HOUSE OF LORDS Library Briefing

Telecommunications (Security) Bill

HL Bill 15 of 2021–22

Author: Edward Scott

Date published: 11 June 2021

On 29 June 2021, the second reading of the Telecommunications (Security) Bill is scheduled to take place in the House of Lords.

The purpose of the bill is to improve the regulation of the UK telecoms market in order to protect the security of the UK's telecoms infrastructure. This follows concerns, raised initially by the Intelligence and Security Committee of Parliament, about the degree to which the Chinese supplier Huawei had become involved in the UK's telecoms supply chain. In 2019, the then government published the findings of the telecoms supply chain review. This recommended that the Government strengthen the regulation of the telecoms market. It also recommended the Government introduce measures to improve the enforcement of the UK's telecoms cyber security.

Following the publication of the review, the Government has committed to establish in the UK what it called one of the most robust security frameworks in the world. The Government said this was necessary to meet the security challenges arising from the expansion of 5G and full fibre broadband. Separately, in 2020 the Government published a strategy to encourage greater diversity in the telecoms supply chain to prevent the UK network from being dependent on a limited number of suppliers.

The bill makes a series of amendments to the Communications Act 2003. The bill would establish new security duties on public telecoms providers. It would also expand the role of Ofcom to monitor the compliance by telecoms providers with these new duties. The bill would also enable the secretary of state to introduce measures to prevent telecoms providers from doing business with vendors that the Government has identified as posing a risk to national security.

The bill was introduced in the House of Commons in November 2020. Following the passing of a motion after second reading, it was carried over into the new session and completed its House of Commons stages on 25 May 2021.

The aims of the bill have received cross-party support. However, concerns were raised, including whether powers granted to the secretary of state in the bill will be subject to adequate parliamentary scrutiny. The Opposition asked the Government about the extent to which Ofcom would be resourced to meet its expanded role. It also raised concerns about the delivery of the Government's commitment to improve diversification of the supply chain. Amendments to the bill reflecting these concerns were tabled by the Opposition at committee stage and report stage. These amendments were voted on and defeated.

The Scottish National Party also tabled amendments requiring the secretary of state to consult with the devolved governments on matters concerning the security of the UK's telecoms infrastructure. These amendments were also unsuccessful.

1. Introduction

The Telecommunications (Security) Bill is a government bill intended to establish a new security framework for the UK telecoms sector. The bill would:[1]

- Create new duties on public telecoms providers to ensure that their networks are protected from security threats. This would include monitoring their supply chains for potential threats.
- Strengthen the powers of Ofcom, enabling it to enforce this new security framework.
- Give powers to the secretary of state to make regulations and issue codes of practice about the new security duties.
- Enable the secretary of state to establish controls over the use by telecoms providers of goods, services, and facilities from vendors identified as 'high risk'.

The bill applies to the whole of the United Kingdom.[2] Telecommunications is a reserved matter and the responsibility of the UK government.

2. Background

Roll-out of 5G and full fibre networks

In 2018, the then Government stated it intended to increase deployment of the UK's 5G and full fibre broadband networks.[3] This included a commitment that the majority of the UK would have 5G mobile coverage by 2027.[4] The Government has also committed to delivering full fibre and gigabit-capable broadband for every home and business across the UK by 2025.[5]

Threats to UK telecoms infrastructure

In 2013, the Intelligence and Security Committee published a report entitled *Foreign Involvement in the Critical National Infrastructure*.[6] This investigated the involvement of the Chinese company Huawei in British Telecom (BT). It concluded that Huawei's involvement posed a risk to national security.[7] It also noted that private providers were currently responsible for ensuring the security of key parts of the UK's telecoms network.[8]

In 2017, the then government stated in its *National Security and Infrastructure Investment Review* that

---

[1] Explanatory Notes, p 5.

[2] ibid, p 39.

[3] Department for Digital, Culture, Media and Sport, *Future Telecoms Infrastructure Review*, July 2018.

[4] Further information on 5G mobile technology is provided in the Parliamentary Office of Science and Technology (POST) briefing, *5G Technology*, 24 July 2019.

[5] Conservative Party, *Conservative Party Manifesto*, December 2019, p 28.

[6] Intelligence and Security Committee, *Foreign Involvement in the Critical National Infrastructure*, June 2013, Cm 8629.

