

Research Briefing

By Sarah Barber,
Georgina Hutton

24 January 2022

The Product Security and Telecommunications Infrastructure Bill 2021-22



Summary

- 1 Part 1: Safety requirements for connectable products
- 2 Part 2: Telecommunications infrastructure

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

The Commons Library does not intend the information in our research publications and briefings to address the specific circumstances of any particular individual. We have published it to support the work of MPs. You should not rely upon it as legal or professional advice, or as a substitute for it. We do not accept any liability whatsoever for any errors, omissions or misstatements contained herein. You should consult a suitably qualified professional if you require specific advice or information. Read our briefing [‘Legal help: where to go and how to pay’](#) for further information about sources of legal advice and help. This information is provided subject to the conditions of the Open Parliament Licence.

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	6
1 Part 1: Safety requirements for connectable products	10
1.1 Background: Concerns about security of connectable products	10
1.2 Measures to increase security	11
Secure by Design report and the Code of Practice 2018	11
Consultation on regulating product security (2019-2020)	13
Consultation on legislative proposals (2020-2021)	14
1.3 The Bill	15
Clauses 1-3: Security requirements	15
Clause 4-6: Relevant products	16
Clause 7: Relevant persons	18
Clauses 8-25: Duties of relevant persons	18
Clauses 26-52: Enforcement	19
2 Part 2: Telecommunications infrastructure	21
2.1 Background: Digital infrastructure roll-out	21
2.2 Electronic Communications Code (ECC)	22
What is the ECC?	22
2017 reforms	22
2.3 ECC reforms: 2021	24
Government consultation	24
Stakeholder comment on proposed ECC reforms	24
Government's response	25
Stakeholder comment on the Bill	26
2.4 The Bill	27
Clause 57 – Definition of ‘occupier’	27

Clauses 58–60 – Rights to upgrade and share	27
Clause 61–65 – Renewal of expired agreements	29
Clause 66 – Unresponsive operators	31
Clause 67 – Interim orders	33
Clause 68 – Alternative dispute resolution	33
Clause 69 – Complaints about operators’ conduct	33
Clause 70 – Time limits on code proceedings	34
Clause 71 – rights of network providers in relation to infrastructure of other utilities	34

Summary

The Product Security and Telecommunications Infrastructure Bill has its second reading on 26 January 2022.

The 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](#).

Security requirements for consumer connectable products

Part 1 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 distributors 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

Part 2 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.

1

Part 1: 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 distributors with regards to these requirements.

An [Impact Assessment](#) of the product security part 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 [National Cyber Security Strategy 2016 to 2021, November 2016 \(A new National Cyber Security Strategy was published in December 2021 - National Cyber Strategy 2022\)](#)

⁵ [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 consumer organisation 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

Some have 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.”¹⁷

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.¹⁸

1.3

The Bill

This section provides a brief overview of the contents of part 1 of the Bill. A more detailed description of the Clauses in the Bill is provided in the [Explanatory Notes](#) produced by the Government.

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 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;

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 [Is the UK government’s new IoT cybersecurity bill fit for purpose? | TechCrunch](#)

¹⁸ [UK introduces PSTI bill to protect IoT devices \(iotttechnews.com\)](#)

- 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.¹⁹

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

- 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 negative 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.

¹⁹ DCMS, [The Product Security and Telecommunications Infrastructure \(PSTI\) Bill – product security factsheet](#), 24 November 2021

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..²⁰

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..²¹

Some products would be excluded, such as smart meters, medical devices, vehicles and smart chargepoints..²²

Clause 6 would establish regulation-making powers for the Secretary of State to set out which products are not considered relevant products for

²⁰ [Product security and Telecommunications Infrastructure Bill: Explanatory notes](#)

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

²² [Product security and Telecommunications Infrastructure Bill: Explanatory notes](#)

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 distributors 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 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, distributors 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 distributor 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 1 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 could delegate these enforcement powers.

