Internet Telephony Services Providers' Association

ITSPA submission on The Electronic Communications (Security Measures) Regulations 2021 (the "Regulations")

The Internet Telephony Service Providers Association ("**ITSPA**") would like to thank the Department for Culture, Media and Sport ("**DCMS**") for the time on January 29 where we discussed the practical implications of the Regulations.

As discussed, we have expanded upon the three main case studies referred to and cross-referenced to the Regulations and suggested amendments to the legislation to mitigate some of the consequences that arise.

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. 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 takes into account the true scale of the industry. It is worth remembering that the UK telecommunications industry is comprised of hundreds of PECNs, with thousands of independent entities providing Public Electronic Communications Services (PECS) to end users. 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. We would respectfully suggest DCMS engage with major central government telecommunications users, which we are sure is an exercise that will reaffirm the sentiment.

ITSPA members take the issue of security seriously and are not going to treat running a system missing an important patch lightly, however constraining the timescales as a matter of law is not the best approach.

We would suggest 4(k)(i) and (ii) are replaced by appending "as soon as reasonably practicable" to the end of 4(k).

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;*"

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 layman 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 is a valid monitoring and diagnostic tool and that relates to the content of signals.

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 borders.
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.

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, an ITSPA 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 ITSPA members with significant UK operations run global NOCs abroad which would be severely disrupted.

We do not believe it is the intent for DCMS to create these issues and therefore we would make the following suggestions:

- Increase the geographic limits of Section 4(3)(f) to include the Five Eyes Countries, NATO, NATO plus the European Union or some other compromise position.
- Fetter the same section by including the words "nothing in this section shall preclude a network provider from diagnosing faults or monitoring the integrity of their network using Affiliated Companies outside the UK nor seeking assistance from a vendor for the same".

Affiliated Companies is a standard term in common usage which would encompass parent companies and their subsidiaries as well as subsidiaries of the network provider.

Section 6 would, in our opinion, either as drafted or as we suggest it should be drafted, provide a basis for ensuring such Affiliated Companies or vendors take their UK legal obligations with respect to security seriously.

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

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).

We would strongly suggest that this entire section is reduced in scope to "security critical functions" as defined in the Regulations and fettered by "all reasonable steps to".

Risks

If these widely drafted requirements become law, there is a very real risk that it will increase costs, which will be passed on to consumers, or reduce choice – ultimately leading to the same inflationary outcome.

This is a time when Parliamentarians are calling for a "social tariff" for broadband for the less privileged and when businesses have been seriously disadvantaged due to a pandemic. We recognise and support the need to procure a secure telecommunications infrastructure for the UK; however, how Parliament achieves it must be proportionate to the issues and not jeopardise the achievement of other political objectives.