[7] Further information on the debate concerning the involvement of Huawei in the UK's telecommunications network is provided in the House of Commons Library briefing, *Security Implications of Including Huawei in 5G*, 3 March 2020.

[8] ibid, p 4.

foreign control of UK businesses should be viewed as a potential risk to national security where those businesses were responsible for key parts of the UK's critical national infrastructure.[9]

Telecoms supply chain review

In 2019, the then government published the findings of its telecoms supply chain review, led by the Department for Digital, Culture, Media and Sport.[10] The review made a series of recommendations, including that the government strengthen the regulation and enforcement of telecoms cyber security. It also warned that a lack of diversity in the telecoms supply chain had resulted in the UK being dependent on a small number of suppliers.

Restricting Huawei's involvement in the UK's telecoms supply chain

In January 2020, the Department for Digital, Culture, Media and Sport announced the Government would be introducing measures to identify "high risk vendors" whose involvement in the UK's telecoms supply chain posed a security risk.[11] It said the Government would take action to limit the ability of such vendors to operate in the UK market.

In July 2020, the Government announced that, following a technical review by the National Cyber Security Centre, it would restrict Huawei's involvement in the UK's telecoms supply chain.[12] Specifically, UK operators would be banned from buying new Huawei equipment for 5G after 31 December 2020. It also said that all Huawei equipment would be removed from the UK's 5G network by the end of 2027.

Diversification strategy

In September 2020, the Government said that it would publish a telecoms diversification strategy.[13] It said this strategy would address what it described as a "market failure" that meant mobile companies were limited to using three major suppliers in their telecoms networks. It also announced the establishment of a "telecoms diversification task force".

In November 2020, the Department for Digital, Culture, Media and Sport published its 5G supply chain diversification strategy.[14] This stated that, in the short-term, the Government would support existing suppliers and attract new suppliers to the UK market. It also said that, in the longer term, the Government would work to prevent UK providers being dependent on a small number of suppliers.

---

[9] Department for Business, Energy and Industrial Strategy, *National Security and Infrastructure Investment Review*, 17 October 2017, p 21.

[10] Department for Digital, Culture, Media and Sport, *UK Telecoms Supply Chain Review Report*, July 2019, CP 158.

[11] Department for Digital, Culture, Media and Sport, 'New plans to safeguard country's telecoms network and pave way for fast, reliable and secure connectivity', 28 January 2020.

[12] Department for Digital, Culture, Media and Sport, 'Huawei to be removed from UK 5G networks by 2027', 14 July 2020.

[13] Department for Digital, Culture, Media and Sport, 'Ex-BT boss leads task force to attract new vendors to UK telecoms', 23 September 2020

[14] Department for Digital, Culture, Media and Sport, *5G Supply Chain Diversification Strategy*, 30 November 2020.

National Security and Investment Act 2021

The Government introduced separate legislation during the 2019–21 session intended to prevent hostile governments or other entities using inward investment as a means of undermining the UK's national security. Further information is provided in the House of Lords Library briefing, *National Security and Investment Bill: Briefing for Lords Stages*.[15]

3. Bill provisions

The Telecommunications (Security) Bill was published and received first reading in the House of Commons on 24 November 2020.[16] The Government said the purpose of the bill was to meet the security challenges presented by the widespread deployment of 5G and full fibre networks.[17]

The current regulatory framework for protecting the security of the UK's telecoms infrastructure is contained in the Communications Act 2003 (the 2003 act). This gives Ofcom certain limited powers to regulate the market. The changes in the Telecommunications (Security) Bill are primarily made through amending the 2003 act.

The bill includes the following provisions.

Security duties for telecoms providers (clauses 1–4)[18]

The bill would create a new duty on telecoms providers to take appropriate measures to identify and reduce the risk of security compromises occurring.[19] The bill would also require that providers take action in response to security compromises when they occur.[20] In both cases, the secretary of state would also have the power to introduce regulations imposing specific security duties on providers.

The secretary of state would be given the power to issue codes of practice to providers.[21] These are intended to provide guidance to providers on the measures they would need to take to fulfil the new security duties created by the bill.[22]

In addition to these duties, providers would be required to report any security incidents to Ofcom.[23] They would also have to inform users of networks and other services about the risks arising following the security incident.

