Department for Digital, Culture, Media & Sport

Baroness Barran
Minister for Civil Society
4th Floor
100 Parliament Street
London SW1A 2BQ

www.gov.uk/dcms
enquiries@dcms.gov.uk

Lord Alton of Liverpool; Lord Balfe; Baroness Bennett of Manor Castle; Lord Clement-Jones; The Earl of Erroll; Lord Fox; Lord Holmes of Richmond; Lord Maxton; Baroness Merron; Baroness Morgan of Cotes; Baroness Northover; Lord Stirrup; Baroness Stroud; Lord Vaizey of Didcot; Lord Vaux of Harrowden; Lord West of Spithead; Lord Young of Cookham

MC2021/13509/DC
6 July 2021

My Lords,

Telecommunications (Security) Bill - Second Reading

I am grateful for your contributions to the considered debate at Second Reading of the Telecommunications (Security) Bill. I am writing to you to expand on some of the points that were raised. I want to thank all of those who took part, and appreciate your overall support of the Government's aim to protect our critical telecoms networks for years to come.

The role of Ofcom

In the debate, I stated that this bill provides Ofcom with a new general duty to seek to ensure public telecoms providers[1] comply with their new security duties. We have published a factsheet[2] that provides more details on Ofcom's role.

As I set out in the House, to reflect its increased role, Ofcom's budget for telecoms security this financial year has been increased by £4.6 million. This is in addition to its current security budget of £2 million. This funding will allow Ofcom to double the number of people working on telecoms security. Ofcom will be working with a recruitment partner to ensure they have access to the specific cyber skills needed to implement this regime, which will include seconding technical expertise to further develop Ofcom's capability.

[1] Providers of public electronic communications networks and services as defined in the Communications Act 2003.

[2] https://www.gov.uk/government/publications/telecommunications-security-bill-factsheets/factsheet-4-ofcom-and-telecoms-security

In addition, as the UK's world-leading national authority on cyber security, the National Cyber Security Centre will share its technical expertise with Ofcom to support the regulator's implementation of the new regime. The National Cyber Security Centre and Ofcom have a well established relationship, working closely and effectively on network security matters. They are in the process of agreeing a memorandum of understanding to formalise their roles under the framework. Ofcom has also published a joint statement[3] that summarises what will be contained in the memorandum, on its website.

In the debate, I listened carefully to points about the proportionality, accountability, and transparency of the new regime, and in particular how Ofcom would interpret these principles in relation to enforcement action.

Ofcom is an independent body that is accountable to Parliament. When carrying out its security functions, Ofcom will remain bound by its general duties under Section 3 of the Communications Act 2003 as it is now. Section 3(3) provides a duty on Ofcom to have regard to the need for transparency, accountability and proportionality when carrying out its functions. Ofcom will also be bound by its duty under Section 6 of the Communications Act 2003 to review the burden of its regulation on public telecoms providers. If Ofcom fails to carry out its security functions in line with these duties, then it is likely to be subject to legal challenge.

The Bill has transparency and reporting at its heart. It includes four separate clauses on reporting, two of which apply to Ofcom. Clause 10 requires Ofcom to publish a policy statement explaining how it will ensure public telecoms providers comply with their new security duties. Clause 11, amongst other things, requires Ofcom to report publicly on the extent to which providers are complying with their security duties. Collectively, these reports will ensure that Parliament is able to scrutinise Ofcom's role effectively.

Development of the telecoms security framework

As I mentioned in my closing speech, the new security framework introduced by Clauses 1 to 14 of the Bill will comprise three distinct but complementary parts, each consisting of measures of appropriate technical breadth and detail. The Bill sets out strengthened overarching security duties for public telecoms providers in primary legislation. It provides the powers that allow the Government to make regulations in secondary legislation. It will also enable the Secretary of State to issue codes of practice, as technical guidance, setting out the steps public telecoms providers could take to meet their legal obligations.

The duties in primary legislation are based around the concept of a 'security compromise', which is defined in new Section 105A in Clause 1 of the Bill. The noble Baroness, Baroness Bennett, asked about the scope of security compromises and whether they would extend to hazards posed by a changing climate. The intent of this Bill is to address the cyber security risks to public telecoms networks. Public telecoms providers will need to ensure appropriate and proportionate measures to protect against the security compromises, irrespective of their causes. Public telecoms providers already take steps to manage the effects of climate change on the availability of their networks, under their legal duties set out in the current Section 105A of the Communications Act. The Bill will replace this duty with the strengthened overarching duty contained in the new Section 105A in Clause 1. That means the work carried out

[3] https://www.ofcom.org.uk/__data/assets/pdf_file/0028/219628/ofcom-ncsc-joint-statement-telecoms-security-bill.pdf

by telecoms providers and government to ensure the availability of networks will continue going forward.

