delegate functions should be exercised by regulations and that the regulations should be subject to the

150 Delegated Powers and Regulatory Reform Committee, Fourth Report of Session 2022-23, HL Paper 23, 16 June 2022, paras 3-11.

151 Delegated Powers and Regulatory Reform Committee, Eighth Report of Session 2022-23, HL Paper 45, 12 July 2022, p6.

152 Delegated Powers and Regulatory Reform Committee, Eighth Report of Session 2022-23, HL Paper 45, 12 July 2022, p7.

153 Delegated Powers and Regulatory Reform Committee, Fourth Report of Session 2022-23, HL Paper 23, 16 June 2022, para 22.

affirmative resolution procedure. These amendments implement that recommendation.

Lord Kamall (Parliamentary Under-Secretary of State for DCMS) confirmed during the Report stage debate that the Government intended to appoint the Office of Product Safety and Standards, part of BEIS, as the enforcement authority. He said that due to the Carltona principle (which permits civil servants to act as the Secretary of State) the Government would not be required to introduce regulations under Clause 27.[154]

Amendments withdrawn or not moved

Amendments 1, 3, and 13 were the same as amendments tabled at Lords Committee stage. They sought to: add a set of product security principles to Clause 1; bring online marketplaces into the scope of the Bill; and introduce a statutory defence for ethical hacking. The Government reiterated its opposition to these proposals.

Amendments to Part Two of the Bill

Government amendments 15, 18, and 23 were agreed without votes. Amendment 28, moved by Labour peer Baroness Merron, was successful on division.

Amendment 15 – definition of 'occupier'

Government amendment 15 removes Clause 57 from the Bill.

As discussed in section 2.4 above, Clause 57 sought to provide a way for operators to renew or amend an existing agreement in circumstances where the operator is already in occupation of the land. The Upper Tribunal and Court of Appeal had decided that, in such circumstances, the operator may be both the 'operator' and the 'occupier' for the purposes of the ECC. It would, therefore, not be able to seek new code rights because that would involve entering into a legal agreement with itself.

In June 2022 the Supreme Court issued a ruling which overturned the relevant parts of the Upper Tribunal's and Court of Appeal's decisions. The Supreme Court took the view that "the fundamental premiss" of the ECC is that "the 'operator' and the 'occupier of the land' are different persons."[155] It held that if an operator was in occupation of the land it would be able to seek additional rights from the landowner instead.[156]

---

154 HL Deb 12 October 2022 vol 824 c796

155 Cornerstone Telecommunications Infrastructure Ltd v Compton Beauchamp Estates Ltd [2022] UKSC 18, para 117.

156 Gowling WLG, Operators secure victory in the Supreme Court: access to the Code obtained for thousands of sites, 22 June 2022.

Lord Kamall said that the Supreme Court's judgement achieved the purpose of Clause 57. Given the potential unintended consequence of the Clause, as raised in previous debates, the Government decided to remove it:

> The effect of the judgment is … broad and comprehensive; the Government consider that it will ensure that any operator, whatever the nature of its agreement, will have a means through which it can seek new or additional code rights, as the case may be. As a result, the Government no longer consider it necessary to retain Clause 57 in the Bill. Its removal will, in light of the Supreme Court judgment, ensure clarity and certainty for all users of the code.[157]

Lord Bassam, for Labour, and Lord Fox, for the Liberal Democrats, agreed that it was "very sensible" to remove Clause 57 given the Supreme Court's judgement.[158]

Amendment 18 – telegraph poles

In the Growth Plan 2022 the Government stated that it would introduce amendments to the PSTI Bill to "give telecoms operators easier access to telegraph poles on private land, supporting the delivery of gigabit capable broadband."[159]

Government amendment 18 adds a new Clause 60 to the Bill. The new Clause would amend paragraph 74 of the ECC, which gives operators the right to fly cables between telegraph poles on private land. Clause 60 would extend that right. It would permit the owner of the poles (the 'main operator') to share access with other operators. It would also permit the main operator and other operators to upgrade infrastructure on the poles.

The Government had been unwilling to accept similar amendments tabled at previous stages of the Bill due to concerns about the impact on landowners. Lord Harlech, speaking on behalf of the Government, said that the new rights would be subject to conditions:

- The exercise of these rights cannot have more than a minimal adverse impact on the appearance of the pole;
- The exercise of these rights cannot have more than a minimal adverse impact on the land on which the pole is kept;
- These rights cannot be used to carry out works that will cause loss, damage or expense to any person with an interest in the land on which the pole is kept;
- Operators must have the landowners permission before entering private land.[160]

In response to a question from Baroness Harding, Lord Harlech confirmed that the 'landowners permission' could in principle be secured through a

---

157 HL Deb 12 October 2022 vol 824 c797.

158 HL Deb 12 October 2022 vol 824 c797.

159 HM Treasury, Growth Plan 2022, 23 September 2022, para 3.37.

160 HL Deb 12 October 2022 vol 824 c803.

verbal agreement. The Clause would not require proof of permission in any particular form.[161]

Amendment 23 – national security

Government amendment 23 would grant the Secretary of State powers to intervene to prevent a court from granting code rights in circumstances where granting the request would "prejudice national security, defence or law enforcement." Lord Sharpe, Parliamentary Under-Secretary of State at the Home Office, said that this was to prevent operators from gaining access rights to sensitive sites without the landowner's consent.

