HOUSE OF LORDS Library Briefing

Product Security and Telecommunications Infrastructure Bill
HL Bill 16 of 2022–23

Author: James Tobin

Date published: 1 June 2022

Table of Contents

1. Key provisions in the bill and background to the proposals
2. Measures in the bill: Clause by clause
3. House of Commons stages

The Product Security and Telecommunications Infrastructure Bill is legislation introduced by the government intended to do the following:

- Provide regulation-making powers to introduce mandatory security requirements for consumer connectable products (so-called smart or Internet of Things (IoT) devices) sold in the UK. (Part 1)
- Make changes to the electronic communications code (ECC) which governs the rights of telecoms companies to install infrastructure on land, in part to further the expansion of mobile, full fibre and gigabit capable networks across the UK. (Part 2)

Among the measures provided for by part 1 include a requirement for consumable connectable products to have a vulnerability disclosure policy through which any security weakness in a product is identified and notified; a ban on default passwords; and a transparency requirement on how long a manufacturer will provide security updates for the product. The provisions in part 1 have largely been welcomed by industry stakeholders and opposition parties. Though some fears have been voiced about the additional burden on manufacturers, particularly small companies.

The measures in part 2 are focused on encouraging faster and more collaborative negotiations for the installation and maintenance of telecoms equipment on private land. Stakeholder debate on part 2 has been highly polarised between the telecoms and mobile industry on one side, and property owner groups on the other. In Parliament, opposition parties have been broadly supportive of the aims of the legislation but have raised concerns on several areas, including whether the bill goes far enough to advance the rollout of new technology and digital capacity; accessing property owned by absentee landlords; and calling for a review of the economic impact of the ECC. The bill also does not address the question of land valuation reforms introduced to the ECC in 2017, which observers such as the Law Society have said appear to lie at the heart of many disagreements on land usage.

The bill has been carried over from the 2021–22 parliamentary session. It has completed its passage through the House of Commons, and its second reading in the House of Lords is scheduled to take place on 6 June 2022.

Table of Contents

1. Key provisions in the bill and background to the proposals 1
1.1 Part 1: Safety requirements for consumer connectable products 1
1.2 Part 2: Telecommunications infrastructure 5
2. Measures in the bill: Clause by clause 7
2.1 Part 1: Product security 7
2.2 Part 2: Telecoms infrastructure 12
2.3 Part 3: Final provisions 19
3. House of Commons stages 19
3.1 Second reading 19
3.2 Committee stage 21
3.3 Report stage 22
3.4 Third reading 29

1. Key provisions in the bill and background to the proposals

1.1 Part 1: Safety requirements for consumer connectable products

Consumer connectable products are consumer products which can connect to the internet or other networks and can transmit and receive digital data. Examples of these products include smartphones, smart TVs, smart speakers, connected baby monitors and connected alarm systems. They are also known as 'Internet of Things' (IoT) or 'smart' devices. This is a rapidly growing market. The number of IoT devices in the UK is projected to increase from 13mn in 2006 to over 150mn in 2024.[1]

Currently, whilst consumer connectable products must meet specific standards relating to product safety, there are no minimum standards required for security. As a result, the Government Office for Science notes that such devices can be vulnerable to a range of cyber threats, particularly as their usage increases:

> Greater connectivity will increase the demand for consumer connectable products such as smart speakers, smart TVs and wearable technology and the digital services they enable. In 2021, the average UK household had nine consumer connectable products in their home, with many lacking basic cyber security protections. Poorly secured consumer connectable products threaten individuals' online security, and subsequently, their privacy and safety.
>
> When security flaws of products in the home are exploited, significant problems can ensue. Devices with weak security can be compromised, and be used in large-scale cyber attacks, such as Distributed Denial of Service ("DDoS") attacks. The impact of such attacks can reverberate across the wider UK, and global, economy. [2]

Examples of such threats are also provided in the government's explanatory notes to the bill:

> 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 fish tank.

---

[1] Government Office for Science, 'Trend Deck 2021: Technology', 28 June 2021.
[2] Explanatory notes, p 4.

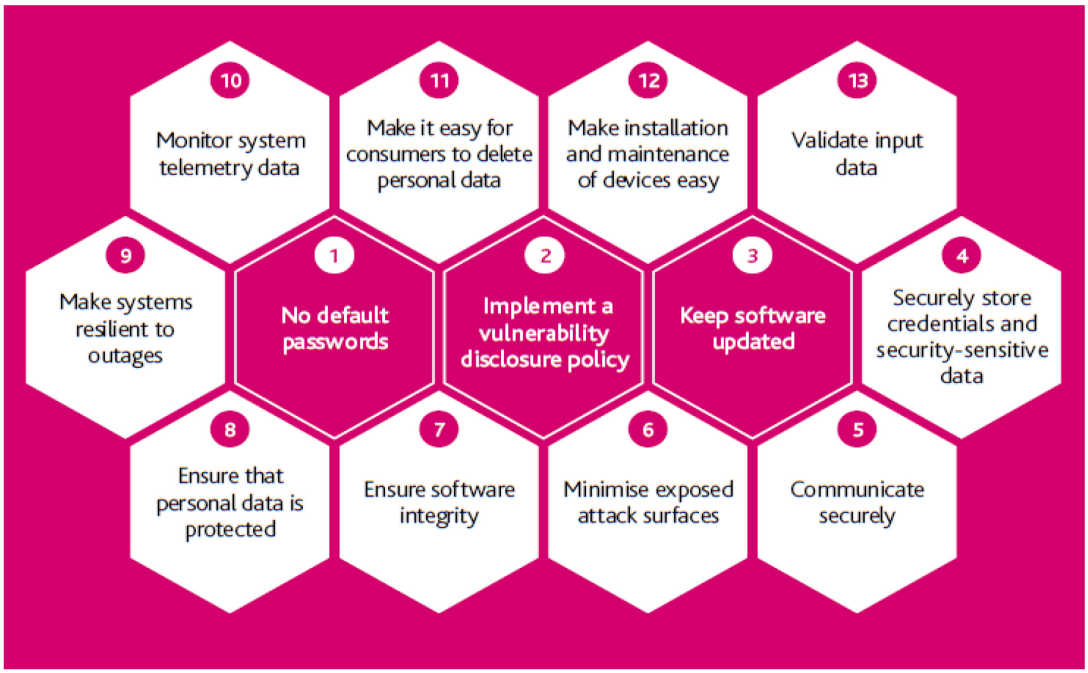
> Devices can be compromised at scale as part of DDoS or 'botnet' attacks. For example, in 2016 cyber criminals compromised 300,000 products with the Mirai malware. The attackers utilised the collective computing power to successfully disrupt the service of many news and media websites including the 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]

The government has been aware of this issue for some time. The vulnerability of smart and IoT devices was highlighted by its national cyber security strategy in 2016, which also included an objective that most online products and services should become "secure by default" by 2021.[4]

In 2018, the government published its secure by design report, calling for greater action in this area.[5] It was accompanied by a (non-mandatory) code of practice for consumer IoT security, developed in coordination with industry.[6] The code provided 13 good practice guidelines for manufacturers and others to increase security, including ensuring that consumer connectable products do not have universal default passwords when sold; that it should be easy for consumers to delete their personal data; and that manufacturers and others should implement a security vulnerability disclosure policy to ensure that such weaknesses are monitored, identified, rectified and reported to stakeholders.

The code's full list of guidelines is represented in the infographic below.