The Bill requires that the duties and requirements on public telecoms providers under the new security framework must be appropriate and proportionate. The Government published its early draft of the security regulations in January[4], to illustrate the types of measures that might be included. We have engaged with industry, including telecoms companies and representative bodies, and will continue to do so throughout the passage of the Bill. The feedback received from industry has been invaluable in helping our policy development and will ensure the final framework is appropriate and proportionate to the specific risks to UK network security.

Furthermore, in line with the Bill's requirements, the Government will consult with affected public telecoms providers and Ofcom on any codes of practice that are issued. This will ensure that we have a full understanding of the code's impact before it is finalised. A consultation on the first code of practice will take place after the Bill receives Royal Assent.

The Government and Ofcom will work collaboratively with the telecoms industry as they implement the new framework. To gauge the framework's effectiveness, Ofcom will provide regular reports to the Secretary of State on industry compliance as required under Clause 11 of the Bill. These reports, as well as continued technical advice from the National Cyber Security Centre, will support ongoing Government policy development in relation to telecoms security. This will help to ensure the new telecoms security framework delivers our intent and keeps pace with new threats and technologies.

High Risk Vendors

As the Secretary of State set out in his statement to the House of Commons on 14 July 2020, we can only realise the benefits of 5G technologies if we have confidence in the security and resilience of the infrastructure on which they are built. This means ensuring that we are able to protect our networks from the risks posed by high risk vendors.

The Bill includes new powers for the Secretary of State to designate specific vendors in the interests of national security, and issue directions to public communications providers. These directions will place controls on a provider's use of goods, services and facilities supplied, provided, or made available by a designated vendor. A direction could, among other things, include requirements to prohibit or restrict the use of goods, services or facilities supplied, provided, or made available by a designated vendor. It could include requirements to remove, disable or modify such goods, services or facilities. Requirements may be made by reference to the *source* of the goods, services or facilities supplied, provided or made available, as well as by reference to the *time* at which goods, services or facilities were procured, developed or produced. These provisions will provide the Secretary of State with the scope and flexibility to address risks associated with telecoms providers' use of high risk vendors' goods, services or facilities.

[4] https://www.gov.uk/government/publications/draft-electronic-communications-security-measures-regulations

The Government has always considered Huawei to pose a relatively high risk to the UK's telecoms networks, compared to other vendors. There has been a risk mitigation strategy in place since Huawei first began to supply equipment to the UK market.

The Government has announced extensive advice to manage the security risks posed by Huawei, based on the analysis of our world-leading experts at the National Cyber Security Centre. The Secretary of State has advised that public telecoms providers should remove all Huawei equipment from 5G networks by the end of 2027. In order to clearly set out the pathway to zero, the Secretary of State also announced that providers should stop procuring new 5G equipment from Huawei after 31 December 2020, and stop installing Huawei equipment in 5G networks after September 2021. Together, all of these measures will help protect our networks from the risks posed by Huawei. Once passed, and subject to the relevant consultation requirements, the Bill will enable the Government to give legal effect to this advice.

Ministers have already had fruitful discussions with telecoms providers, where they have set out the hard work they are doing to meet our advisory timeframes. I am sure they will continue to work hard as the Bill continues its passage through Parliament.

Parliamentary and Judicial oversight

Noble Lords asked questions about how parliamentary and judicial oversight are provided for within the Bill. As I mentioned in my closing remarks at Second Reading, the Bill already includes provision for Parliamentary oversight of the use of the national security powers.

The Bill requires the Secretary of State to lay copies of designation notices and designated vendor directions before Parliament, unless doing so would be contrary to the interests of national security. On the very rare occasion that a designation notice or direction is not laid before Parliament on national security grounds, there is no barrier to the Digital, Culture, Media and Sport Select Committee viewing such directions and notices.

The noble Lord, Lord West, asked about the role of the Intelligence and Security Committee in overseeing the use of the Bill's powers. That Committee's remit extends to the intelligence agencies and other activities of the Government in relation to intelligence or security matters, as they are set out in its memorandum of understanding. But the advice of the intelligence agencies will not be the only factor that the Secretary of State will take into account when deciding what is proportionate to include in a designated vendor direction. The Intelligence and Security Committee doesn't have the remit to consider non-security issues such as the economic and connectivity implications of the requirements in designated vendor directions. Any future changes to the Committee's remit would be best managed through consideration of the Justice and Security Act and the associated Memorandum of Understanding.

My noble friend, Lord Young of Cookham, asked about the grounds upon which the Secretary of State could decide to issue a designation notice or direction, and the grounds not to lay those documents before Parliament. The Secretary of State will only issue designation notices and designated vendor directions where they are necessary in the interests of national security, and where the requirements in the directions are proportionate. However, there may be some specific instances where it could be harmful to national security to lay a direction before parliament - for example, because doing so would expose particular security vulnerabilities.

