Telecommunications Security Bill: ISPA Bill Committee Submission

About ISPA

1. ISPA is the trade association for providers of internet services in the UK. We represent over 150 members, covering the full internet access ecosystem that includes communications providers that serve consumers and businesses, those that build their own networks and those that resell the infrastructure and services of others to end users. Ninety per cent of our members are SMEs, and many would form part of the Third Tier of providers as identified in the upcoming regulations, in addition to many large and multinational companies who would fall into the higher two tiers and subject to greater powers.

Summary of Main Points

In summary, to ensure a more proportionate implementation of the new requirements and strike a fair balance we are calling for:

- A further and full impact assessment of the Bill, and subsequent secondary legislation and Code of Practice, to determine a proper cost benefit analysis
- Sufficient time to be given for parliamentary scrutiny and for consultation with industry to understand, plan and build systems to meet the new requirements
- A streamlined notification system to provide industry with greater clarity against the increasing number of regulatory requirements in this area
- A proportionate approach to implementation that should include writing the three-tier approach into the face of the legislation as well as safeguards to limit the open-ended compliance costs of third parties and use of notification powers
- The criteria for being designated an "authorised person" should be set out in the Bill or in secondary legislation to minimise the risks of sharing data with government and Ofcom
- The removal of a new civil liability for breach of security duties, or failing that additional safeguards around its use
- Consideration of a cost reimbursement scheme in certain circumstances to offset the impact of removal of High-Risk Vendors in certain circumstances
- Further oversight of vendor direction powers through a Technical Advisory Board and Judicial Commissioner

Introduction

2. The UK is a leading digital economy that is powered by a communications infrastructure and services that provide the UK with fast, reliable and secure connectivity. This has been demonstrated throughout the Covid-19 crisis, where our members successfully managed increases and changes to network demand, allowing the country to work from home, support home schooling and communicate with friends and families, and continue to do so.

3. Security is a priority for industry and fundamental to how an ISP runs its network and ensures trusted, good quality and consistent connectivity. Our members recognise the importance of security and have worked to uphold these standards, and as threats change and evolve and as our infrastructure and services develop, we are broadly supportive of the new set of measures that will upgrade security requirements, and we welcome Government's assistance and guidance on what good security looks like. However, the Bill must strike a fair balance between the regulatory and administrative burdens placed on industry against the need to encourage our members to continue with the vital broadband infrastructure upgrade underway.

4. Our members are funding a once in a generation infrastructure upgrade, investing billions in rolling out gigabit capable broadband in the fixed space via fibre and other solutions and 5G in mobile. This is happening on a national, regional and local level and led by a range of providers, from large established names to newer independent networks. These endeavours are funded overwhelmingly by industry with limited Government gap funding to help in remote areas, and even this funding has been scaled back by DCMS in the short term. Government and policymakers can best support this significant infrastructure deployment by providing a consistent, stable and proportionate regulatory framework, reducing barriers and red tape to broadband deployment and ensuring a proportionate approach to new obligations and regulations, including security measures.

Process and consultation

5. The Bill provides the overarching legal framework for a significant upgrade of existing telecoms security powers that will establish new obligations and standards consisting of '5-10 sub-duties, and then 40-50 security requirements'[1]. A significant amount of the actual detail will be left to secondary legislation and delegated powers, including a Code of Practice which has yet to be published and will only be subject to public consultation once the legislation has passed. As Parliament is being asked to scrutinise legislation without seeing this detail in full, it is therefore important that Parliament is given sufficient time and resource for further and full scrutiny of the secondary legislation and its sub duties. The sooner all the relevant documents can be shared, even in draft form, with industry and parliament the better.
   - **Recommendation: a restatement of expected timings with sufficient time to be given for parliamentary scrutiny, and a clear and sensible timeline for implementation to enable our members to understand, plan and build systems to meet the new requirements.**
   -
6. The consultation with industry to date has been selective, which given the detailed technical nature and sensitivities that surround the regulations is somewhat understandable. However, there is a need to now expand consultation from largely closed security group discussions to a broader set of stakeholders. The internet and telecoms sectors are complex, consisting of hundreds of companies that own their own networks or infrastructure or resell others or a mix of the two, sufficient thought therefore needs to be given to this ecosystem and the mostly SMEs that comprise it. The impact assessments that accompany the legislation provide context and background but were compiled without proper industry consultation. Without further detail on the form that the Code of Practice will take, we consider it difficult to make an informed view on the cost benefit analysis of the Bill at this stage.
   - **Recommendation: Further industry consultation, including a more complete impact assessment, be undertaken by Government**