The amendment had broad support although the Earl of Devon (CB), Lord Fox (Lib Dem), and Lord Bassam (Lab) criticised the Government for introducing it at a late stage.[162]

Lord Fox asked for clarification about how and when the power would be used. Lord Sharpe responded that the power would be used "only when all other routes to the mutually consensual solution have been exhausted" and the Secretary of State decides it is appropriate.[163]

Amendment 28 – independent review

Labour peer Baroness Merron moved amendment 28, which adds a new Clause 76 to the Bill. In her speech, Baroness Merron said that the amendment is "an attempt to find a constructive way forward to perhaps the greatest area of discussion throughout this Bill which has not been resolved – how we bring together the balance, the fairness and efficiency that we all say we are looking for."[164] It amalgamates a number of amendments tabled during Committee stage.

The amendment would require the Secretary of State to appoint an independent person to review the impact of the ECC and the Telecommunications Infrastructure (Leasehold Property) Act 2021 on the deployment of gigabit broadband and other telecoms infrastructure. The Secretary of State would be required to do so within three months of the passage of the PSTI Act.

The review would consider:

- the extent to which revisions to the electronic communications code have secured progress towards His Majesty's Government's targets relating to telecommunications infrastructure;
- the balance of rights and responsibilities of land- owners and telecommunications operators;

161 HL Deb 12 October 2022 vol 824 c805-806.
162 HL Deb 12 October 2022 vol 824 c823-825.
163 HL Deb 12 October 2022 vol 824 c825-826.
164 HL Deb 12 October 2022 vol 824 c831.

- the impact of the PSTI Act on the level of competition in the telecommunications sector.

It would be able to make recommendations on matters including but not limited to:

- potential further revisions to the electronic communications code;
- potential amendments to legislation or guidance relating to the valuation of land used to host telecommunications infrastructure;
- the potential benefits of imposing a requirement for telecommunications operators to report annually to Ofcom on their investment in new infrastructure.

Responding for the Government, Lord Kamall argued that the prospect of a review would "create chaos" in market that is "starting to settle" after the 2017 reforms to the ECC. He also questioned the feasibility of quantifying the impact of a single piece of legislation. He pointed to the review and reporting mechanisms that already exist, including Ofcom's Connected Nations reports and Building Digital UK's quarterly Project Gigabit delivery updates.

Baroness Merron pressed the amendment to a division, where it was agreed by 159 votes to 151.

Amendments withdrawn or not moved

As at Committee stage, the House debated amendments regarding land valuation and alternative dispute resolution.

Amendments 20 and 21 would remove Clauses 61 and 62 from the Bill. The two clauses would require courts to renew pre-2017 agreements based on a market valuation method more closely aligned with the 2017 ECC.

Amendments 19, 22, and 24 were also on the subject of land valuation but took a different approach. Speaking for the amendments, the Earl of Devon (CB) said that they did not seek to prevent the Government's preferred 'no scheme' valuation methodology, but sought to "soften the impacts to protect the interests of the individual landlord."[165] The amendments would prohibit rent reductions of more than 50%, require reductions to be phased in over five years, and prevent the backdating of rent reductions.

Lord Kamall said that it remained the Government's view that the 2017 reforms "created the right balance."[166]

The Earl of Devon withdrew amendment 19 in favour of amendment 28, which would require the Secretary of State to commission an independent review of (among other things) the 2017 land valuation regime.

[165] HL Deb 12 October 2022 vol 824 c815-816.

[166] HL Deb 12 October 2022 vol 824 c818.

Amendments 25-27, moved by Baroness McIntosh (Con), would make the Bill's alternative dispute resolution (ADR) provisions mandatory rather than voluntary. The Government remained opposed to mandatory ADR for the reasons discussed at Committee stage.

4.3 Third reading

The Bill was read for a third time on 19 October 2022. No further amendments were tabled.

Baroness Merron, Lord Clement-Jones, and the Earl of Lytton encouraged the Government to retain the review mechanism in new Clause 76.[167] The Earl described it as a measure "that might ultimately address market concerns on telecoms sites." Baroness McIntosh said she regretted that ADR would not be mandatory and hoped that the Government would reconsider it 'next door.'[168]

[167] HL Deb 19 October 2022 vol 824 c1108-1109.

[168] HL Deb 19 October 2022 vol 824 c1110.

The House of Commons Library is a research and information service based in the UK Parliament. Our impartial analysis, statistical research and resources help MPs and their staff scrutinise legislation, develop policy, and support constituents.

Our published material is available to everyone on commonslibrary.parliament.uk.

Get our latest research delivered straight to your inbox. Subscribe at commonslibrary.parliament.uk/subscribe or scan the code below:

commonslibrary.parliament.uk

@commonslibrary