---

[15] House of Lords Library, *National Security and Investment Bill: Briefing for Lords Stages*, 28 January 2021.

[16] HC *Hansard*, 24 November 2020, col 715.

[17] Explanatory Notes, p 4.

[18] These clauses would add new sections to the Communications Act 2003. Where these new sections are referred to by number, the associated clauses are listed in the footnotes.

[19] Telecommunications (Security) Bill, clause 1.

[20] ibid, clause 2.

[21] ibid, clause 3.

[22] Explanatory Notes, p 12.

[23] ibid, clause 4.

Securing compliance with new security duties (clauses 5–14)

The bill would expand the role of Ofcom currently set out in the Communications Act 2003. It would place a new duty on Ofcom to ensure that providers comply with the requirements set out in clauses 1–4 of the bill.[24]

The bill would also grant new powers to Ofcom to assess the degree to which providers had complied with their new duties.[25] Ofcom would be able to issue assessment notices to providers. These would set out what would be required of a provider for Ofcom to carry out its assessment, such as running tests of their network, allowing access to premises and providing access to asset registers. Ofcom would also be given powers to enforce the security duties, including levying fines against providers.[26] Ofcom would be required under the bill to publish a policy statement indicating how it intends to ensure providers comply with their security duties in the bill.[27] Providers would be able to appeal security decisions made by Ofcom in the Competition Appeals Tribunal.[28]

The bill would make provision for civil liability where there has been a contravention of the provider's security duties.[29] When a provider has been found to have contravened its duty to protect the security of its network, and that breach has caused loss or damage, the bill states that the provider would be liable.

The bill also includes the following reporting mechanisms:

- Ofcom must report on matters of security to the secretary of state, including by compiling an annual security report.[30]
- The bill also gives Ofcom the power to require and share information on the security of public communication networks and services.[31]
- The secretary of state must review the impact of the provisions in the first part of this bill (clauses 1–13) every five years.[32]

Designated vendor: directions, monitoring and enforcement (clauses 15–21)

The second part of the bill would provide the secretary of state with powers to prevent telecoms providers doing business with "designated vendors". These are vendors that the secretary of state has identified as posing a risk to the UK's national security.[33] The bill would enable the secretary of state to impose restrictions on providers concerning the use of goods, services and facilities provided by designated vendors. The restrictions would be set out in designated vendor directions issued by the

[24] Telecommunications (Security) Bill, clause 5.
[25] ibid, clause 6.
[26] ibid, clause 7.
[27] ibid, clause 10.
[28] ibid, clause 13.
[29] ibid, clause 8.
[30] ibid, clause 11.
[31] ibid, clause 12.
[32] ibid, clause 14.
[33] ibid, clauses 15 and 16.

secretary of state. The bill would also provide the secretary of state with powers to monitor and enforce these restrictions.[34] These would include through the issuing of inspection notices.

The secretary of state would be required to lay information before Parliament when designated vendors have been identified and designated vendor directions have been introduced.[35] However, exceptions to this requirement exist in the bill if the secretary of state believed information should be protected on grounds of national security.

Powers to amend maximum penalties (clause 24)

The bill would amend the Communications Act 2003 to increase the maximum amount of penalties for withholding security information from Ofcom. The maximum penalty for this would be raised from £2 million to £10 million.[36] For a continuing contravention, the maximum penalty would be raised from £500 per day to £50,000 per day. The secretary of state would be given the power to amend these maximum penalties through regulations.

4. Bill stages in the House of Commons

The bill has received cross-party support in the House of Commons. However, concerns have been raised about issues including:

- Whether the powers in the bill were adequate to protect against the specific threat posed by suppliers like Huawei gaining access to the UK's telecoms network.
- Whether Ofcom would be adequately resourced to enable it to fulfil the new duties created by the bill.
- That the secretary of state would be given powers in the bill without adequate parliamentary oversight of how they would be used.
- The Government's willingness to deliver on its ambitions to achieve greater diversity in the telecoms supply chain.

Amendments were tabled by the Opposition and the Scottish National Party (SNP) during committee stage and report stage. However, none of these amendments were passed. The only changes made to the bill in the House of Commons were 'technical' amendments tabled by the Government and passed during committee stage.