7. We are concerned that the UK framework is moving towards a highly prescriptive, burdensome and inflexible regime which may introduce localised measures for multinational companies. Such localised measures increase cost and burden, and raise the risk of duplication. This is especially true for multi-national providers who operate global security policies based on international standards that ensures a consistent approach to security around the world. Instead, we consider that cybersecurity policies should be more outcomes-based and should define pragmatic and flexible principles, rather than prescriptive measures.

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/937142/FINAL_The_Telecommunications_Security_Bill_2020___The_Telecoms_Security_legislation_-_Acc.pdf

Regulatory duplication

8. Telecoms security is currently subject to a number of existing regulatory requirements. This ranges from the Communication Act which the TSRs will be building on; the Privacy and Electronic Communications Regulations; the Network Information Security Regulations; Investigatory Powers Act; GDPR; and voluntary best practice measures and accreditations. Further, the National Security and Investment Bill will also provide for greater scrutiny of the communications sector through mandatory notification and extensive national security screening powers. These powers cross several different regulators and bodies including the ICO, Ofcom, NCSC, Home Office, Intelligence agencies and DCMS. This ever-growing set of bodies and obligations has the potential to bring about confusion and duplication, particularly as it involves sensitive security information. As an example, if a security breach occurs which regulator and under which regulations would a provider need to inform first? This also leads to the risk of double enforcement and/or penalties. This is further compounded for multi-national operators who must also managing diverging regimes across other countries.
    - **Recommendation: We recommend DCMS lead on a streamlined breach notification process to help manage the growing and competing requirements in this area**

Proportionality

9. We welcome Government's commitment to proportionality by applying the measures through the proposed three-tier system in the initial code of practice. However, there is currently no reference to this in the Bill, despite several detailed clauses in the Bill on the codes of practice. This means that ISPs do not currently know which Tier they will be in and therefore will find it difficult to determine the impact and resulting cost of compliance at this stage.
    - **Recommendation: To provide full and complete clarity the tiered approach should be written into the face of legislation.**

10. The Bill contains extensive and potentially open-ended measures to enable Ofcom to perform its duties. For example, Clause 1050(2) sets out a range of measures that Ofcom can give to enforce an assessment notice. Providers will be expected to cover undisclosed costs accumulated through the provision of information to Ofcom and DCMS, as well as potential costs such as re-planning the network or running new procurement exercises. This includes the ability for Ofcom to use external consultants for compliance assessments with the costs passed on to industry (clause 105N(2)(b)) and there is currently no set financial limit nor any proportionality considerations. This also differs from the existing funding model where annual fees are paid to Ofcom, based on relevant turnover, to fund all other Ofcom compliance work.
    - **Recommendation: the Bill should consider a cost sharing principle to limit third party costs**

11. We are concerned about the requirements around the flow of sensitive security information between ISPs, Ofcom and the Secretary of State, which is likely to increase risks to ISPs. Indeed, it is noted that Ofcom staff or Ofcom contractors can be "authorised persons" and therefore will have the ability to access sensitive information, systems, premises and documents; yet there is no requirement in the Bill for these people to be appropriately security cleared.
    - **Recommendation: the criteria for being designated an "authorised person" should be set out in the Bill or in secondary legislation.**

12. Section 4, informing others of security compromises, puts duties on providers and Ofcom to notify customers of compromises in certain situations. While we are supportive of transparency and

openness driving better security practices, we feel it is important that these potentially intrusive powers are handed proportionately:

- Clause 105J: Duty to inform users of risk of security compromise – while we understand the importance of transparency and informing and educating the public, there is the potential for this to be exploited for nefarious means, particularly if customers are advised to take technical measures to fix a reported problem.
- Clause 105L(7) – Ofcom has the power to inform the public of security compromises where it is in the public interest. We recognise this could be helpful in informing the public and recommending what steps to take, but in what context will this be used, does a certain threshold have to be met and is there a way of measuring whether appropriate actions have been taken by users?

