Telecommunications (Security) Bill – Briefing

About Comms Council UK

Founded in 2004 (and formerly known as ITSPA) Comms Council UK is a UK, membership-led organisation that represents companies who provide or resell business and residential customers voice services over data networks (VoIP) as well as other "over the top" applications including instant messaging and video. The membership is a mixture of network operators, service providers, resellers, suppliers and consultants involved in a sector that is diversifying rapidly from just voice services to other innovative IP applications.

Contact

For more information, please contact:

Comms Council UK
team@commscouncil.uk
020 3397 3312

Telecommunications (Security) Bill

The Bill represents an unprecedent shift of power from Parliament to the DCMS Minister in relation to how telecommunications networks operate.

The Minister will be able to unilaterally make decisions that impact the technical operation and direction of technology companies, with little or no oversight or accountability.

DCMS have been attempting to overcome objections raised by the industry regarding the heavy-handedness of the legislation by referring to future clarification in Guidance or the anticipated Code of Practice.

Neither of these will be published before the Bill is expected to receive Royal Assent. Therefore, as it stands, the industry must trust that this and all future administrations, will not avail themselves of the extensive executive power the Bill allots.

By way of two examples:

1. The Regulations (a draft of which was published here) are likely to be laid before Parliament under the negative procedure; statistically this is a near guarantee of their coming into force. Section 105B of the Bill affords the Minister the ability to make regulations that have highly invasive provisions as currently drafted (some cited in the Annex to this briefing). There is no provision for any independent or specialist oversight of these Regulations.
2. The Bill, if enacted, will require the Minister to consult with various stakeholders on the Code of Practice (Section 105F(1)), but does not contain a provision requiring him to take account of consultees' views prior to enacting such a Code.

Severally, these two proposed statutory provisions amount to a near unfettered ability for the Minister to interfere in the normal operations of an otherwise innovative and successful industry. Any guidance from DCMS, or provisions in a Code of Practice, may give some comfort today, but are no guarantee or protection from a Ministerial retraction tomorrow.

Comms Council UK recognises the moral hazard posed by certain vendors, such as Huawei, whose pricing can be seductive to an industry characterised by high competition and low margins. We equally

recognise the risk to national security posed by networks which do not take such matters seriously. However, Government intervention in a highly innovative industry, which is often operating cross-border, must be proportionate to what it intends to achieve.

In a similar context, in the Investigatory Powers Act 2016 (the "**IPA**"), the risks of an unfettered concentration of power in the executive were addressed with two simple solutions:

- The establishment of a Technical Advisory Board[1] ("**TAB**"), whose role is to advise the Home Secretary on the reasonability of obligations imposed on communications providers, and
- The establishment of the Investigatory Powers Commissioner's Office[2] (the "**IPCO**"), to provide independent judicial oversight of the exercise of the powers in the IPA.

Comms Council UK understands that, for reasons of national security, a public consultation on the exercising of certain powers in the Bill will not be possible. However, we see no difference to having technical and judicial oversight in requiring bulk surveillance capabilities, with proposed specified security measures. We also note that the IPCO and TAB already exist and therefore any additional burden on public resources is merely incremental and should not be material.

As an aside, Comms Council UK is also concerned of the use of negative procedure for such invasive regulations. As an example, our members have recently endured the extensive cost of the sudden implementation of the reverse charge VAT regime upon mere days' notice and absent consultation. Additionally, we believe the Intelligence and Security Committee would appear to be a logical scrutiny forum, especially given the security clearance concerns relating to the material it may need to scrutinise, to at least supplement the work of DCMS.

To address the concerns above, we would suggest an amendment to the Bill by inserting two sections as follows[3].

1. Insert 105D(7) to say "*In making regulations under this Section, the Secretary of State must take the utmost account of the advice of the Technical Advisory Board and a Judicial Commissioner concerning the proportionality and appropriateness of any measures therein.*"
2. Insert 105F(1)(d) *"be satisfied that the Code of Practice is necessary and proportionate to what it intends to achieve and does not place an unfair burden on any electronic communications networks or electronic communications services".*

These will give rise to two further amendments to enable, firstly a requirement to define the TAB and Judicial Commissioner by simple reference to the IPA and secondly it would be advisable to list the TAB and IPCO as bodies to consult in section 105F(1)(b).

[1] https://www.gov.uk/government/organisations/technical-advisory-board [accessed 25th June 2021]
[2] https://www.ipco.org.uk [accessed 25th June 2021]
[3] These are nearly identical to those in CCUK's submission to the Public Bill Committee on the subject.

Annex – Examples of Overburdensome Regulations[4]

Case Study 1 – The Patch

Section 7(2)(k) of the Regulations requires that all providers *"take proportionate measures to deploy appropriate and effective patches or mitigation relating to risks [..] within 14 days from which the patch or mitigation becomes available*" unless the provider maintains a written record of why it was not reasonable to do so.

There are several reasons why this provision is disproportionate, even unworkable.

There are 450+ Public Electronic Communications Networks ("**PECNs**") in the UK which the Office of Communications (Ofcom) knows of and more than 1,000 independent providers of Public Electronic Communications Services[5]. There is no registration requirement in the UK, therefore the number is likely to be higher. Many of these are smaller operations without dedicated teams focussed on this, yet they will have to ensure they either always patch their system in a fortnight or have a process by which they record their inability to do so in writing.