4.1 Second reading

During the second reading debate in the House of Commons on 30 November 2020, the Secretary of State for Digital, Culture, Media and Sport, Oliver Dowden, said the bill acted upon the recommendations of the UK telecoms supply chain review and had been informed by technical advice from the National Cyber Security Centre (NCSC) and GCHQ.[37] He noted that, according to the

[34] Telecommunications (Security) Bill, clauses 18 and 23.

[35] ibid, clause 17.

[36] The current maximum penalties are set out in s139 of the Communications Act 2003 (as amended).

[37] HC *Hansard*, 30 November 2020, cols 70–126.

NCSC, the UK had suffered malicious cyber attacks from Russia, China and other state actors in recent years. He said that currently the Government did not have adequate powers to counter these threats. He argued the bill would ensure that the UK had one of the most robust security frameworks in the world.

Jo Stevens, the Shadow Secretary of State for Digital, Culture, Media and Sport, said that Labour supported the aims of the bill.[38] However, she argued the Government had been slow to introduce these measures. She noted the UK's Five Eyes allies, Australia and New Zealand, had both taken action to limit the activities of high-risk vendors in their telecoms markets in 2018. She also raised concerns including whether the bill provided adequate oversight of the use of new powers by the secretary of state and whether the Government was taking appropriate steps to ensure there was greater diversity in the UK's telecoms supply chain.

Richard Thomson, the then SNP Shadow Spokesperson for Business and Industry, also stated his party's support for the aims of the bill.[39] However, he argued that the bill should be amended to ensure there was consultation between the secretary of state and the relevant ministers in the devolved government on the issue of the UK's telecoms infrastructure.

Carry-over motion

Following second reading, the House of Commons agreed a motion to carry the bill over into the new session.[40]

4.2 Committee stage

The House of Commons public bill committee considered the bill over the course of eight sittings between 14 and 26 January 2021. During the first four sittings, the committee took evidence from witnesses including representatives of telecoms providers and Ofcom. It also heard from organisations working in the security and the telecoms sectors such as the Royal United Services Institute and Oxford Information Labs.

The committee examined the bill during the last four sittings. Labour and the SNP tabled 15 amendments and new clauses.[41] Of these, four were voted on and defeated following a division. All of these were Labour amendments and were defeated by 3 votes to 10. The amendments were:

- That Ofcom reports on the security of the UK telecoms network should include an assessment of the diversification of the supply chain (amendment 14).
- That Ofcom be required to publish a report indicating whether it believes it has adequate resources to meet its new obligations under the bill (new clause 3).
- To add further reporting mechanisms to the bill, requiring the secretary of state to provide a report to the Intelligence and Security Committee and requiring Ofcom to

[38] HC *Hansard*, 30 November 2020, cols 76–82.
[39] ibid, cols 84–88.
[40] ibid, col 126.
[41] House of Commons, *Public Bill Committee Proceedings: Telecommunications (Security) Bill*, 26 January 2021.

report on its assessment of future risks to the UK's network security (new clause 5).
- To require the secretary of state to publish a report on the impact of the Government's network diversification strategy (new clause 6).

The Government tabled four 'technical' amendments to the bill concerning the commencement date. These amendments were passed and made to the bill.[42]

Further information on committee stage proceedings in the House of Commons is provided in the House of Commons Library briefing, *Telecommunications (Security) Bill 2019–21*.[43]

4.3 Report stage

Report stage of the bill took place on 25 May 2021.[44] Further amendments from the Opposition and the SNP were debated. These amendments concerned:

- The role of Ofcom and whether it would be adequately resourced to take on its expanded role under the bill.
- Scrutiny by the Intelligence and Security Committee on the use of powers in the bill by the secretary of state.
- The implementation of the Government's supply chain diversification strategy.
- Ensuing there would be consultation between the secretary of state and devolved governments.

No amendments were made to the bill at this stage. Three Labour amendments were voted on and defeated.

In addition to these amendments, Conservative MPs tabled further amendments but these were not selected for debate. However, they were referred to during the report stage debate.

Ofcom annual report (new clause 1)

The Opposition tabled new clause 1 which would have required Ofcom to include statements in its annual report on the following:

- Whether Ofcom had received the resources it needed to fulfil its expanded role set out in the bill. This would include whether it had: adequate budget and funding; adequate staffing; and whether it faced any skill shortages.
- Whether the security measures taken by network providers in the last 12 months had been adequate to ensure the UK telecoms network was protected. This would include

[42] A version of the bill indicating the amendments made during committee stage has been published on the UK Parliament website: House of Commons, *Telecommunications (Security) Bill: Public Bill Committee Amendments as at 26 January 2021*, 26 January 2021.