Civil Liability

13. Clause 8 - a new civil liability for a breach of security duties – appears to be incredibly broad and a significant extension of the existing liability regime. No service can be wholly secure and so there is potential to open up a large number of claims, many of which would be frivolous and likely to be unsuccessful, yet it would be immensely costly for CPs to manage this process at a time where the focus is on investing in security and network upgrades. Serious breaches of security obligations ought to be a matter investigated by Ofcom, and there are already significant penalties for failure to meet these security duties. Third parties currently have access to recourse and bring a claim in tort if they had suffered a loss. This clause would however put any such potential claim onto a breach of statutory duty footing.
    - **Recommendation: Removal of Clause 8 or if retained the addition of safeguards**

14. The requirement for Ofcom to approve the bringing of proceedings would act as a safeguard, yet it also effectively means that if Ofcom were to give its permission, it would be signalling that it thinks the duty has been breached, and then any claimant simply needs to show in court that they have suffered damage and that it arose from the breach. Whilst a CP could challenge in court that it did not think the duty had been breached, it makes the task much harder given Ofcom would have already made its view clear. Also, for example, in a scenario where there has been a data breach caused by a security breach, a CP would be facing two potential claims (one for data protection breaches and one for security), as well as a potential fine.

15. If the clause is retained, we suggest some further steps to act as safeguards:
    - Implementation - At present, Clause 28(3)(b) provides that clause 8 will be introduced at the discretion of the Secretary of State via statutory instrument. This could theoretically be the day the Act is brought into force. This would mean that legal action could be taken against a CP before we have implemented the security requirements. Therefore, this clause should only come into effect at least six months after we have implemented each new security requirement.
    - Liability - The drafting of Clause 8(5) suggests the onus is on the CP to show it has taken "all reasonable steps […] to avoid contravening the duty in question", suggesting the default position will be that unless the CP shows this, then the CP is liable. We believe that the default position should be a CP is only liable if the breach arose directly out of a failure to comply with the TSRs, and not otherwise.
    - Clarification – Government should provide more clarity on what exactly the scope of liability would be and whether there will be any guidance on this.

High-Risk Vendor Restrictions

16. The Bill is implementing the findings from the Telecoms Supply Chain Review which concluded that new restrictions on the use of high-risk vendors be introduced through a cap and ban in sensitive parts of the network. A number of our members have made public statements on implementation of the review and are working closely with Government on this. To help the rollout of gigabit broadband we now need to see a clear and proportionate direction and consistency based on the review's conclusions rather than ever-changing expectations.

17. The High-Risk Vendor policy is enacted through the Designated Vendor Notice and Direction powers. These contain detailed measures and considerations and represent a significant extension of Government's powers. We welcome the commitment for consultation with the communications provider which is subject to the vendor direction. Such powers, however, do not appear to require any oversight, particularly in cases of "national security" as cited by the Secretary of State. Whilst we do not seek to underplay the importance of protecting national security, we believe it reasonable, under the circumstances, that oversight be provided in a similar way to that of the Investigatory Powers Act 2015 (IPA) through a Technical Advisory Board and Judicial Commissioner to provide scrutiny and ensure that any Executive action is proportionate, feasible and warranted.
    - **Recommendation: Further oversight through a Technical Advisory Board and Judicial Commissioner**

18. The full impact of the HRV restriction policy on fixed fibre networks is still being determined. There are a large and diverse number of companies involved in providing an often-interlinked range of networks and services to end users. Some of these companies will be SMEs that may lack the same level of compliance and financial support as others in the industry. We note that in the US, the FCC will reimburse smaller operators impacted by a direction to remove high risk vendors from their networks through the Secure and Trusted Communications Networks Reimbursement Programme[2]. As the impact on fibre networks is being considered, ISPA suggests Parliament consider whether a cost reimbursement scheme may be appropriate in certain circumstances. This has long been the case in relation to communications data legislation compliance.
    - **Recommendation: A cost reimbursement scheme for removal of High-Risk Vendors should be considered in certain circumstances**

Conclusion

We are broadly supportive of the new legislation but as set out above we believe it can be strengthened in several areas. We hope the Committee find the briefing paper of use. We would be happy to follow up on any of the points raised.

[2] https://www.congress.gov/bill/116th-congress/house-bill/4998/text