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.

- 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 2: Telecommunications infrastructure

Part 2 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 2 of the Bill would come into force on a date set out by the Secretary of State in Regulations.²³

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;²⁴
- 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 2027.²⁵

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.²⁶

As of September 2021: 46% of UK premises had access to gigabit-capable broadband according to telecoms regulator, Ofcom. The Library's [broadband](#)

²³ Clause 77 of the Bill.

²⁴ HM Treasury, [National Infrastructure Strategy](#), 25 November 2020

²⁵ DCMS, [Future Telecoms Infrastructure Review](#), 23 July 2018; DCMS, [Shared Rural Network](#), 9 March 2020.

²⁶ [Gigabit-broadband in the UK: Government policy and targets \(CBP 8392, 21 December 2021\)](#) and [5G \(CBP 7783, 6 November 2019\)](#)

[data dashboard](#) allows users to explore where these premises are by Parliamentary constituency.²⁷

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.²⁸

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.²⁹

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.

2017 reforms

The ECC was significantly reformed in 2017.³⁰ 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.

²⁷ Commons Library data dashboard, [Constituency data: broadband coverage and speeds](#).

²⁸ 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.

²⁹ 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.

³⁰ The reforms were implemented by the [Digital Economy Act 2017](#).

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.³¹ 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.³² 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.³³

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.³⁴ Lawyers have said the drafting has created “frustration and confusion” among stakeholders.³⁵

The issue is highly polarised between the mobile industry and property owner stakeholder groups, with accusations of aggressive or vexatious behaviour on both sides.³⁶ 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.

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

³¹ [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.

³² Centre for Cities, [Delivering change How cities can make the most of digital connections](#), Simon Jeffrey and Lahari Ramuni, July 2018.

³³ [Upwardly Mobile: How the UK can gain the full benefits of the 5G revolution](#), 1 October 2021.

³⁴ Ashurst, [The Electronic Communications Code – Are changes afoot?](#), 4 February 2021.

³⁵ 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.

³⁶ [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

2.3

ECC reforms: 2021

Government consultation

In January 2021, the Government opened a [consultation on potential reforms to the ECC](#).³⁷

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.³⁸

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”..³⁹

Stakeholder comment on proposed ECC reforms

Reforms to the ECC have always been highly contested..⁴⁰ 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 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

³⁷ DCMS, [Consultation on changes to the Electronic Communications Code](#) 27 January 2021; press release: [Government reviews law on access to land for digital infrastructure](#).

³⁸ DCMS, [Consultation on changes to the Electronic Communications Code](#), 27 January 2021, paragraph 1.18.

³⁹ DCMS, [Consultation on changes to the Electronic Communications Code](#), 27 January 2021, paragraph 2.14.

⁴⁰ 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.

sites and to allow an efficient renewal process for expired pre-code agreements.

- [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 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.⁴¹

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).⁴² 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.⁴³

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”.⁴⁴ 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.

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:

⁴¹ BPF, [Property owner perspectives on the Electronic Communications Code \(ECC\)](#), June 2021, accessed 15 December 2021.

⁴² APPG for Broadband and Digital Connectivity, [#BetterBroadband inquiry](#) [accessed 19 January 2021]

⁴³ Letter from Selaine Saxby MP (Chair of APPG for Broadband and Digital Connectivity) to Secretary of State for DCMS on [#BetterBroadband inquiry findings](#).

⁴⁴ The Law Society, [Changes to the Electronic Communications Code – Law Society response](#), 20 April 2021.

...that the statutory valuation framework which underpins negotiations ... remains appropriate for the installation and maintenance of digital communications infrastructure systems.⁴⁵

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.⁴⁶

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.⁴⁷ Property owner campaign group, Protect and Connect, were disappointed the Government had not changed its position on valuation, arguing that sticking to this approach would continue to delay infrastructure roll-out.⁴⁸

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

⁴⁵ DCMS, [Consultation on changes to the Electronic Communications Code - government response](#), 24 November 2021, paragraph 1.14.