[3] Explanatory notes, p 5.
[4] HM Government, 'National cyber security strategy 2016 to 2021', 1 November 2016.
[5] Department for Digital, Culture, Media and Sport, 'Secure by design', 2018.
[6] Department for Digital, Culture, Media and Sport, 'Code of practice for consumer IoT security', 2018.



(Department for Digital, Culture, Media and Sport, 'Code of practice for consumer IoT security', 2018)

At the time of the publication of the code, the government said that its preference would be for the "market to solve this problem", but that if this did not happen it would look to introduce measures through legislation.[7]

Subsequently in 2019, the government published a consultation on introducing a regulatory approach to connectable products' security. As part of that exercise, it acknowledged that self-regulation had not worked.[8] The consultation documents noted that companies which manufactured smart devices had been disincentivised by costs relating to supply chains, and that companies who attempted to invest resources into securing their products risked losing a competitive market advantage.[9]

In its consultation response published in 2020, the government said that it intended to introduce primary legislation to give the secretary of state regulation making powers to introduce security requirements for devices on sale in the UK. Following feedback on making all the elements in the code of practice mandatory, and fears about the burden this would place on industry,

[7] House of Commons Library, 'The Product Security and Telecoms Infrastructure Bill', 20 May 2022, p 11.
[8] Department for Digital, Culture, Media and Sport, 'Consultation on the government's regulatory proposals regarding consumer Internet of Things (IoT) security', updated 3 February 2020.
[9] Department for Digital, Culture, Media and Sport, 'Consultation on the government's regulatory proposals regarding consumer Internet of Things (IoT) security', updated 3 February 2020.

the government said that it had concluded that the top three guidelines from the code should be the focus. These were as follows:

1. IoT device passwords must be unique and not resettable to any universal factory setting.
2. Manufacturers of IoT devices need to provide a public point of contact as part of a vulnerability disclosure policy.
3. Manufacturers of IoT devices need to explicitly state the minimum length of time for which the product will receive security updates.[10]

Later in 2020, the government consulted on the detail of the proposed legislation, publishing its response in 2021. In it, ministers said that the government intended that a range of devices would be covered by the legislation but that some exemptions would be made as a result of specific circumstances:

> The government will now legislate, when parliamentary time allows, to create a new robust scheme of regulation to protect consumers from insecure connected products. The regulation will apply to all consumer connected products such as smart speakers, smart televisions, connected doorbells and smartphones. A number of devices will be exempt due to the specific circumstances of how they are constructed and secured, including desktop computers and laptops. The security requirements will align with international standards and are familiar to all manufacturers and other relevant parties across the industry. An enforcement body will be equipped with powers to investigate allegations of non-compliance and to take steps to ensure compliance.
>
> This legislation, which will apply across the whole of the UK, will protect consumers at home, but also demonstrate our continued global leadership in cyber security. In 2016 our objective within our national cyber security strategy was that the majority of online products and services coming into use become 'secure by default' by 2021. We have seen successes through the publication of our code of practice, and the adoption of these thirteen principles abroad and within globally applicable standards from international standards bodies. However, aspects of industry still persist in using out-of-date and dangerous practices (such as universal default passwords), and the risk to consumers can no longer be tolerated. Our proposed legislation will further close the door on insecure technology.[11]

---

[10] Department for Digital, Culture, Media and Sport, 'Consultation on the government's regulatory proposals regarding consumer Internet of Things (IoT) security', updated 3 February 2020.

[11] Department for Digital, Culture, Media and Sport, 'Government response to the call for views on consumer connected product cyber security legislation', 21 April 2021.

The specific measures included in the bill are detailed in section 2 of this briefing.

1.2 Part 2: Telecommunications infrastructure

Part 2 of the bill would make changes to the electronic communications code (ECC), which governs the rights of telecoms companies to install infrastructure on land.[12] Specifically, it aims to encourage faster and more collaborative negotiations for the installation and maintenance of telecoms equipment on private land.

Significant reforms to the ECC were introduced in 2017, implemented by the Digital Economy Act 2017.[13] This included changes to the way in which rent for hosting telecoms equipment on land is calculated when a court is imposing an agreement under the ECC. Under those provisions, rent is now determined based on the value of the land to the site provider without taking account of its value as a telecoms site. This is called the "no network assumption" or "no scheme" valuation approach.[14]

The 2017 reforms to land valuations have reportedly led in some cases to a dramatic reduction in rents for hosting infrastructure.[15] Observers such as the Centre for Cities also report that such reduced rents have meant that site providers are less willing to engage with operators, resulting in delays to rolling out infrastructure.[16] Indeed, the Law Society have said the reforms have failed to achieve the appropriate balance between the needs of operators and landowners:

> [The reforms] have tilted the balance of rights too heavily in favour of operators to assist them in securing site facilities in practical terms.
>
> The implied presumption in favour of operators has resulted in site providers being on an unequal footing when challenging decisions, with many reacting with obstruction, unwillingness to cooperate and litigation.[17]

A survey of the telecoms industry by the Centre for Policy Studies found that approximately 80% of negotiations were taking over six months to

---

[12] The ECC is contained within the Communications Act 2003, schedule 3A (as amended).
[13] Digital Economy Act 2017.
[14] House of Commons Library, 'The Product Security and Telecoms Infrastructure Bill', 20 May 2022, p 22.
[15] House of Commons Library, 'The Product Security and Telecoms Infrastructure Bill', 20 May 2022, p 22.
[16] Centre for Cities, 'Delivering change: How cities can make the most of digital connections', 12 July 2018.
[17] Law Society, 'Changes to the electronic communications code: Law Society response', 20 April 2021.

complete and that average negotiating time was 11 months.[18]

The government consulted on changes to the ECC in 2021. It identified three main areas of reform:

- Issue 1: Obtaining and using code agreements.
- Issue 2: Rights to upgrade and share apparatus.
- Issue 3: Expired agreements.[19]

However, the consultation did not revisit the issue of land valuation and compensation for site providers. In the consultation document, the government said that it recognised that these reforms had had an impact but that its position on the valuation regime was unchanged:

> We recognise that the 2017 code reforms had an impact on site providers' willingness to agree or renew code rights. In particular, some stakeholders have expressed the view that changes to the code's valuation provisions, and the reductions in the amounts paid to site providers that those reforms were intended to deliver, have made entering these agreements significantly less attractive for site providers.
>
> The government's policy position on this valuation regime has not changed. We still believe that underpinning negotiations with the valuation model (ie that set out in paragraph 24 of the code) is appropriate for the installation and maintenance of digital communications infrastructure systems. We do not intend to revisit the valuation framework contained in the electronic communications code.[20]

The document added that the government did not believe disagreement on financial terms was the only reason why negotiations were taking longer:

> We do not think that disagreements about financial terms are the only reason that negotiations are not progressing as smoothly as they could be. Other issues have been brought to our attention, including: non collaborative behaviour or poor communications by operators, occupiers and professional representatives; a lack of trust between negotiating parties; and concerns about ensuring both parties adhere

[18] Centre for Policy Studies, 'Upwardly mobile: How the UK can gain the full benefits of the 5G revolution', 2021.
[19] Department for Digital, Culture, Media and Sport, 'Access to land: Consultation on changes to the electronic communications code—government response', 24 November 2021.
[20] Department for Digital, Culture, Media and Sport, 'Access to land: Consultation on changes to the electronic communications code', 27 January 2021, pp 19–20.

