**ISPA Response to the draft Investigatory Powers Act Technical Capability Notices consultation**

## Introduction

ISPA welcomes the opportunity to submit comments to this draft Investigatory Powers (Technical Capability) Regulations targeted consultation. We represent a broad range of companies with the potential to be affected by these regulations in different ways, including companies with direct experience of dealing with similar obligations under previous legislation and companies that may be affected now and in the future.

## Consultation process

ISPA received notice of the consultation and a copy of the draft regulations less than an hour before the commencement of purdah on April 21st. Cabinet Office guidance states new consultations should generally not be published during purdah, so we find it unusual that a consultation in this area is being undertaken over a short four-week period where there is no sitting parliament and at a time when government traditionally does not develop new policy.

Technical capability notices (TCNs) are a significant part of the Investigatory Powers Act and have the potential to place very burdensome obligations on industry. The Act and draft regulations go substantially further than the previous obligations under RIPA. Therefore, the supporting Regulations and Codes of Practice must be drafted carefully to avoid placing a disproportionate burden on providers. This is especially the case in this instance given the increased scope of the Act. It extends obligations beyond interception to include communications data and equipment interference, extends the definition of telecommunications operator to private as well as public networks, and also applies to the development of new services. In light of this we would hope to see our recommendations addressed and full and appropriate consultation across all of the industry going forward.

## Smaller operators

There is a notable inconsistency between the accompanying Home Office letter and the draft Regulations in the application of the powers. The letter says that small telecommunications operators (both public and private networks) with under 10,000 persons cannot be obligated to maintain a technical capability in relation to interception and equipment interference, but may be required to give effect to a warrant. This is also set out in the draft Equipment Interference draft code of practice. However, in the draft Regulations the 10,000 limit only applies to Schedule 1 (interception warrants) and Schedule 3 (equipment interference), but not Schedule 2 (communications data). This suggests that even operators serving less than 10,000 persons could be required to build a capability to provide communications data acquistion. Not only is this inconsistent, it runs counter to the aim of only serving a notice where there is a recurrent need. The potential impact of smaller companies operating both public and private networks under the new Act having to maintain a capability for

communications data is significant, disproportionate and would be a costly undertaking. The draft Regulations should therefore be amended to make clear that the 10,000 persons threshold also applies to Schedule 2, communications data acquisition.

Furthermore, the draft Regulations do not make clear that the 10,000 persons applies to those provided with services in the UK. This should also be clarified in the final text.

**Communications data apparatus**

Schedule 2, point 10 of the draft Regulations includes an obligation for providers to "install and maintain any apparatus provided to the operator on behalf of the Secretary of State". This is not included in Schedule 1 and Schedule 3, nor was it included in the 2002 Regulation of Investigatory Powers (Maintenance of Interception Capability) Order**.** ISPA cannot recall this being mentioned during the passing of the Act and is a significant extension of the capabilities. This obligation should be removed and any future policy in this area must be subject to consultation with industry, starting with an operational case and justification for such as inclusion.

**Notification process**

TCNs should seek to minimise as far as possible the impact on an ISP's network and user privacy. We note that the accompanying letter references the need to have regard to the public interest in the integrity and security of systems and that the powers will be subject to strict safeguards and rigorous oversight. To help address this, the draft Regulations should be strengthened in the following ways:

- The draft Regulations should be amended to explicitly include the safeguards mentioned in the text of the letter and the Act itself. Specifically, this should include the addition of the need to meet "the public interest in the integrity and security of telecommunication systems" and "any other aspects of the public interest in the protection of privacy" (Part 1, section 2 of the Act). This should also include a commitment of a full risk assessment by the public authority issuing a notice, which should be a requirement every time a Notice is amended.

- The draft Regulations should be further amended to take account of their impact on similar obligations placed on CSPs in this area. For example, the impact of a TCN may impact on competing obligations under the Communications Act and the EU Framework obligations, such as the requirement to manage risks and protect network availability. When considering issuing a TCN, the relevant authorities should consider these additional obligations as part of its assessment of whether the Notice is necessary and proportionate. Where appropriate, CSPs served a notice should have the ability to report the existence and impact of a TCN to other authorities. Rather than the current situation of having to seek permission each time, an addition of 'deemed permission' should be inserted into the draft regulations to help minimise the impact of the competing obligations placed on CSPs.

**Notification for changes to services and new services**

The draft Regulations include a number of provisions requiring notification to the Secretary of State of changes to services as well as the development of new services (see for example s.13 of Schedule 1 of the draft Regulations). There is no specification of the type of change which requires notification, nor a focus on complying with the specificities of the TCN. We consider that this is very burdensome, and should be removed from the Regulations.

Furthermore, the requirement to "consider the obligations and requirements imposed by any technical capability notice when designing or developing new telecommunications services or telecommunication systems" (see for example s.14 of Schedule 1 of the draft Regulations) is also unduly burdensome and unjustified. Communications providers should be allowed to develop and run their businesses independently, and such provisions would curtail on innovation. In addition, it may go against certain other important policy steers such as ensuring that new communications services are built with "privacy by design". There is a concern that this may not only be stepping beyond the limits of any Notice that is in place; and may also raise concerns around commercial confidentiality of new services in development. We suggest removal of these provisions in all Schedules.

**Equipment Interference Technical Capability Notices**

The draft Regulations include a new obligation for providers to put in place a technical capability to make its network 'hackable', going much further than the previous targeted warrant-based system. This specific power was subject to little debate during the passing of the Bill, and was accompanied by Government claims that "the draft Bill does not provide for new powers for the security and intelligence agencies or law enforcement in respect of equipment interference.[1]" Network security is at the core of a provider's business yet the maintenance of an ongoing technical capability has the potential to undermine security and creates significant vulnerabilities. As was demonstrated recently with the WannaCry hack, vulnerabilities can be exploited by criminals and lead to serious harm. In the interests of to protecting the security and integrity of telecommunications networks, we recommend the removal of Schedule 3 from the draft Regulations.

**Encryption**

The Regulations enforce the removal of electronic protection applied by or on behalf of the telecommunications operator. This was subject to much debate and discussion during the passing of the Bill and remains an area where our members still lack clarity. Such a lack of certainty inevitably

[1] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26435.html

chills incentives for developing and investing in new innovative services. There are still concerns as to how the provisions would work in practice and whether it would be possible for a provider subject to a notice to comply with all circumstances under which electronic protection is applied - for example if it is applied end-to-end by a third party. Encryption gives people confidence and reduces the potential for cybercrime. The industry needs and deserves further clarity around this point.

**Conclusion**

We have made a number of suggested recommendations to the draft Regulations. We ask that an updated version of the draft regulations with changes be published for further consultation across all of industry.