My noble Friend also asked if the decision to issue a designation notice or direction was justiciable. As I set out in my closing speech, decisions to issue designation notices and designated vendor directions are subject to the ordinary principles of judicial review. This will enable affected telecoms providers and vendors to challenge decisions made by the Secretary of State.

The noble Lord, the Earl of Errol, raised concerns that the details of, and reasons for, a designation notice would be likely to leak. I wish to provide assurance that there are mechanisms in place to ensure information related to national security remains classified at an appropriate level. The Bill allows the Secretary of State to exclude, from the copies of a designation notice or designated vendor direction laid before Parliament or from the copies issued to the vendor and to providers, anything the disclosure of which the Secretary of State considers would be contrary to the interests of national security. This means that the Secretary of State will be able to withhold from publication any particularly sensitive material. Furthermore, the Secretary of State will be able to require recipients of notices or directions not to disclose the contents of those documents. There are substantial fines of up to £10 million if a vendor or provider fails to comply with a requirement not to disclose the contents of notices or directions.

Diversification

Noble Lords across the House have shown keen interest in the progress of our work to diversify the telecoms supply chain. As I set out at Second Reading, this work sits alongside the Bill, rather than as a part of it.

The Government's 5G Supply Chain Diversification Strategy[5] is primarily focused on addressing the risks presented by a lack of choice in the radio access network. However, it also noted that there may be a lack of diversity in other network domains, and work is ongoing to assess the wider telecoms supply chain. Where it is appropriate to share the conclusions of this assessment, I will update in due course.

With regard to the make-up of the supply chain of our networks today, as the noble Lord, Lord Fox raised, currently there are three major vendors supplying the UK radio access network: Huawei, Ericsson and Nokia. Following the removal of Huawei from our 5G networks by the end of 2027, the UK will be reliant on the two remaining incumbent vendors - Ericsson and Nokia. Through the Diversification Strategy we aim to deliver a more healthy supply market for telecoms by attracting new vendors into the UK market and promoting open-interface solutions and deployment. This will ensure the long-term resilience and security of our telecoms networks.

New vendors are coming into the market - Vodafone recently announced they would be using six new suppliers as part of their Open RAN deployment, including major players such as Samsung and NEC.

However there is further work to be done to ensure these new solutions are effective and so we must take a multi-faceted approach to developing solutions to long standing structural barriers. In particular we are making investments in an R&D ecosystem which will accelerate and pull forward the development of interoperable technologies shown by the recent launch of FRANC (Future RAN Competition)[6]. The competition will invest up to £30 million in innovative projects that begin to address the key

[5] https://www.gov.uk/government/publications/5g-supply-chain-diversification-strategy

[6] https://www.gov.uk/guidance/future-ran-diversifying-the-5g-supply-chain

technological challenges of high-performance Open RAN. This will mean accelerating the availability of RAN solutions that can be deployed across the UK's networks, including in the most demanding environments.

The long term success of our strategy is dependent on international collaboration and to this end, the Government has engaged with a range of international partners, including with the Five Eyes and through the G7 under the UK's Presidency. In the G7, we worked collaboratively with our partners to agree a statement on the importance of secure, resilient and diverse telecommunications, ICT and digital infrastructure supply chains in the G7 Digital and Technology Ministerial Declaration, as well as a commitment to continue discussions on this issue in the G7 over the longer-term. The UK will continue to actively engage with partners both bilaterally and through multilateral mechanisms to further build international consensus and progress opportunities for collaboration.

The Government is working closely with industry, the National Cyber Security Centre, Ofcom and a wide range of international partners to increase UK influence and presence at major standards development organisations, such as ETSI and 3GPP. We are working with Ofcom in addressing barriers to innovation and new vendor entry, through planning for legacy networks being made redundant; providing clarity on resilience requirements and a mechanism for collaboration with operators; and monitoring relevant standards and vendor progress.

On 2 July 2021, the Government set out its response to the recommendations of the Telecoms Diversification Taskforce. This can be found on GOV.UK[7].

International Collaboration

Noble Lords asked how we were working with international partners on the Bill and these issues. We have engaged with international partners including the US and the EU throughout the drafting of this Bill, and will continue to do so once it is passed. The UK's telecoms networks face similar challenges to networks in other countries, and it is vital that we seek international solutions for this international challenge.

In response to the Noble Lord Maxton's question regarding international regulation of the telecommunications networks, governments across the world are taking steps to limit their networks' exposure to high risk vendors. In many cases, governments are adopting similar measures as the UK to address these risks and adapting them to meet national circumstances.

Collaboration across Whitehall

My noble friend, Lord Young of Cookham, and other noble Lords asked if I could explain the responsibilities for managing cyber security across government.