> to the terms of a completed agreement.
>
> We think changes are needed that will encourage more collaborative negotiation and offer ways for disagreements to be dealt with quickly and cheaply.[21]

Following the consultation, the government intends to implement reforms through the bill which 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.[22] Those measures are set out in detail in the next section of this briefing, but include:

- New measures to actively encourage alternative dispute resolution rather than legal proceedings.
- A new procedure allowing operators to get temporary rights to access land where an owner is unresponsive.
- Changes to drafting regarding the renewal of expired agreements.
- Alterations to the 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 to what can be sought as temporary, interim orders while a code agreement is being renewed.

2. Measures in the bill: Clause by clause

2.1 Part 1: Product security

Chapter 1: Security requirements (clauses 1 to 7)

Clause 1 of the bill would introduce regulation-making powers for the secretary of state to introduce requirements to improve the security of consumer connectable products sold in the UK. As above, the government intends to use these powers to introduce the top three guidelines from the code of practice:

- a ban on default passwords
- a requirement for a vulnerability disclosure policy

---

[21] Department for Digital, Culture, Media and Sport, 'Access to land: Consultation on changes to the electronic communications code', 27 January 2021, pp 19–20.
[22] Department for Digital, Culture, Media and Sport, Access to land: Consultation on changes to the electronic communications code—government response', 24 November 2021.

- transparency requirements on the time period a manufacturer will provide security updates

Clause 2 would make further requirements about the regulations that can be introduced under clause 1, including that a security requirement may be ongoing and require action in respect of a product that is already on the market in the UK. It also provides that regulations made under clause 1 would be made under the affirmative procedure unless they make very limited changes.

Clause 3 would provide that security requirements which wholly satisfy exacting conditions such as an international standard (such as the European Standard EN 303 645, for example) can be specified in regulations as meeting the relevant standards in the UK.

Clause 4 would provide that a relevant product is an internet or network connectable device (and not an excepted product specified in clause 6). An internet connectable device is one which can connect to the internet. Clause 5 defines a network connectable product as one which is not connected to the internet but can send and receive data and may connect to other products capable of connecting to the internet.[23]

The government has said that it intends the following products to be covered 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[24]

[23] For further detail, see the explanatory notes (pp 11–12).
[24] Department for Digital, Culture, Media and Sport, 'The Product Security and Telecommunications Infrastructure (PSTI) Bill: Product security factsheet', 24 November 2021.

Some products would be excluded from the provisions to avoid the issue of dual regulation. They include smart meters, smart chargepoints, medical devices and vehicles.[25] Clause 6 of the bill would provide regulation making powers for the secretary of state to specify which products are not considered relevant to the provisions of clause 1.

Clause 7 would define the 'relevant persons' to whom the regulations would apply as manufacturers, importers and distributors of a product.

Chapter 2: Duties of relevant persons (clauses 8 to 25)

Clause 8 would establish a duty for a manufacturer to comply with security requirements for a product in the UK. Clause 9 would also provide that a manufacturer must make a certificate of compliance available with the connectable product.

Clauses 10 and 11 would place a duty on manufacturers to investigate potential compliance failures and act where this is identified. The manufacturer must take all reasonable action to prevent the product being sold and must notify the enforcement authority of any compliance failure. Clause 11 provides regulation-making powers to this effect, and also sets out the information that must be provided. Clause 12 would also require that a manufacturer must keep records of any compliance failure investigations and compliance failures.

Clause 13 would enable manufacturers not based in the UK to nominate an authorised person to perform its duties under the legislation.

Clauses 14 to 19 would place duties on importers of a connectable product that are equivalent to those on manufacturers. Clause 19 would also require that, if an importer becomes aware of a compliance failure, they must notify the manufacturer as soon as possible. Clause 20 would again require that records of any failures or failure investigations in this context are kept.

Clauses 21 to 25 would place duties on a distributer equivalent to those placed on importers.

Chapter 3: Enforcement (clauses 26 to 52)

Clause 26 of the bill would make the secretary of state responsible for enforcing the measures in part 1, amending the Consumer Rights Act 2015 to provide powers of investigation. However, clause 27 would also allow the delegation of these powers to an authorised person.

---

[25] Explanatory notes, p 12.

Clauses 28, 29 and 30 would enable the secretary of state to issue compliance orders, stop notices and recall notices where there are reasonable grounds to suspect a lack of compliance with the security requirements. Clause 31 would provide the power to vary or revoke enforcement notices.

Clause 32 would provide that any person who fails to comply with an enforcement notice has committed an offence. Clause 33 would allow the right of appeal against enforcement notices and clause 34 for compensation where stop or recall notices are wrongly given. Clause 35 further sets out the detail on appeal provisions under clause 34.

Clauses 36 to 38 would specify the financial penalties and fines that can be imposed. They include setting the maximum penalty for breaches as the greater of £10mn or 4 percent of the qualifying worldwide revenue for the most recent complete accounting period.[26]

Clauses 39 and 40 would set out further provision on penalty notices, including the procedure for their enforcement in England and Wales, Scotland, and Northern Ireland. Clause 41 sets out appeal provisions for penalty notices.

Clauses 42 to 44 would set out the conditions under which the secretary of state can apply to the courts for the forfeiture of products, the process for doing so, and the appeals process. Clause 45 provides a power for the secretary of state to publish information about the compliance failure.

Clause 46 would provide the power to publish details of enforcement action taken against relevant persons, and clause 47 provides the secretary of state with the power to recall non-compliant products.

Clause 48 would provide for information disclosure measures with regard to the secretary of state's enforcement functions. Clause 49 would also provide for an offence of wrongly purporting to act as authorised to exercise an enforcement function.

Clause 50 would provide for the means through which notices can be given. Clause 51 sets out that when an overseas manufacturer engages the services of a UK authorised person, that person must comply with those duties. Finally, clause 52 would provide for the liability of a director, manager, secretary, or other similar officer of a corporate body, or any person purporting to act in such a capacity.

[26] Explanatory notes, p 26.

Chapter 4: Supplementary provisions (clauses 53 to 56)

Clauses 53 to 56 make further supplementary provisions, including further defining terms relevant to part 1 and providing the secretary of state with the power to issue guidance.

Timescales, assessments of cost to business and stakeholder reaction to part 1

The factsheet published alongside the bill states that manufacturers will be given time to implement the required standards:

> The government is committed to ensuring that businesses are given an appropriate amount of time to adjust their business practices before instances of non-compliance are actively enforced against. Following royal assent of the bill, the government will provide at least 12 months notice to enable manufacturers, importers and distributors to adjust their business practices before the legislative framework fully comes into force.[27]

An impact assessment of the measures in part 1 of the bill was published by the government in May 2021, which estimated a cost to business per year of £23.9mn (in 2019 prices).[28]

The provisions in part 1 have largely been welcomed by cyber security experts and industry stakeholders. Dr Ian Levy, Technical Director of the National Cyber Security Centre (NCSC) said:

> I am delighted by the introduction of this bill which will ensure the security of connected consumer devices and hold device manufacturers to account for upholding basic cybersecurity.
>
> The requirements this bill introduces—which were developed jointly by DCMS [Department for Digital, Culture, Media and Sport] and the NCSC with industry consultation—mark the start of the journey to ensure that connected devices on the market meet a security standard that's recognized as good practice.[29]

---

[27] Department for Digital, Culture, Media and Sport, 'The Product Security and Telecommunications Infrastructure (PSTI) Bill: Product security factsheet', 24 November 2021.
[28] Department for Digital, Culture, Media and Sport, 'Impact assessment: Regulation of consumer connectable product cyber security', 21 May 2021.
[29] Info security magazine, 'UK introduces new cybersecurity legislation for IoT devices', 24 November 2021.