[43] House of Commons Library, *Telecommunications (Security) Bill 2019–21*, 6 April 2021.

[44] HC *Hansard*, 25 May 2021, cols 278–324.

specific measures set out in regulations by the secretary of state.
- What future threats Ofcom believed may be emerging based on its interrogation of network providers' asset registers.

Speaking in support of her amendment, Chi Onwurah, the shadow minister for Science, Research and Digital, said the proposed expansion of Ofcom's role in the bill would put strain on its resources.[45] She also argued that Ofcom lacked experience in the area of national security. Citing evidence provided during committee stage by Oxford Information Labs, she argued that Ofcom would need to expand its capacity in this area to fulfil its new role.[46]

She noted that a memorandum had recently been published by Ofcom and the National Cyber Security Centre about how they would work together as part of the new regulatory regime.[47] However, she said this did not provide adequate reassurance. She said that, while the National Cyber Security Centre would be able to provide advice on national security matters, Ofcom needed to have greater expertise to understand this advice.

Ms Onwurah also argued the amendment was necessary to ensure that Ofcom assessed future risks to the security of UK telecoms. She identified the new types of threats that had emerged over recent years, such as attacks to healthcare systems. She also referred to potential future risks, such as the dependence of cloud computing infrastructure on Amazon Web Services (AWS), the dominant vendor in this market. She described the dangers that might arise if AWS were bought by a hostile foreign state or hacked by a hostile operator.

Responding to new clause 1, Matt Warman, the Parliamentary Under Secretary of State for Digital, Culture, Media and Sport, argued additional reporting requirements were unnecessary.[48] He told the House that Ofcom already produced annual reports on the UK's communications infrastructure.[49] He also said the bill as currently drafted already included requirements for Ofcom to report to the secretary of state on the compliance of providers with their new security duties. The secretary of state would also report every five years on the impact of measures in the first part of the bill, he argued.

On the issue of the resources available to Ofcom, Mr Warman said the regulator's security budget would be increased by £4.6 million during the current financial year. He said this would enable Ofcom to increase the amount of staff working in telecoms security. On the specific issue of skills, he said that Ofcom already had a role in protecting the security of UK telecoms as part of its existing duties under the Communications Act 2003.

Mr Warman argued the bill already included measures intended to support the identification of future security risks. He argued clause 12(3)(b) would enable Ofcom to require information from providers about future developments in their networks. He also said Ofcom would be required to provide any information to the secretary of state that was relevant to forming the UK's security policy.

---

[45] HC *Hansard*, 25 May 2021, col 281.

[46] Public Bill Committee, *Telecommunications (Security) Bill*, 14 January 2021, session 2019–21, 1st sitting, col 72.

[47] Ofcom, 'Joint statement from Ofcom and the National Cyber Security Centre', accessed 7 June 2021.

[48] HC *Hansard*, 25 May 2021, col 304.

[49] The reports referred to by the minister are available on the connected nations and infrastructure reports: Ofcom, 'Connected Nations and infrastructure reports', accessed 8 June 2021.

New clause 1 was moved to a division and defeated by 365 votes to 263.[50]

Intelligence and Security Committee scrutiny (new clause 2)

New clause 2, also tabled by the Opposition, concerned specific provisions in the bill whereby the secretary of state would be able to withhold information from publication on security grounds. The new clause would have required the secretary of state to share this information with the Intelligence and Security Committee (ISC). This would include:

- Copies of designated vendor directions, designated notices and notices of variation or revocation not laid before Parliament.[51]
- Copies of notifications issued to providers believed to have contravened a designated vendor direction.[52]
- Copies of confirmation decisions given to providers. These would either confirm that a provider had contravened a designated vendor direction or that no further action would be taken.[53]
- The reasons for making an urgent enforcement direction which had been withheld by the secretary of state in the interests of national security.[54]
- The reasons for confirming or modifying an urgent enforcement direction.[55]

Ms Onwurah said that the purpose of the new clause was to increase the transparency of decisions taken by the secretary of state. She reminded the House of similar amendments tabled in both the House of Commons and the House of Lords during the passage of the National Security and Investment Bill, which sought to ensure scrutiny of the government's powers by the ISC. She said ensuring there was a role for the ISC in the bill would ensure that use of powers in the bill were overseen by Parliament.