⁴⁶ DCMS, [Consultation on changes to the Electronic Communications Code - government response](#), 24 November 2021, paragraph 2.5.

⁴⁷ [Speed Up Britain - Electronic Communications Code Progress](#), Mobile UK, 13 January 2021.

⁴⁸ [Campaigners outraged as government rejects mobile phone mast overhaul](#), CityAM, 25 November 2021.

...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.⁴⁹

2.4

The Bill

Clause 57 – Definition of ‘occupier’

Clause 57 would clarify the definition of an ‘occupier’ of land in the Code.

Code rights are normally conferred by the occupier of the land. This is usually the landowner.

Currently, legal difficulties are created when the telecoms operator is the occupier (because equipment has already been installed) and a new renewed code agreement is required (for example, because the previous agreement has expired).⁵⁰ The operator cannot grant code rights to itself.

This clause would add a new sub-paragraph to the effect that where land is exclusively occupied by an operator, code rights can be granted by whoever “exercises powers of management or control” over the land. This would usually be the landowner.

Clauses 58–60 – Rights to upgrade and share

Clauses 58 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 there is difficulty tracing access agreements over such a long time.⁵¹

⁴⁹ [Code reforms can bolster UK digital connectivity](#), Michael Smith, Pinsent Masons, 5 January 2022.

⁵⁰ DCMS, [Consultation on changes to the Electronic Communications Code - government response](#), 24 November 2021, para 3.50-3.51. This issue was considered by the Court of Appeal in *Cornerstone Telecommunications Infrastructure Ltd v Compton Beauchamp Estates Ltd* [2019] EWCA Civ 1755.

⁵¹ DCMS, [Consultation on changes to the Electronic Communications Code - government response](#), 24 November 2021, para 4.25.

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.

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.⁵²

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.⁵³ Rights to upgrade can already be imposed as a separate code right (paragraph 3) but sharing is not listed as a separate right.

Clause 58 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 59–60 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 60 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

⁵² DCMS, [Consultation on changes to the Electronic Communications Code - government response](#), 24 November 2021, para 4.23.

⁵³ DCMS, [Consultation on changes to the Electronic Communications Code - government response](#), 24 November 2021, para 4.15.

potential for telecoms equipment to interfere with services' own equipment.⁵⁴ Some professional bodies raised concerns about implications for contract law and believed the commercial relationship was better served by negotiations between operators and site providers.⁵⁵

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).⁵⁶

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 before the Code came into force (28 December 2017) and continued after (called a “**subsisting agreement**”), is more complicated.⁵⁷

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.⁵⁸ 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.⁵⁹ There is no

⁵⁴ DCMS, [Consultation on changes to the Electronic Communications Code - government response](#), 24 November 2021, para 4.29.

⁵⁵ DCMS, [Consultation on changes to the Electronic Communications Code - government response](#), 24 November 2021, para 4.27.

⁵⁶ DCMS, [Consultation on changes to the Electronic Communications Code - government response](#), 24 November 2021, para 5.1

⁵⁷ 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).

⁵⁸ [Explanatory Notes](#) (PDF), para 250.

⁵⁹ 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

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.⁶⁰ The Government's consultation response said there continues to be uncertainty about how operators can renew these agreements and/or obtain new code rights.⁶¹

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.⁶²

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.⁶³ 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.⁶⁴ 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

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).

⁶⁰ 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:

⁶¹ DCMS, [Consultation on changes to the Electronic Communications Code - government response](#), 24 November 2021, para 5.3.

⁶² DCMS, [Consultation on changes to the Electronic Communications Code - government response](#), 24 November 2021, para 5.6.

⁶³ DCMS, [Consultation on changes to the Electronic Communications Code - government response](#), 24 November 2021, para 5.10.