Consumer groups such as Which? have said that the bill will need to be backed up by rigorous enforcement so that consumers get effective redress when they purchase devices that fail to meet security standards which leave them exposed to cyber threats.[30]

CEO of the Chartered Institute of Information Security, Amanda Finch, has also said that the process of developing security measures should not stop with the bill, but should be a constant process of review and refinement taking account of new developments and technologies.[31] She added that "attackers and, sadly, unscrupulous manufacturers and vendors, are endlessly creative" in exploiting security vulnerabilities.

Kim Bromley, a senior analyst at Digital Shadows, said the UK may struggle to enforce these regulations on overseas manufacturers, drawing particular attention to those in China, placing a large burden on UK importers and distributers:

> Some [Chinese] manufacturers release products that are cheaper than other products on the market, and therefore users will continue to buy products that may contain security flaws, or at the very least, do not comply with UK legislation. […] The new requirements will also place huge burdens on UK resellers that may use manufactured products [from China] on their own; keeping pace with the requirements and changing working practices could prove difficult.[32]

Others have also warned about the increased burdens for manufacturers created by the regulations. Martin Tyley, Head of Cyber at KPMG, said the extra regulations could overwhelm smaller manufacturers in particular, and called for more government support and guidance.[33]

2.2 Part 2: Telecoms infrastructure

Part 2 of the bill deals with telecoms infrastructure and proposed reforms to the ECC to ensure the quicker rollout of infrastructure, particularly the expansion of mobile, full fibre and gigabit capable networks across the UK.

---

[30] Which?, 'Which? response to Product Security and Telecoms Infrastructure Bill unveiled in the Queen's speech', 11 May 2021.
[31] Techcrunch, 'Is the UK government's new IoT cybersecurity bill fit for purpose?', 4 December 2021.
[32] Techcrunch, 'Is the UK government's new IoT cybersecurity bill fit for purpose?', 4 December 2021.
[33] IoT News, 'UK introduces PSTI bill to protect IoT devices', 25 November 2021.

Defining 'occupiers' and rights to upgrade and share (clauses 57 to 60)

Clause 57 of the bill would clarify an 'occupier' in the context of the ECC. Currently, difficulties have arisen when the telecoms operator is the occupier and a new renewed code agreement is required, because the operator cannot grant code rights to itself.[34] The clause would add a new provision stating that, where land is exclusively occupied by an operator, code rights can be granted by whoever manages or controls the land.

Clauses 58 to 60 would amend rights under the ECC to share apparatus between operators and the right to upgrade equipment. Such upgrades are important in the context of the roll out of 5G networks, which are largely installed on top of existing masts. In addition, for fixed-line broadband, upgrading and sharing rights are often needed to utilise existing underground tunnels or ducts and poles that already host cables to replace them with fibre-optic cables.[35]

The automatic right to upgrade and share was introduced as part of the 2017 ECC reforms. However, it only applied to agreements entered into after this point and the government's 2021 consultation response observed that around 80% of the UK's telecoms networks were installed prior to this date.[36] As a result, the measures would apply this right to pre-2017 agreements under limited circumstances as set out in the bill (they include when upgrading and sharing would have no adverse impact on the land).

The bill would also provide such rights with regard to equipment installed before 2003 (when the ECC came into force) for which there may not be evidence of a code agreement.

Renewal of expired agreements (clauses 61 to 65)

Clauses 61 to 65 would make provision for all code agreements when renewed by a court order, including those made prior to 2017, to be done so on land valuation terms consistent with the 2017 code. The clauses would apply to England and Wales or Northern Ireland only.

These measures are a response to a consequence of the 2017 ECC reforms on the treatment of certain expired code agreements which are up for

---

[34] House of Commons Library, 'The Product Security and Telecoms Infrastructure Bill', 20 May 2022, p 26.
[35] House of Commons Library, 'The Product Security and Telecoms Infrastructure Bill', 20 May 2022, pp 26–7.
[36] Department for Digital, Culture, Media and Sport, 'Access to land: Consultation on changes to the electronic communications code—government response', 24 November 2021.

renewal. The issue is set out in the government's 2021 consultation response as follows:

> The 2017 reforms introduced clear procedures relating to the termination and renewal of expired code agreements. These are dealt with in part 5 of the code. However, part 5 does not apply to all code agreements. Leases that are regulated by other statutory frameworks are specifically excluded, and the courts have also held that part 5 cannot be used in certain circumstances where there is no written evidence of continuing code rights.
>
> Since the 2017 reforms came into force, there has been disagreement about how code agreements not covered by part 5 should be treated on expiry, with a number of cases being brought before the courts. The position in relation to expired code agreements regulated by other statutory frameworks has been clarified. But there continues to be uncertainty about the position of these and other expired agreements and how operators can either renew those agreements and/or obtain new code rights.
>
> We believe that the present situation on expired code agreements does not reflect the policy aims of the 2017 reforms. When those reforms were introduced, we were clear that we did not think they should have retrospective effect. By this, we meant that the new rights and protections introduced by the reforms should not be automatically extended to existing and ongoing code agreements.
>
> […]
>
> Problems with the existing procedure for renewing code agreements is creating particular problems in relation to 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.[37]

As a result, the government said that it intended to do the following:

> [The government will] bring forward provisions to amend legislation

[37] Department for Digital, Culture, Media and Sport, 'Access to land: Consultation on changes to the electronic communications code—government response', 24 November 2021.

> that applies to code agreements currently excluded from the scope of part 5 so that the procedures for dealing with any renewal dispute, and the terms of any new code agreement (including any financial terms) imposed will be more closely aligned to part 5, where the main aim of that agreement is to confer code rights. In England and Wales, this means we will introduce changes to the Landlord and Tenant Act 1954 ('the 1954 act'). Equivalent changes will be made to the Business Tenancies Order (Northern Ireland) 1996 ('the BTO 1996') to ensure consistency across the UK.
>
> These changes will ensure that while the procedure and framework is more closely aligned to part 5, in so far as the renewed agreement will relate to code rights, other statutory provisions and protections provided for by the 1954 act or the BTO 1996 will be retained.
>
> The changes we intend to make will include transferring jurisdiction for the resolution of disputes under the 1954 act from the county court to the first-tier and upper tribunal, who deal with all other code cases. These changes will not be needed in Northern Ireland, where BTO 1996 disputes are already dealt with by the lands tribunal.[38]

Unresponsive operators (clause 66)

Clause 66 would introduce new provisions into the ECC setting out a new procedure for operators to gain temporary access to land when a site provider does not respond to repeated requests for access. The ECC does offer a route through the courts to gain access rights, but operators have argued that this is costly and lengthy. Clause 66 aims to create a faster process for operators to gain access in these circumstances. Certain conditions would be applied to the provisions, including that it would only apply to 'relevant land' not covered by buildings or used as a garden, park or other recreational area.[39]

Interim orders (pending determination of certain applications under the ECC) (clause 67)

Currently, the ECC only allows site providers, and not operators, to apply for an order through the courts regarding the amount of rent which should be paid on an interim basis when both parties cannot agree on the terms of a renewal agreement and the full amount is in the process of being determined. The bill would amend this so that either party can apply for

---

[38] Department for Digital, Culture, Media and Sport, 'Access to land: Consultation on changes to the electronic communications code—government response', 24 November 2021.
[39] House of Commons Library, 'The Product Security and Telecoms Infrastructure Bill', 20 May 2022, p 32.

such an interim order.