The chair of the ISC, Dr Julian Lewis, also spoke in support of new clause 2.[56] He restated the committee's support for the bill. However, he said there was "a significant gap in Parliament's oversight" of the powers in the bill.[57] He said that the ISC was best placed to fill this gap because it had been established with the specific purpose of scrutinising national security issues that could not be laid before Parliament. He argued the ISC's memorandum of understanding with the prime minister did not give it adequate authority to scrutinise the work of departments which were not traditionally concerned with security, including the Department for Digital, Culture, Media and Sport. He said his preferred solution would be for the ISC's memorandum of understanding to be amended accordingly. He said this would be recommended in the ISC's next annual report. However, he told the House that he would support proposals such as new clause 2 while the memorandum of understanding remained unamended.

---

[50] HC *Hansard*, 25 May 2021, cols 310–14.

[51] The secretary of state would be able to withhold these under section 105Z11(2) and (3) of the amended Communications Act 2003 (if the bill was passed) in clause 17 of the Telecommunications (Security) Bill.

[52] The powers to issue confirmation decisions are set out in section 105Z18(1) in clause 20.

[53] The powers to issue confirmation decisions are set out in section 105Z20(2)(a) in clause 20.

[54] The power to withhold this information is set out in section 105Z22(5) in clause 21.

[55] These may also be withheld by the secretary of state using powers set out in section 105Z23(6) in clause 21.

[56] HC *Hansard*, 25 May 2021, col 285.

[57] ibid, col 286.

Mr Warman said the Government valued the advice provided to it by the ISC.[58] He told the House that decisions made by the secretary of state about the use of powers in the bill would be informed by National Cyber Security Centre advice. He said that the National Cyber Security Centre was subject to the scrutiny of the ISC. In response to Dr Julian's comments about amending the ISC's memorandum of understanding, he said the Government would look closely at the recommendations in the ISC's next report.

New clause 2 was moved to a division and defeated by 363 votes to 263.[59]

Report on impact of supply chain diversification strategy (new clause 3)

The third amendment tabled by the Opposition, new clause 3, would have required the secretary of state to publish a report on the progress of efforts to encourage greater diversification of the telecoms supply chain. This report would include an assessment of factors including:

- The implementation of the government's telecoms diversification strategy.
- Changes in the market that might have an impact on diversification, such as the ownership of existing businesses in the supply chain or new areas of market consolidation.
- The amount of public funding available to support diversification.

Ms Onwurah argued the Government needed to ensure that greater diversification of the telecoms supply chain was achieved if the new security regime envisaged in the bill was to work in practice.[60] She welcomed the measures in the bill to impose restrictions on the involvement of high-risk vendors in the UK telecoms network. However, she said the UK would remain dependent on a small number of vendors unless greater diversification was achieved. For example, she argued that the removal of Huawei from the supply chain left the UK with effectively only two remaining service providers: Ericsson and Nokia.

Ms Onwurah criticised the Government, arguing it had not yet acted to achieve greater diversification. Specifically, she said the telecoms diversification taskforce had been slow to act, arguing that answers she had received to written parliamentary questions suggested none of the £250 million allocated to the taskforce had been spent or earmarked. Mr Warman had said in response to Ms Onwurah's question tabled on 24 May 2021 that the funding would not be allocated to the taskforce itself and that the taskforce had now completed its work.[61] However, he said that this funding would be spent to ensure the diversification strategy is delivered. He indicated the Government would outline the next steps for the delivery of the diversification strategy in the summer of 2021.