Many of these operations have fewer than 10 employees and we are not aware of any cost-benefit analysis that considers the true scale of the burden on the industry. An assumption that the world is composed of a handful of vertically integrated major household names is a dangerous one.

The Regulations introduce a moral hazard of quick patching to tick a legislative box, which increases the risk of unstable patches being applied to networks – while they may, on the face of it, increase security, they may cause other issues, such as outages affecting the ability for users to access emergency services.

Fourteen days for an end-to-end process is not realistic. During this period, a provider is expected to become aware of a patch being available, assess the patch, test the patch, and then create a maintenance window with their customers. Customers in turn may have to onwardly notify or require it in their own test environment before application may go live. This is just not feasible, especially when many enterprise and government users require more than fourteen days' notice of system changes.

Case Study 2 – Foreign Network Operations Centres ("NOCs") and Diagnostics

While the definition of Signals in Section 32 of the Communications Act 2003 is very widely drafted and can be interpreted as encompassing almost anything, we recognise that the reference to "content" in Section 4(3)(f)(ii) in the Regulations is fettered by the definition of Systems Data in Section 263(4) of the Investigatory Powers Act 2016.

That excludes "*any data that enables or facilitates, or identifies or describes anything connected with enabling or facilitating, the functioning of any of the following—[..] a telecommunications system [..] any telecommunications service provided by means of a telecommunication system;*"

[4] This is an abridged extract from a letter from CCUK to DCMS [09.01.21]

[5] See Gamma Communications plc Annual Report, which cites the number of channel partners and resellers it services by way of example of just one whole network's supply chain.

While we consider it a slightly circuitous way of achieving a result of excluding metadata about past events, there remain three problems with the drafting of the Regulations.

1. Monitoring and audit are not defined terms, which means their ordinary and natural meaning applies; it is difficult to see how a reasonable layperson would not consider the traditional functions of a NOC to be 'monitoring and audit.'
2. The reference to "real-time" is not captured by the Systems Data definition.
3. Media sampling[6] is a valid monitoring and diagnostic tool and that relates to the content of signals – the regulation would prevent third line support operations, e.g. Cisco or Juniper in the USA, from performing such diagnostics.

The effect of the provision as drafted causes the following significant issues for providers;

1. If they operate a NOC outside of the UK (including in a British Crown Dependency for that matter), they will be required to create a new NOC within the UK's border.
2. It renders them unable to seek assistance from vendors where real-time diagnostics are required or where media sampling is required, including those vendors producing security-critical systems in Britain's long-standing allies, such as the United States of America.

Ironically, this could leave systems exposed to security risks for longer as cumbersome work arounds are used to comply with the Regulations.

Case Study 3 – Long Supply Chains

As we noted in Case Study 1, the value chain in UK telecommunications can be quite complex.

Even if we assume that the contractual bargaining power DCMS appear to rely on in Section 6(2)(b) is stronger in the likes of BT and Vodafone, there are 450+ PECNs in the UK, the majority of which have little or no bargaining power, especially when dealing with Amazon Web Services, Ribbon, Google, or Microsoft.

We do recognise that a legislative change in the UK may create market forces which incentivise such suppliers from making appropriate changes, however DCMS is promoting a supply chain diversification strategy which will dilute that impact.

Additionally, Regulation 6(1) is so widely drafted, it includes anyone involved in the provision of the service.

[6] Media sampling is a technical means by which the root cause of an issue with the quality of a voice communication (or, where relevant, data over voiceband communications, such as PDQ machines, red pull cords etc) can be diagnosed. This may be done algorithmically through dedicated monitoring equipment or can require a qualified engineer listens to the media in question.

Gamma, a CCUK member, reports that such an activity occurs within their NOC in the order of 2-3 times a day and would be impossible under the draft Regulations if that NOC were located abroad. Other CCUK members with significant UK operations run global NOCs abroad which would be severely disrupted.

It says;

> "*A network provider or service provider must identify and reduce the risks of security compromises occurring as a result of the provider depending on other persons ("third party suppliers") to supply, provide or make available goods, services or facilities for use in connection with the provision of the public electronic communications network or public electronic communications service*."

We assume that the definition of "security compromise" in the Telecommunications (Security) Bill applies. We note that this is also very widely drafted.

It is entirely possible that a major mobile network operator depends upon their bank to provide automatic top-up services to prepaid customers, or to payment intermediaries for credit card processing in the provision of their service.

Street works are often performed by small local subcontractors of a subcontractor in a long value chain. Installations of routers on end user premises may be outsourced to a local IT company.

The scale and complexity of the value chain is such that it would be a monumental task to include the required Regulations in all future negotiations, let alone modify all existing ones – even assuming that the counterparty will corporate (e.g. Amazon) or has the resource to (e.g. a one-man band local installer).

Amendments to Regulations

Comms Council UK believes that if appropriate oversight were to apply to the making of these regulations, the issues cited above would be fettered through (1) a relaxation of countries where NOCs could be located, such as in a NATO country etc., (2) that patch application be 'reasonable and proportionate,' and supply chain audits required 'to the extent feasible'.