Use of alternative dispute resolution (clause 68)

Clause 68 would add provisions to the ECC to encourage the use of alternative dispute resolution (ADR) to settle disputes rather than the courts. The government intends that this will make dispute resolution quicker and less costly:

> After considering the responses to this consultation, the government agrees that greater use of ADR would help parties reach a code agreement, or agree that the land or property would not be suitable for the operator's purposes, more quickly and cheaply than going through the courts. Even where parties are unable to reach an agreement via ADR, the process should assist the parties in at least narrowing down the issues between them. This in itself is useful, as it reduces the amount of resources and court time needed to determine the dispute.
>
> We are not proposing to make ADR mandatory before a case can be referred to the courts, as we recognise there will be situations, for example, where there is a point of law in dispute, where this might not be suitable.
>
> We also note operators' concerns that ADR should not delay the overall time it takes for cases to be heard by the courts. However, under the current court procedure rules, there is already provision to ensure ADR does not have a negative impact on the courts' timescales, unless otherwise agreed by the parties. We therefore do not think we need to introduce specific measures on this point.
>
> However, we do want to make sure that use of ADR, rather than litigation through the courts, is encouraged wherever possible, to promote better engagement between the parties during negotiations and assist in disagreements being resolved in a more collaborative way.[40]

Complaints about the conduct of operators (clause 69)

Clause 69 would place an obligation on Ofcom to include guidance concerning how operators handle complaints about their conduct in a code of practice published under paragraph 103 of the ECC. The government

[40] Department for Digital, Culture, Media and Sport, 'Access to land: Consultation on changes to the electronic communications code—government response', 24 November 2021.

consultation considered whether a statutory complaints/compliance process should be introduced. Most site providers and professional bodies were in favour of such a measure, though most operators were not.[41] The government has said that it does not intend to pursue a mandatory process but that discussions were ongoing between the telecoms industry and site providers on potential reforms to Ofcom's code of practice.[42]

Jurisdiction of First-tier Tribunal in relation to code proceedings in Wales (clause 70)

This clause makes amendments to paragraph 95 of the ECC. Currently paragraph 95 gives the secretary of state power to confer jurisdiction for Code disputes on both the First-tier Tribunal or the Upper Tribunal in relation to England, but only on the Upper Tribunal in relation to Wales. This clause would amend that power so that the secretary of state can confer jurisdiction for code disputes on the First-tier Tribunal, as well as the Upper Tribunal, in relation to Wales. This clause was introduced at report stage, as discussed below.

Power to impose time limits on the determination of code proceedings (clause 71)

Clause 71 would enable the secretary of state to introduce regulations which set out the time period within which applications made under the ECC must be determined. Such a specification may include the extension or removal of any time limits, or the application of different time limits to different types of proceedings (provided they are in scope of the provisions).

Rights of network providers in relation to infrastructure (clause 72)

Clause 72 would give powers to the secretary of state to make regulations concerning the rights of network providers in respect of relevant infrastructure required for the purpose of facilitating the development of public electronic communications networks. The circumstances in which such regulations can be made are set out in the explanatory notes.[43] They include that, before making such regulations, the secretary of state must consult Ofcom and others considered "appropriate".

---

[41] House of Commons Library, 'The Product Security and Telecoms Infrastructure Bill', 20 May 2022, p 33.
[42] House of Commons Library, 'The Product Security and Telecoms Infrastructure Bill', 20 May 2022, p 33.
[43] Explanatory notes, p 45.

Stakeholder reaction to the measures in part 2

As noted in the government's response to its 2021 consultation exercise, property owners and telecoms operators had opposing views on almost all the proposed changes including those incorporated into the bill.[44]

Telecoms and mobile industry stakeholders have welcomed many of the changes in the bill. Speed Up Britain, a campaign group for better mobile connectivity, said the measures would help speed up the UK's move to a more digital capable economy:

> The Campaign is delighted the government plans to move forward with code reform and is optimistic about the potential this move has to transform connectivity in the UK, speeding up Britain and enabling the country to fulfil the promise of a truly connected future.[45]

In contrast, Protect and Connect, a campaign group led by land and property owners, said it was disappointed that the government had not changed its position on valuation, and that it was worried about a number of measures in the bill which would further erode the position of landowners. In its submission to the public bill committee in the House of Commons, Protect and Connect said:

> If not corrected, the bill as drafted will make things worse: further damaging the interests of communities and small site providers, further holding back roll-out [of 5G] while providing further subsidies to operators who already make multi-billion pound profits. This is at a time where those operators have announced increases in consumer pricing, while simultaneously receiving direct state funding to cover areas they have failed to cover, such as the shared rural network.[46]

In its submission, Protect and Connect called for:

- a "fair" valuation system that incentivises site owners to host infrastructure
- rent changes not to be backdated to before the court's decision to avoid bankruptcies caused by backdated payments and respect existing contracts

---

[44] Department for Digital, Culture, Media and Sport, 'Access to land: Consultation on changes to the electronic communications code—government response', 24 November 2021.
[45] Speed Up Britain, 'Speed Up Britain reacts to Queen's speech commitment to propose code reform', 17 May 2021.
[46] Protect & Connect, 'Protect & Connect submission to the Product Security and Telecommunications Infrastructure Bill Committee', accessed 27 May 2022.

- changes to the definition of the term 'occupier' to avoid unintended consequences if this is interpreted wider than the specific circumstances intended in the consultation response
- further measures against abuse by telecoms companies[47]

In its response to the 2021 consultation, the Law Society also voiced concerns that the measures proposed in the bill would fail to tackle the "root causes" of disputes between landowners and operators, particularly around land valuation.[48]

2.3 Part 3: Final provisions

Part 3 of the bill provides for measures such as the territorial extent of the bill and commencement arrangements.[49]

3. House of Commons stages

3.1 Second reading

Second reading of the bill took place in the House of Commons on 11 May 2022. Opening the debate, Secretary of State for Digital, Culture, Media and Sport Nadine Dorries, said:

> As we have upgraded our networks, we have invested more than £4 billion in our cyber defences since 2016, including by setting up the National Cyber Security Centre. As we all know, the nature of tech is incredibly fast-paced and constantly changing and growing. Monthly broadband usage has doubled since 2018 and continues to rise year on year. But the more we log on, the more open we are to cyber-threats, particularly as new technology—including cutting-edge consumer products such as smart baby monitors—is not always secure by design. To stay ahead of the game we need to keep investing in tomorrow's networks and to secure ourselves against future threats, which is why we have introduced the bill.[50]

On telecoms infrastructure, she added:

> We need to ensure that the legal framework underpinning our digital infrastructure encourages and enables the deployment of the latest

[47] Protect & Connect, 'Protect & Connect submission to the Product Security and Telecommunications Infrastructure Bill Committee', accessed 27 May 2022.
[48] Law Society, 'Changes to the electronic communications code: Law Society response', 20 April 2021.
[49] Explanatory notes, p 46.
[50] HC Hansard, 26 January 2022, cols 1025–32.