Ministerial responsibilities for cyber security are necessarily distributed across departments, given the various departmental equities and the need for a whole of government response to the challenges we face.

The First Secretary of State provides leadership across departments to ensure the Government's response to cyber threats and our ambitions as a cyber power are fulfilled. He chairs a ministerial small group to coordinate cyber decision-making across government, as described in the Integrated Review. Other members of the

[7] https://www.gov.uk/government/publications/government-response-to-the-telecoms-diversification-taskforce

group are the Chancellor of the Exchequer, the Chancellor of the Duchy of Lancaster (currently delegated to the Paymaster General), the Home Secretary, the Defence Secretary and the Secretary of State for Digital, Culture, Media and Sport. Other ministers are invited to attend depending on the topics being discussed and senior officials from the intelligence community and law enforcement agencies also attend. The meeting is supported by the National Security Unit in the Cabinet Office.

My noble friend, Lord Young of Cookham, asked about the membership of the National Security Council. The membership of all Cabinet committees, including the National Security Council, is published on GOV.UK[8]. Other Cabinet ministers attend the Committee as required and depending on what the Council is discussing.

National Security and Investment Act

The noble Baroness, Baroness Merron, raised the definition of the communications sector within the National Security and Investment Act. The Department for Business, Energy and Industrial Strategy will be publishing draft notifiable acquisition regulations in due course, which Parliament will then have an opportunity to discuss.

Human Rights

As I said at the despatch box, this Bill is not the right legislative vehicle to address the important issue of human rights. The Bill is focused on the security of the UK's public telecoms networks and services, and a designation notice can only be issued to a vendor where the Secretary of State considers it necessary in the interests of national security. The Government shares noble Lords' serious concern about the human rights situation in Xinjiang, and has taken a wide range of action this year to address the human rights violations taking place in the region. I detailed these in my closing remarks to the House on Tuesday.

I would encourage noble Lords with concerns about this issue to engage with the Foreign, Commonwealth and Development Office and Home Office, who are the lead departments on this topic.

National Infrastructure Commission

The noble Lord, Lord Stirrup, asked about the 2020 report of the National Infrastructure Commission into infrastructure resilience. The Cabinet Office and HM Treasury have been working with relevant departments and agencies to develop the Government's response to the report. The response will be published this summer. The recommendations have been considered within wider Critical National Infrastructure policy and the development of the National Resilience Strategy. Where the recommendations will be implemented, they will be done so within this wider context.

[8] https://www.gov.uk/government/publications/the-cabinet-committees-system-and-list-of-cabinet-committees

Fraud
The noble Lord, Lord Vaux, raised the important issue of fraud that is facilitated via calls or text messages. As I said during the debate, this Bill is not intended to address these issues. There is already legislation in place aimed at tackling fraud. This Bill will, however, help to protect against security vulnerabilities and compromises in our networks that might be exploited to facilitate fraud more widely. I would encourage noble Lords to engage with the Home Office on these matters as the lead department on these issues.

Computer Misuse Act
My noble Friend, Lord Holmes of Richmond, asked about progress with the review of the Computer Misuse Act 1990. The Home Secretary announced a review of the Act in May this year, the first stage of which was a public Call for Information to seek the views of those with an interest in this legislation as to how it could be enhanced.

The Integrated Review committed the UK to fortifying its position as a world-leading and responsible cyber power, taking a new, full spectrum approach to the UK's cyber capability through keeping our people safe, staying ahead of our enemies and improving the lives of the British people.

As part of that, the Government is clear that we need to ensure that we have the right legislation in place to criminalise the activity that causes harms to UK citizens in cyberspace, the right powers to support law enforcement agencies in carrying out investigations, and that it supports the overall Government aim of protecting the UK. We will consider the proposals that we have received to the Call for Information, and will provide a response in due course.

Retiring of copper networks
My noble Friend, Lord Holmes of Richmond, asked for assurance that vulnerable consumers will not be impacted by the retiring of the copper network in the Public Switched Telephone Network (PSTN). The withdrawal of PSTN is industry-led. Fixed-line operators, including Openreach and Virgin Media, will cease to provide copper, legacy services in a phased approach with the network expected to switch-off entirely in 2025. The PSTN will be replaced by 'voice over internet protocol' (VoIP) technology, which carries voice calls over a broadband connection. The change is expected to offer consumers clearer and better quality phone calls. The Government, Ofcom and industry are working together to ensure consumers - in particular those who might be considered vulnerable - and businesses are protected and suitably prepared for the withdrawal process.

I hope this letter is helpful, but please do get in touch with my officials via dcmslordsminister@dcms.gov.uk if you have any further questions about the Bill or you would like to meet with me to discuss it. I will place a copy of this letter in the library of both Houses.

With best wishes

Baroness Barran
Minister for Civil Society