Science and Tech Committee Report into Draft Investigatory Powers Bill - Summary

On Monday 1 February, the Science and Technology Select Committee submitted its report on the draft Investigatory Powers Bill following its inquiry last year. The Committee’s inquiry focused on the technological aspects of the draft Bill and how these measures affect the digital economy.

The Committee agreed with, and cited, techUK on what it felt were the most important aspects of the draft Bill, which included: clear definitions, obligations on Communication Service Provider’s, clarity on encryption and equipment interference and the technical feasibility of Internet Connection Records (ICRs).

A summary of the report can be found below:

**On definitions:** The Committee has agreed with techUK that the current definitions in the draft Bill have led to significant confusion. **Recommendation:** The report specifically states that terms such as “telecommunications service”, “relevant communications data”, “communications content”, “equipment interference”, “technical feasibility” and “reasonably practicable” need to be clarified urgently.

**On ICRs** – the Committee received a lot of evidence concerning the difficulties in defining ICRs and the breadth of the definition in the draft Bill. The report also acknowledges the difficulty in distinguishing between content and metadata when retaining ICRs due to the fact that the web is not a single application and a typical internet user uses a number of different services at any one given time. **Recommendation:** The Government must be more explicit about the obligations it will and will not place on industry in relation to ICRs.

**On Encryption** – the report states that, on the face of it, the technical capability notices and the requirement to “remove electronic protection” do not affect “end to end encryption” as the protection in these instances is applied by the user of the service and not the CSP. It does, however, acknowledge that language in the draft Bill regarding encryption has caused a lot of concern for industry and privacy campaigners. **Recommendation:** Although the report states that “in tightly prescribed circumstances” the security services should be able to seek and obtain un-encrypted data from CSPs, they should only seek such data when it is “clearly feasible”, “reasonably practicable” and “where its provision would be consistent with the right to privacy in UK and EU law”. The report also states that obligations on CSPs in regards to encryption should be clarified in the Codes of Practice and that the Government should clarify and state clearly in the Codes that it will not be seeking unencrypted content when the communications are encrypted end to end.

**On Equipment Interference:** the Committee highlighted the problems with Equipment Interference in relation to the definition of “equipment”, the extent of the provisions, (especially in relation to bulk equipment interference) and the technical difficulties associated with it. The Committee also quoted Antony Walker’s (techUK Deputy CEO) oral evidence regarding the effect of equipment interference on the growing deployment of open source software and accepts that because CSPs cannot reveal that they are subject to equipment interference, their customers might assume that it is being applied. **Recommendation:** The Committee states that it “remains to be seen” whether public avowal of equipment interference affect the nature or extent of it in practice. The report recommends that industry concerns regarding equipment interference are “well founded” and that the Investigatory Powers Commissioner should carefully monitor public reaction to equipment interference powers. The report also recommends that Government refine its approach to equipment interference if industry concerns regarding public confidence are realised.
On cost implications for businesses: the report also highlights the costs associated with certain measures in the draft Bill and the knock-on effects for UK businesses. The report is also sceptical as to whether the figure of £175m for reimbursing the costs associated with storing ICRs were sufficient enough. **Recommendation:** Government must do more to work with industry to improve cost estimates and also reconsider its reluctance to including full cost reimbursement in the Bill.

**On Codes of Practice and compliance:** The report highlights that the issue of compliance with provisions in the draft Bill rely in large part to the as yet unpublished Codes of Practice. Until these are published, the full extent of the Bill will not be understood. **Recommendation:** The Codes of Practice must be published alongside the final Bill. Issues related to compliance burdens, proportionality, cost recovery and the security standards that will have to be applied to keep ICRs safe must be explicitly addressed in the Codes of Practice. The report also states that businesses based in the UK and serving UK customers should not be placed at a commercial disadvantage to their overseas competitors. The regular updating of the Codes of Practice should also be an explicit requirement in the Bill, as should consultation with the Technical Advisory Board (TAB) on keeping the Codes of Practice up to date. The membership of the TAB should also be reviewed.