During his speech at report stage, Mr Warman said the Government remained committed to the diversification strategy it had published in November 2020.[62] He said the strategy included plans to

---

[58] HC *Hansard*, 25 May 2021, col 305.
[59] ibid, cols 314–19.
[60] ibid, col 283.
[61] House of Commons, 'Written Question: Telecoms Diversification Task Force: Finance', 24 May 2021, 2290.
[62] HC *Hansard*, 25 May 2021, col 306.

invest in research and development and would remove technical barriers preventing new suppliers from entering the market. He told the House that the Government had already acted to support this strategy:

> To give the House an idea of some of the non-legislative measures that we are already pursuing, they include the investment in R&D development facilities such as the National Telecoms Lab and the SONIC—SmartRAN Open Network Interoperability Centre—lab that is jointly at work with Ofcom. We are also working to remove barriers to entry for vendors such as by co-ordinating the sunsetting of legacy network technologies, working internationally to co-ordinate diversification objectives, and exploring the use of commercial incentives to address the cost of incorporating new suppliers into a network.[63]

Mr Warman said the Government did not support new clause 3. He said that, by defining diversification in legislation, the amendment risked creating limitations on what he described as a "rapidly evolving market".[64]

New clause 3 was moved to a division and defeated by 357 votes to 271.[65]

Consultation with devolved ministers (amendment 1)

Amendment 1, tabled by the SNP, would have required the secretary of state to consult with appropriate ministers in the devolved governments when conducting the five-yearly review of the impact and effectiveness of clauses 1 to 13 of the bill.[66]

Speaking in support of the amendment, Stephen Flynn, the Shadow SNP Spokesperson for Business, Energy and Industrial Strategy, said it was important for the UK Government to work with the governments in Scotland, Wales and Northern Ireland. Chi Onwurah also spoke in favour of the amendment, arguing it was important that measures to protect the telecoms network should extend to all parts of the UK.[67] Jim Shannon (Democratic Unionist Party MP for Strangford) argued that the Government should ensure that these discussions should happen as a matter of course.[68]

Responding to amendment 1, Mr Warman said that, while telecoms was a reserved matter, the Government recognised the importance of maintaining a constructive and close working relationship with the devolved governments.[69] However, he did not support the amendment. The amendment was not called at the end of the debate and therefore fell.

---

[63] HC *Hansard*, 25 May 2021, col 306.

[64] ibid, col 307.

[65] ibid, cols 320–4.

[66] To achieve this, the amendment would have inserted a new subclause to clause 14.

[67] HC *Hansard*, 25 May 2021, cols 284–5.

[68] ibid, col 297.

[69] ibid, col 307.

Amendments not selected for debate

A further two amendments were tabled by backbench Conservative MPs, amendments 2 and 3.[70] These were not selected for debate. These amendments would have created a new requirement for the secretary of state to make a designated vendor direction if that vendor:

> […] is required under certain circumstances to yield its data to the government or intelligence services of the country where it has its headquarters.[71]

One of the three MPs that tabled these amendments was Sir Iain Duncan Smith (Conservative MP for Chingford and Woodford Green). Sir Iain said he believed the bill should have been amended in this way.[72] He said that China's 2017 national intelligence laws required companies to share information with the Chinese government. He said this meant that such companies could not operate independently and were unable to ensure information held on behalf of their clients could be protected.

Addressing the amendment in his comments, Mr Warman said the existence of powers such as those described in amendment 2 would not necessarily mean that companies headquartered in that country were high-risk vendors.[73] He argued that it was important to consider not just that such powers might exist in a country where a vendor is headquartered. He said it was also important to consider how these powers might be used. For example, he said that companies based in friendly democracies where such powers existed were unlikely to pose a threat to the security of the UK's telecoms network.

On the specific threats posed by suppliers headquartered in China, Mr Warman noted the UK government had already recognised that the powers of the Chinese state to collect information from Chinese companies had represented a threat to the security of the UK's telecoms infrastructure. He said the powers in the bill were already sufficient to combat this specific threat.

4.4 Third reading

Third reading took place in the House of Commons directly after report stage on 25 May 2021.[74] Mr Warman said the bill would ensure that the UK's telecoms network was protected from security threats in the future.[75] He also thanked MPs for the constructive spirit in which the bill had been debated.

Ms Onwurah restated Labour's support for the aims of the bill.[76] However, she argued that there remained gaps in the new regime, including the lack of parliamentary oversight concerning some of the powers given to the secretary of state and the absence of an effective plan for ensuring the diversification of the telecoms supply chain.

---

[70] House of Commons, *Telecommunications (Security) Bill: Consideration of Amendments as at 25 May 2021*, 25 May 2021.
[71] ibid.
[72] HC *Hansard*, 25 May 2021, cols 290–1.
[73] ibid, col 307.
[74] ibid, cols 324–28.
[75] ibid, col 325.
[76] ibid, cols 325–8.

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 the Members 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.