> networks. In 2017, we made changes to that legal framework. Implementing reforms to the electronic communications code […] requires installation agreements between landowners and telecom operators. The aim was to make it easier for digital networks to be installed, maintained and upgraded, and now we will go even further. The bill will update the electronic communications code to deliver on the government's ambitions for digital connectivity and levelling up. Specifically, it will do three things: make the most of existing infrastructure; encourage stronger and more collaborative relationships between telecom operators and site providers; and build on previous measures to tackle the issue of non-responsive landowners.[51]

Ms Dorries also said that the government had listened to landowners in bringing forward the proposals:

> We have listened to landowners. We have not introduced the legislation without involving them in its development. We have included measures in the bill that make it easier for landowners and operators to use a dispute resolution if landowners feel that they are not getting a fair price. That means greater collaboration, and it makes preposterously low offers less likely. Hopefully, a fair and reasonable price would be agreed. If landowners were not happy with it, it would go to independent arbitration. If they were then unhappy with that, they would have recourse to the courts, which we know would look very dimly on a situation where the telecom providers had been neither reasonable nor fair to landowners. We think that that is a fair and reasonable process.[52]

Speaking for the Labour front bench, Lucy Powell, the Shadow Secretary of State for Digital, Culture, Media and Sport, said that she welcomed the measures in part 1 of the bill.[53] However, she did question why they were being introduced now given the government's 2016 commitment that devices would be "secure by default" by 2021. She also voiced concerns about the UK being slow to act in response to new technologies:

> I have real concerns that we are always behind the technology curve. These devices are already being used in ways beyond the scope of this bill—for example, by stalkers and abusive partners in tracking those they are abusing, as well as in fraud and criminal activity. There is nothing in this bill about that, let alone measures to address new waves of technology that are already making their way into people's homes and lives, such as virtual reality.[54]

---

[51] HC Hansard, 26 January 2022, cols 1025–32.
[52] HC Hansard, 26 January 2022, cols 1025–32.
[53] HC Hansard, 26 January 2022, cols 1032–5.
[54] HC Hansard, 26 January 2022, cols 1032–5.

On the measures in part 2 of the bill, Lucy Powell said that Labour's main concern was that they were more likely to "slow down, rather than speed up, the broadband and 5G roll-out".[55] She added:

> The unequal roll-out of next generation gigabit broadband will mean that the same households that do not have superfast or, in many cases, as we have already heard, any functioning broadband at all, will continue to fall behind—for years, if not decades, to come. As the Public Accounts Committee said last week, the government have no detailed plan in place for reaching communities where it is not commercially viable to do so, and there is little in the bill to address that key issue.
>
> The bill does make further changes to the electronic communications code, which governs the agreements between telecoms companies and the landowners who host their masts. The code was last updated as recently as 2017, but those changes have not had the desired effect of speeding up roll-out.
>
> Despite promises that rent would not reduce by more than 40%, many community sports grounds, churches and local authorities that host phone masts have had their rents cut by up to 90% or even 95% in some of the cases that we have already heard about today. That will be further exacerbated by the bill, which hands more power to the telecoms companies in court and disincentivises people from coming forward to have phone masts put on their land in the first place.[56]

For the SNP, shadow DCMS spokesperson, John Nicholson, said that he was seeking clarity from the government over the powers of the Scottish government to regulate connectable products in Scotland.[57] He also said that whilst the SNP was in favour of reform of the ECC in principle, "the need for a fast roll-out must be balanced with the rights of landowners, such as farmers".[58]

3.2 Committee stage

The bill's public bill committee stage in the House of Commons began on 17 March 2022. The committee held five sittings, concluding on 22 March 2022.[59]

---

[55] HC Hansard, 26 January 2022, cols 1032–5.
[56] HC Hansard, 26 January 2022, cols 1032–5.
[57] HC Hansard, 26 January 2022, cols 1036–7.
[58] HC Hansard, 26 January 2022, cols 1036–7.
[59] House of Commons Public Bill Committee, 'Product Security and Telecommunications Infrastructure Bill', 15–22 March 2022, session 2021–22.

Part 1 of the bill was not amended during committee stage. Several opposition amendments were moved, but only one was pressed to a division. Amendment 7, which would have considered online marketplaces as product distributors. It was defeated by 8 votes to 4.[60]

The government made five amendments to part 2 of the bill at committee stage, all of which were technical or consequential in nature, and passed without votes. Several opposition amendments were moved to part 2. They included:

- A new clause requiring a full economic review of the effect of the ECC, defeated on division by 9 votes to 4.[61]
- A new clause introducing a requirement to consult on imposition of minimum periods of time for which products would need to receive security updates, which was defeated by 10 votes to 4.[62]
- Amendment 9 (and related amendments 10, 11 and 12) which would apply a different regime under the ECC to private landlords, giving automatic upgrade rights for operators to properties owned by private landlords subject to the condition that the upgrading imposes no additional burden on the other party to the agreement. All four amendments were pressed to a vote, and all were defeated by 7 votes to 4.[63]
- Amendment 8 which would provide a legal guarantee that site providers' rents fall by no more than 40% under any new agreement. It was defeated by 7 votes to 4.[64]

3.3 Report stage

The bill was carried over into the 2022–23 session and report stage of the bill took place on 25 May 2022. The government moved several amendments at report stage, as set out below, which were agreed without division. Several opposition and backbench amendments were also moved, one of which was pressed to a division where it was defeated. The remaining opposition and backbench amendments were withdrawn.

---

[60] House of Commons Public Bill Committee, 'Product Security and Telecommunications Infrastructure Bill', 17 March 2022, session 2021–22, 3rd sitting, col 78.
[61] Public Bill Committee, Product Security and Telecommunications Infrastructure Bill, 17 March 2022, session 2021–22, 4th sitting, col 123.
[62] Public Bill Committee, Product Security and Telecommunications Infrastructure Bill, 17 March 2022, session 2021–22, 4th sitting, col 126.
[63] Public Bill Committee, Product Security and Telecommunications Infrastructure Bill, 17 March 2022, session 2021–22, 3rd sitting, cols 92–6.
[64] Public Bill Committee, Product Security and Telecommunications Infrastructure Bill, 17 March 2022, session 2021–22, 3rd sitting, col 105.

Government new clause 1 (and consequential amendments 1 to 3): Meaning of "occupier" in relation to land occupied by an operator

Julia Lopez, minister of state at the Department for Digital, Culture, Media and Sport, moved new clause 1 on those who are defined as 'occupiers' of land in the context of ECC rights. In other words, those who can grant rights for operators to install and maintain telecoms equipment on the land.

Introducing the new clause, Julia Lopez noted that some operators with apparatus on land are currently unable to follow an existing statutory process to renew their agreement once it ends. In addition, they cannot get a new agreement because only the occupiers can grant code rights and operators cannot grant such rights to themselves.

Clause 57 of the bill (as introduced) was intended to solve this issue by ensuring that operators could obtain code rights from another party in these circumstances. However, the minister said that subsequent engagement with stakeholders had made it clear that the provisions would not cover all scenarios, and that "a more focused approach" was required.[65]

As such, she said new clause 1 would replace clause 57, and was drafted to take account of these more complex situations:

> The new clause will ensure that all operators in exclusive occupation of land who do not have a statutory renewal option can still seek a code agreement. The person who can grant those code rights will usually be the owner of the land, although the new drafting makes provision for less straightforward situations. As well as resolving the problem of "stuck" operators, new clause 1 also assists operators with an existing, ongoing agreement. Where such operators need additional code rights that are not already provided by their current agreement, the new clause ensures they can seek such rights. Currently, some such operators are unable to do so because they are in occupation of the land.[66]

The minister said this would not let an operator unilaterally change, or ask the court to impose a change to, the terms of their current agreement. It is intended to allow additional code rights to be conferred on the operator via a new, separate code agreement. She added that if a consensual agreement cannot be found on the additional right needed the operator would be able to ask the court to impose an additional agreement conferring those additional rights.