⁶⁴ DCMS, [Consultation on changes to the Electronic Communications Code - government response](#), 24 November 2021, para 5.7–5.7.

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 – Unresponsive operators

Clause 66 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 ‘descope’.

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.⁶⁵

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.⁶⁶

Clause 66 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 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.⁶⁷

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.

⁶⁵ DCMS, [Consultation on changes to the Electronic Communications Code - government response](#), 24 November 2021, para 3.33-3.34

⁶⁶ DCMS, [Consultation on changes to the Electronic Communications Code - government response](#), 24 November 2021, para 3.35.

⁶⁷ DCMS, [Consultation on changes to the Electronic Communications Code - government response](#), 24 November 2021, para 3.43.

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 – 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 while the full case is determined.⁶⁸ There is no provision for seeking an interim order regarding non-financial aspects of the agreement.

Clause 67 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 67(4) sets out the factors the court must consider when making an interim order, including the operators' business and technical needs.

Clause 68 – Alternative dispute resolution

Clause 68 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 site 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 69 – Complaints about operators' conduct

Clause 69 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.

⁶⁸ DCMS, [Consultation on changes to the Electronic Communications Code - government response](#), 24 November 2021, para 35.

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.⁶⁹ Following feedback, including that the Code of Practice was not suitable for statutory enforcement in its current form, the Government decided not to pursue a mandatory complaints and compliance process.⁷⁰

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.⁷¹

Clause 70 – Time limits on code proceedings

Clause 70 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.⁷² There is no such requirement for disputes regarding the termination or renewal of agreements.

Clause 71 – rights of network providers in relation to infrastructure of other utilities

Clause 71 does not amend the Electronic Communications Code.

Clause 71 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

⁶⁹ DCMS, [Consultation on changes to the Electronic Communications Code - government response](#), 24 November 2021, para 3.16-3.17.

⁷⁰ DCMS, [Consultation on changes to the Electronic Communications Code - government response](#), 24 November 2021, para 3.28-3.29.

⁷¹ DCMS, [Consultation on changes to the Electronic Communications Code - government response](#), 24 November 2021, para 3.29.

⁷² 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 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.⁷³

The regulations include a requirement for operators of utilities (including gas, electricity and water as well as telecoms) to share physical infrastructure with competing network operators. Sharing the physical infrastructure of other utilities can lower the cost of telecoms network build by, for example, allowing cables to be installed in water pipes.⁷⁴

The Government has noted that the ATI regulations have so far had limited success on increasing infrastructure sharing.⁷⁵ In June 2020 the Government launched a [Call for Evidence](#) as part of a review of the ATI Regulations to assess whether further improvements could be made to encourage infrastructure sharing and boost infrastructure investment.⁷⁶

The Government’s [response to the call for evidence](#) on the ATI regulations was published in November 2021. The Government found that the regulations were “broadly appropriate” and that it was not “necessary or proportionate” to make major changes at present.

However, the Government did still consider that the regulations were not being used to the full potential and that clarifications to the scope of the regulations would be helpful. The Government also identified some smaller changes that could be made aimed at speeding up processes and

⁷³ Directive 2014/61/EU on measures to reduce the cost of deploying high-speed electronic communications networks (the Broadband Cost Reduction Directive).

⁷⁴ 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.

⁷⁵ DCMS, [Future Telecoms Infrastructure Review](#), 23 July 2018, para 69.

⁷⁶ DCMS, [Review of the Access to Infrastructure Regulations - call for evidence](#), June 2020.

strengthening Ofcom's enforcement powers. It said a further consultation will follow on potential changes to the regulations.⁷⁷ Clause 71 of the Bill would give the Government power to bring changes to the ATI Regulations through secondary legislation.

⁷⁷ DCMS, [Review of the Access to Infrastructure Regulations call for evidence - government response](#), 24 November 2021.

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](https://twitter.com/commonslibrary)