ISPA comments on Telecoms Security Bill draft Statutory Instrument

Introduction

ISPA welcomes the opportunity to submit comments on the Telecoms Security Bill draft statutory instrument (SI) regulations. We have identified several concerns and questions with the draft SI that we have set out below. We would be happy to expand on these points further.

Services outside the UK

We recommend reviewing the duties that seek to limit reliance on foreign services so that it allows some reliance on countries that share the UK's overall approach and attitude to security and where we have existing cooperation channels, such as the 'Five Eyes' alliance and EU.

The SI contains several references to maintain the operation of a network or service 'without reliance on persons, equipment or stored data located outside the UK'. This has the potential to significantly change and disrupt how providers operate their networks and even undermine their viability. This will impact both national-headquartered operators and global operators, including providers of services to multi-national organisations that support the UK's participation in international trade.

Telecommunications is a global interconnected industry with many different parts and layers. It is not unusual for an operator to rely on offshore support and technical assistance in some shape or form. In doing so, the provider would take the necessary steps to secure the data and service for which its reputation and performance depends on. At a time when the UK looks to a more global international role, this proposed more protectionist approach could harm the UK's critical tech sector. If Government's intention is to ensure providers must only rely on UK services, then it should clearly state this and explain how this is to be achieved, how to procure the same services in the UK and over what timescale.

Data Localisation

We recommend reviewing whether the data localisation duty is proportionate and workable.

There are several sections of the SI which appear to impose some form of data localisation (eg: Sections 3(3)(f), 4(3)(f), 5(3)(h), and 8(2)(a)). This would go against the cross-border data flows provisions of the recently agreed EU-UK Trade and Cooperation Agreement[1] and could jeopardise future trade deals that the UK is seeking to pursue. Duplication of data increases costs and does not necessarily increase data security – indeed it creates further attack vectors by increasing the number of potential entry points. What matters is not where the data is stored but rather how secure it is. We strongly reject these provisions.

Section 4, protection of data and network functions, states tools enabling monitoring or audit cannot be accessed from outside the UK. It is not clear how this would impact providers with global or multinational operations, who are subject to a range of national, governance and auditing requirements. Therefore, for businesses that operate in multiple jurisdictions, meeting these

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22020A1231(01)&from=EN, specifically Title III, Chapter 2, Article DIGIT.6 "Cross-border data flows" (page 119).

requirements could directly conflict with laws in other jurisdictions. These provisions, combined with the large scope and extra-territorial impact of the National Security and Investment Bill, will reduce the attractiveness of the UK for investment.

Monitoring and Audit

The data storage requirements in section 5 are unclear, risk undermining competition and seem disproportionate compared to existing powers in the investigatory powers regime.

Section 5 (3) (a) & (d) includes a duty to hold data to maintain a record of all access to the network and service for at least 13 months. It is not clear exactly what level of data will need to be recorded in order to meet these requirements beyond excluding the content of signals. For example, is it aimed at holding data on end user access to services, internal access logs or Internet Connection Records? Until further detail is provided of what is required, it will be difficult to give a complete response as to the technical or practical challenges in meeting this obligation. However, any storage requirements that go beyond what our members already store for business purposes is disproportionate and risks undermining competition and the Government's wider targets for the rollout of gigabit-capable networks.

Powers to retain communications data have been place for many years through the Investigatory Powers Act and preceding legislation. These powers include a range of safeguards and support for providers, including a SPOC regime and cost recovery, to meet these obligations, which are limited to 12 months and are targeted through a notice regime, in addition to privacy controls. If the Regulations are looking to impose similar or even remotely similar obligations, an equivalent framework should apply. This should include financial compensation and assistance to meet the obligations.

As mentioned, existing communications data retention powers are served under notice in a targeted manner, rather than applying to all providers of public electronic communications network and services. There is therefore a competition issue in that some providers will have developed systems, with Government support, to retain data that could potentially be repurposed for these regulations. Providers that do not currently have an obligation to retain data would be disproportionately affected as they would have to build, develop and manage systems from scratch without Government support and without ongoing cost recovery. This will particularly impact those providers who are currently making a significant effort to meet the wider gigabit-capable rollout targets.

More clarity is needed on what measures would be required to prevent activities that unreasonably restrict monitoring.

Section 5(2)(e) has potentially wide-ranging consequences, particularly as there are ongoing changes to encrypt various layers of the internet architecture. We require more detail on what action would be required from providers to comply with this section before we can provide an assessment of its impact.

Patches

The proposed time limit is too restricted to appropriately recognise and address a security compromise. We recommend a less prescriptive time for patching of 'within a reasonably practical timeframe'.

Section 7 (2)(K) includes a specific time limit of 14 days to deploy an appropriate patch to mitigate risks of security compromises, although a longer time period may be determined by the provider on reasonable grounds. Fourteen days is too short a period to become aware of and react to a security patch in what is a complex, multi-layered sector. Providers should be encouraged to plan and implement patches effectively and safely, rather than meeting an arbitrary deadline. The fact that there is a caveat that allows further time to patch reinforces this point. We therefore suggest, a less prescriptive time of 'within a reasonably practical timeframe' rather than 14 days while retaining the flexibility for providers currently in the text at Section 7 (2)(k)(ii).

More generally, the Regulations should not limit effective security remedies to just "patches" and should allow for other forms of remedial solutions that effectively mitigate or cure a security risk.

Supply Chain

Government should investigate how there could be more incentive for the supply chain to fulfil its security obligations.

Telecoms supply chains are complex interlinked networks that comprise global, multinational companies. Any regulatory-driven changes to contractual conditions between our members and their third-party suppliers which go beyond the robust processes they already have in place would be a significant undertaking that would require significant time to achieve.

Contractual negotiations with large vendors may be challenging and present a significant challenge for smaller firms in particular to be able to manage and, where necessary, change practices. Where the supply chain includes smaller, less established suppliers or innovative start-ups, understanding their supply chain will present a separate but equal challenge, potentially shutting less established but innovative suppliers out of the market.

Government should also consider that not all vendors and/or equipment in the market can support some of the requirements – Government needs to allow for technical feasibility or a "where possible" flexibility at least in the initial implementation period for the more prescriptive technical requirements and should be realistic about the timelines for meeting the end-state foreseen by the Regulations. If a significant supplier is unable to meet the demands or obligations of new UK rules it could reduce choice in the market. It could also act as a disincentive for new entrants into the market, a key government priority through its diversification strategy.

Recognising that security risks exist at numerous points in the online ecosystem, there is a fundamental role for all actors of the digital value chain to do their part to ensure the UK's digital infrastructure remains secure and resilient. That said, the current framework places the burden of compliance and enforcement measures on the service or network providers. We question whether such providers should bear the full responsibility, especially for elements which are outside of their control. Government should be investigating how there could be more incentive for the supply chain to fulfil its security obligations.

Security critical definition

We recommend limiting the definition of security critical function to include only functions that are security critical.

The aim of the legislation is to boost security critical functions and standards. It is important that the legislation is limited to this and does not extend beyond it. In the definitions, we recommend limiting the definition of 'security critical function' to only focus on security critical functions and not any function which could materially have an impact, drawing the definition of security critical function too widely. To achieve this, we suggest deleting *"and includes any function of the network or service whose operation is likely to have a material impact on the proper functioning of a security critical function."*

Implementation timelines

While we understand the Codes of Practice will give further detail on the implementation timelines for providers, we stress that the prescriptive and detailed nature of the SI will mean that providers will need sufficient time to digest the new requirements and plan for implementation. This will be a significant undertaking, regardless of size of the provider, and Government should be conscious and plan sufficient time for this.