---

[65] HC Hansard, 25 May 2022, col 322.
[66] HC Hansard, 25 May 2022, col 322.

Julia Lopez provided the following example of how the government intended that the measures would work:

> An operator may have an existing agreement which contains a code right to install a 3-metre high mast. Subsequently, the operator realises that it needs to install a 5-metre high mast on the same piece of land. That could enable the operator to install 5G technology or to improve or expand its network. The original agreement allowing the 3-metre mast will continue to run for its remaining term, and the operator will ask the site provider to enter into a second agreement, which contains a code right allowing it to install the 5-metre high mast.[67]

Noting the speed at which advances in technology can occur, the minister added that if an operator had to wait until its existing code agreement ends before obtaining additional rights it would be unable to install the latest technology. As a result, she said "our constituents will be deprived of faster, more reliable services such as 5G and in time 6G". She added that the new clause was "vital to give UK businesses the infrastructure they need".

Responding for Labour, Chris Elmore, shadow minister for digital, culture, media and sport, said the new clause was an improvement on the government's previous attempt to define occupier in these circumstances.[68] However, he said the changes put forward were still "not watertight" when it came to preventing unintended consequences, adding:

> The new clause does not address the underlying issue that operators could theoretically use it in situations other than when existing agreements have expired, which could lead to financial consequences for small site providers who have been hard done by since the electronic communications code review in 2017. More work is needed when the bill moves to the other place to ensure it does not unintentionally punish site providers further.[69]

The new clause was added to the bill without division, as were consequential government amendments 1 to 3.[70]

Government new clause 2 (and consequential amendment 8): Jurisdiction of first-tier tribunals in relation to code proceedings in Wales

Speaking to government new clause 2, Julia Lopez said that the government intended that any disputes related to the ECC are dealt with as quickly and

[67] HC Hansard, 25 May 2022, col 323.
[68] HC Hansard, 25 May 2022, col 328.
[69] HC Hansard, 25 May 2022, col 328.
[70] HC Hansard 25 May 2022, col 337.

effectively as possible. She noted that currently paragraph 95 of the ECC allows the secretary of state to make regulations that confer jurisdiction on either the first-tier tribunal or upper tribunal in relation to England, but only the upper tribunal in relation to Wales. The current provisions state that all code disputes must commence in the upper tribunal, although in England, appropriate cases may then be handed down to the first-tier tribunal. The minister noted, however, that first-tier tribunal has greater administrative resources and more judges than the upper tribunal, meaning that code disputes can be processed and heard more quickly.[71]

As a result, Julia Lopez said that the government was introducing new clause 2 to allow for a greater role for the first-tier tribunal in hearing code disputes, including making further regulations using the power in paragraph 95 of the code as appropriate. The measures will enable the secretary of state to make regulations conferring jurisdiction on both the upper tribunal and the first-tier tribunal in Wales.

Responding for Labour, Chris Elmore said that his party had no issue with the proposals.[72]

The new clause was added to the bill without division, as was consequential government amendment 8.[73]

Government amendments 4 to 7 and backbench amendments 9 to 11: Alternative dispute resolution (ADR)

Julia Lopez moved government amendments 4 to 7 which she said had been tabled to make a minor clarification to the text of clause 68 on the use of alternative dispute resolution (also known as ADR) to "avoid any unintended interpretation of the legislation".[74] She said that clause 68 as drafted made clear that an operator can give notice at any time to a person, from whom they are seeking code rights, that they wish to engage in ADR. However, she said nowhere was it set out that such a notice can be sent from a person to the operator. As a result, the amendments would clarify that when an operator seeks code rights from a person, either the operator or that person may give notice to the other expressing a wish to engage in ADR.

At the same time, Sir Desmond Swayne (Conservative MP for New Forest West) moved amendments 9 to 11 which would make it mandatory for operators to engage in the ADR process. Speaking to the amendments, Sir Desmond said these provisions were necessary because operators had

[71] HC Hansard, 25 May 2022, col 323.
[72] HC Hansard, 25 May 2022, col 328.
[73] HC Hansard 25 May 2022, col 337.
[74] HC Hansard, 25 May 2022, col 323.

"such disproportionate power" compared to landowners.[75]

Responding to that point, Julia Lopez said that the provisions on ADR processes in the bill aimed to create more collaborative discussions between landowners and telecoms operators to ensure that litigation was only used as a last resort. She said that she believed amendments 9 to 11 were intended to achieve the same and thus she was sympathetic to that. However, she said that the government did not believe the provisions were necessary or that ADR would be appropriate in every circumstance, and further that the amendments could be counterproductive to that underlying intention. She explained:

> If ADR were compulsory, some parties would be compelled to participate in an ADR process they do not want to be involved in, and so would be less inclined to actively engage in the process. That would increase the risk that ADR would fail, which would mean that parties would have to go to court anyway. If that were the case, all that compulsory ADR would have achieved is to add an additional layer of time and costs for landowners, such as charities, sports clubs and farmers. It should also be noted that, when consulted, a clear majority of stakeholders were not in favour of compulsory ADR.[76]

Speaking for Labour, Chris Elmore said that his party welcomed the government's amendments 4 to 7, noting that while the pace of new agreements between landowners and operators had slowed in recent years, small landowners were often unable to afford the cost of going to tribunal to defend their property rights.[77] On amendments 9 to 11, Mr Elmore said that this was an issue worth further exploration in the House of Lords:

> When the bill moves to the other place, we hope that a debate can continue on the possibility of making ADR mandatory, as suggested by amendments 10 and 11, for telecoms operators before threatening to take landowners to court for an agreement to be imposed.[78]

Government new clauses 4 to 7 were added to the bill without division. Amendments 9 to 11 were withdrawn.[79]

Opposition amendments 14 to 17: Imposing a different regime under the ECC to private landlords

Chris Elmore moved amendment 14, and consequential amendments 15

---

[75] HC Hansard, 25 May 2022, col 324.
[76] HC Hansard, 25 May 2022, col 328.
[77] HC Hansard, 25 May 2022, col 330.
[78] HC Hansard, 25 May 2022, col 330.
[79] HC Hansard, 25 May 2022, col 337.

to 17, on behalf of Dame Meg Hillier (Labour MP for Hackney South and Shoreditch) which sought to apply a different regime under the ECC to private landlords. The provisions would grant operators automatic upgrade rights in respect of property owned by private landlords, subject to the "strict condition" that such upgrading imposes no additional burden on the other party to an agreement.[80]

Mr Elmore cited the backlog in upgrading sites to provide gigabit broadband, and said much of this was a result of difficulty accessing a large number of properties owned by absentee landlords who "have little to no incentive to respond to requests to upgrade and improve connectivity".[81] He cited statistics which stated that the operator Openreach had been unable to access 620,000 multiple dwelling unit (MDU) properties, including 65,000 added since December 2021 alone.[82]

He said that amendments 14 to 17 would not give operators carte blanche to act as they chose. On the contrary, the conditionality imposed by the amendments would ensure that automatic upgrade rights can only be granted if the sharing and upgrading of apparatus had no adverse effect on a person's enjoyment of the land and there is no loss, damage or expense incurred for the person receiving the upgrade.

