2015 - Science and Technology Committee Enquiry into draft Investigatory Powers bill

Jisc response to the House of Commons Science and Technology Select Committee inquiry into aspects of the draft Investigatory Powers Bill [1].

Jisc is the UK's expert body for digital technology and digital resources in higher education, further education and research. Since its foundation in the early 1990s, Jisc has played a pivotal role in the adoption of information technology by UK universities and colleges, supporting them to improve learning, teaching, the student experience and institutional efficiency, as well as enabling more powerful research.

In particular Jisc is the operator of Janet, the UK's world-leading National Research and Education Network (NREN), connecting around a thousand universities, colleges and research organisations to each other, to peer NRENs around the world, and to the global Internet. Janet is classed as a private electronic communications service under current telecoms and security legislation.

The following are our views on the questions raised by the enquiry

The technical feasibility and costs of meeting the obligations imposed by the Bill

The feasibility and costs of the draft Bill [2] are impossible to predict. The Bill itself creates few direct obligations. Instead it gives the Secretary of State powers to impose a very wide range of obligations on any or all telecommunications operators. For the first time, duties to retain communications data (clause 71), install and maintain "filtering arrangements" (clause 51) or "technical capabilities" (clause 189) may be imposed on any "telecommunications operator". Whereas previous legislation has limited these duties to public telecommunications services, the draft Bill also allows them to be imposed on any private telecommunications service including networks in businesses and homes (clause 193). The costs arising from the Bill will depend on the extent to which the Secretary of State chooses to exercise these wide powers.

The impact on communications service providers and related businesses

We are particularly concerned at the impact of orders to deploy "technical capabilities" and "filtering arrangements" on telecommunications systems in case targeted interception or data access warrants may be issued in future. The Bill appears to place no statutory limit on what these orders might contain: examples of technical capabilities include preparations to remove electronic protection (clause 189(4)(c)) while the definition of communications data in clause 193(5)(b) appears to imply the provision of direct access to telecommunications systems other than that available to the operator. Such measures will affect all communications using the system, not just those that are the subject of subsequent targeted warrants. Modifying an encryption system to make it easier to decrypt some messages will inevitably make it easier to

decrypt all of them. If such means of access are provided it is inevitable that they will be discovered by people other than their intended users, as backdoor access to Vodaphone systems in Greece and, more recently, TSA master keys to luggage locks have been. Such preparations for future access will therefore reduce the security of all communications that may pass through affected systems.

It appears to us that orders under the draft Bill could go even further. For example it would be technically feasible for an operator to reduce the speed or resilience of their telecommunication system. Such a change of design would no doubt "facilitat[e] the … efficient and effective obtaining of communications data" (c51(1)(b)). An order to do so would therefore appear to be a "filtering arrangement" permitted by clause 51. However such an order would contradict the goals of networks such as Janet to provide the state of the art performance that the UK's research and education sectors require.

The likely consequences for citizen/consumer use of ICT services

Since it will be unlawful for any telecommunications provider to admit that they have been ordered to implement a filtering arrangement or technical facility, it will be difficult for them to convincingly deny that they have. Since orders could be made against any business, no longer just the operators of public networks, trust in the security of all organisations as safe places to hold sensitive data is likely to be damaged. Other countries' ICT industries have already experienced the loss of international business that results from such suspicions. This could be particularly harmful for universities and colleges whose national and international research partners – for example in the high-tech or healthcare sectors – have high expectations that shared data will be kept confidential.

The draft Bill imposes legal prohibitions on disclosing the existence or details of orders of any kind. Jisc is often asked to verify the authenticity of communications data orders under section 22 of the *Regulation of Investigatory Powers Act 2000* and has been given access to Home Office accreditation data to do so. We have also worked with law enforcement and universities to reach a common understanding of particular orders. This has allowed us to advise both universities and law enforcement on the efficient requesting and disclosure of communications data. It appears that under the Bill such discussions will carry the risk of legal sanctions, so the opportunity to develop common good practice is likely to be lost.

Links
[1] http://www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/inquiries/parliament-2015/investigatory-powers-bill-technology-issues-inquiry-launch-15-16/
[2] https://www.gov.uk/government/publications/draft-investigatory-powers-bill