Responding to the amendments, Julia Lopez noted their similarity to measures Labour had attempted to introduce at committee stage. She said that as she had explained at that time, any legislation concerning work affecting private land had to take care to strike the right balance between public benefit and individual rights. She added that even more care was required in the case of measures that would apply retrospectively, as was the case with clauses 59 and 60 in the bill which the amendments sought to alter.

She argued that upgrading equipment in a building would "almost always" involve some kind of direct impact, however small, and that as a result the government considered it appropriate that such work should require either agreement from the landlord or imposition by the courts through the processes provided for in the ECC. Further, she said that even if an automatic upgrade right was introduced, operators would still have to successfully engage with the landlords for logistical purposes. Thus, she questioned the proportionality of the measures and whether there was support for the measure from industry stakeholders:

> Members suggest that there is consensus in industry that these changes are needed, but that is not the case. I have received direct

[80] HC Hansard, 25 May 2022, cols 328–9.
[81] HC Hansard, 25 May 2022, cols 328–9.
[82] HC Hansard, 25 May 2022, col 329.

> representations from many fibre providers that strongly oppose these proposals. They say that the proposals would create an unfair advantage for operators with equipment inside buildings, with potentially anti-competitive effects.

Amendment 14 was pressed to a division where it was defeated by 280 votes to 163.[83]

Backbench amendments 12 and 13: Calculating land value

Sir Desmond Swayne also moved amendments 12 and 13 which would remove clauses 61 and 62 enabling operators to calculate rent based on 'land value' rather than 'market value' when renewing tenancies to host digital equipment on private land, as per the reforms to the ECC introduced in 2017 referred to above.

Speaking to his amendments, Sir Desmond criticised the impact of the 2017 reforms:

> Until 2017, compensation was based on market value, and in 2017 the new code changed it to land value, notwithstanding the explicit advice of the Law Commission not to do so. As was entirely predictable and as was predicted, the market dried up as a consequence and there were far fewer agreements. One of the purposes of this bill is of course to address that problem of the reduction in agreements. Therefore, the obvious remedy is to restore the position as it was and return to market value, but far from doing that—far from seizing this opportunity to remedy the situation—the government are compounding their error by wanting to make agreements previously made under the old regime renewable under land value, actually making the problem significantly worse as a consequence.[84]

Chris Elmore also noted the Law Commission's findings in his remarks on the amendments, saying that his party supported the measures:

> The Law Commission voiced clear concerns at the time, arguing that it would lead to a fall in rent for landowners, and therefore a slowdown in the number of agreements being reached. As we heard in oral evidence, some landowners have seen their rents dwindle by as much as 90% in some cases, and as a consequence livelihoods have been turned upside down. These are welcome amendments, as they would mean that small tenant farmers, sports clubs and community organisations get a fairer deal for the land they are renting out.[85]

---

[83] HC Hansard, 25 May 2022, cols 338–40.
[84] HC Hansard, 25 May 2022, col 331.
[85] HC Hansard, 25 May 2022, col 330.

Responding to the amendments, Julia Lopez said that the government recognised that there had been problems between landowners and telecoms operators since changes to the ECC in 2017, and a "level of discontent" about the result of the valuation regime change.[86] However, she said that the government still believed there was significant benefit to bringing telecoms in line with other utilities and had found "little evidence" to suggest the regime required radical overhaul. She added that it was her view that more collaborative discussions would resolve many of the issues that she had observed, which the bill was intended to achieve.

She added:

> [W]e need a legislative framework that keeps costs low, so that we can encourage investment and protect consumers from price increases. The code valuation framework to calculate the sums payable to landowners by operators, which was introduced in 2017, aimed to achieve that. We maintain that the overall framework 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. The purpose of clauses 61 and 62 is to make sure that the valuation framework applies consistently across the UK and to all agreements the code applies to.[87]

Amendments 12 and 13 were withdrawn without division.[88]

3.4 Third reading

Third reading of the bill was held on the same day as report stage. Opening the debate, Julia Lopez, minister of state at the Department for Digital, Culture, Media and Sport, said that the bill would deliver the digital connectivity the UK required and welcomed the cross-party support for the majority of its provisions:

> The bill is one tool that we need to deliver great connectivity for everyone, and I am grateful for the cross-party recognition of the importance of our task. The government also recognise that greater connectivity brings the greater threat of harm to individuals, organisations and networks through an increased risk of cyber-attack. If networks and devices are not secure or trusted, we undermine their potential benefit to people and businesses.
>
> […]

[86] HC Hansard, 25 May 2022, col 326.
[87] HC Hansard, 25 May 2022, col 326.
[88] HC Hansard, 25 May 2022, col 336.

> [T]his bill is vital to the success of our digital economy in the decades ahead. Once passed, its measures will make the UK a better connected place and more resilient against cyber-attacks.[89]

Speaking for Labour, Chris Elmore said his party was supportive of the security elements of the bill, which will make "significant progress" in protecting UK citizens from malign actors.[90]

However, he reiterated that Labour would like to see security requirements expressly set out in the bill rather than defined in regulations. He also repeated calls for the government to publish a report on the security risks to UK connected products. In the process, he noted evidence from Professor Madeline Carr, a cyber-security expert, who told the public bill committee she would not have a smart hub in her house due to the security risks and that there is nothing in the bill that would change her mind. He said due to that statement by an industry expert, and the prominent role that cyber-warfare is playing throughout the conflict zones of the world, Labour believed it was in the national interest to know how secure our connected products are, and called upon the government to go "much, much further".[91]

On part 2 of the bill, Chris Elmore said his party supported the bill's aim of both increasing the security of connected devices and speeding up the roll-out of our telecommunications infrastructure.[92] Noting the ongoing digital divide between rural and urban areas, however, he said that he did not believe the measures in the bill were adequate to close that gap and would not deliver the crucial need of improved broadband access. He said he hoped these points would be picked up as the bill moved to the House of Lords.[93]

For the SNP, Owen Thompson again said his party supported the principles of the bill, but that their concerns over the enforcement of security requirements for consumer connectable products remained.[94]

The bill was given a third reading without division.[95]

---

[89] HC Hansard, 25 May 2022, col 341.
[90] HC Hansard, 25 May 2022, col 342.
[91] HC Hansard, 25 May 2022, col 342.
[92] HC Hansard, 25 May 2022, col 342.
[93] HC Hansard, 25 May 2022, col 342.
[94] HC Hansard, 25 May 2022, col 342.
[95] HC Hansard, 25 May 2022, col 342.

About the Library

A full list of Lords Library briefings is available on the Library's website.

The Library publishes briefings for all major items of business debated in the House of Lords. The Library also publishes briefings on the House of Lords itself and other subjects that may be of interest to members.

Library briefings are produced for the benefit of Members of the House of Lords. They provide impartial, authoritative, politically balanced information in support of members' parliamentary duties. They are intended as a general briefing only and should not be relied on as a substitute for specific advice.

Every effort is made to ensure that the information contained in Lords Library briefings is correct at the time of publication. Readers should be aware however that briefings are not necessarily updated or otherwise amended to reflect subsequent changes.

Disclaimer

Authors are available to discuss the contents of the briefings with Members of the House of Lords and their staff but cannot advise members of the general public.

Any comments on Library briefings should be sent to the Head of Research Services, House of Lords Library, London SW1A 0PW or emailed to hlresearchservices@parliament.uk.