2016 - Investigatory Powers Bill Committee

As submitted to the House of Commons' Bill Committee [1]

Summary

Under current legislation the Government can order public telecommunications service providers to modify their systems and processes to perform data retention and provide "technical facilities" to facilitate Government access to data and content. The Investigatory Powers Bill [2] would extend these powers to all "telecommunications operators" – defined so as to include virtually all Internet-connected organisations and homes in the country. Confidence in the security of electronic systems and data is vital to the UK's social and economic well-being. Jisc is concerned that this expansion of powers may involve a greater risk to that confidence than is necessary.

Evidence

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.

Jisc operates the Janet network, connecting universities, colleges, research organisations and schools to each other and to the Internet. Since Janet and its customers' networks are not available to members of the public they are classed as private networks under the Regulation of Investigatory Powers Act 2000 (RIPA). This means that communications data and interception orders can be made, but not orders to provide data retention or other technical capabilities. The policies for the Janet network require customer organisations to retain logs sufficient to deal effectively with complaints of misuse. To the best of our belief this routine business practice has been sufficient to also provide information required to support criminal investigations; we have seen no evidence that this situation will change in the foreseeable future.

However under clauses 78(1) [3] and 217(1) [4] of the Investigatory Powers Bill, the powers to order data retention and technical capabilities (including filtering arrangements) will no longer be limited to public telecommunications services. Instead these will apply to all "telecommunications operators". This term is defined in clause 223(10) [5] to include anyone with an internet connected router or wireless access point. This is likely to cover most organisations and homes in the country, even though few would consider themselves

"communications service providers". The Bill would nonetheless allow the Home Secretary to order any of them to modify their networks, systems and practices to facilitate future disclosure of communications data or content.

Such modifications will – like previous government-mandated master keys, data stores, and intercept capabilities – become targets for unauthorised, as well as authorised users.

So far as we are aware the Home Office has not given any examples where this extension beyond the RIPA scope would be required. Cafés and other providers of public wifi are already covered by RIPA's (and the Bill's – see clause 223(8) [5]) definition of "public telecommunications service".

Clauses 84(2) [6] and 218(8) [7] will make it unlawful for organisations that have received an order to disclose that fact. If asked 'have you been required to implement data retention or technical measures?' such an organisation cannot admit that its security measures have been changed by Government order.

Given clause 223's broad definition of "telecommunications operator" it seems likely that the majority of organisations within the scope of clauses 78 and 217 will not, in fact, receive an order. However confidence in the security of all these organisations' services, products and information may be undermined because their truthful assertions of non-interference cannot be distinguished from statements by organisations whose responses may be compelled by law.

Information Technology industries in other countries have reported losing business because of suspicions of Government-ordered access mechanisms. If the current Bill becomes law then UK organisations seem likely to fall under the same suspicions. Users, customers and partners may well feel their data are safer in organisations and countries where Government powers are more narrowly defined and more transparently exercised.

This could, in particular, hinder attempts by UK universities and businesses to participate in research collaborations. Work on medical, commercial and other sensitive data involves specific security requirements, with reputational and legal consequences for all partners if any one fails to deliver these. Organisations whose security assurances cannot be relied upon may not be welcome in such collaborations.

Furthermore, these effects on trust in "telecommunications operators" are likely to occur as soon as the Bill passes, irrespective of whether orders are actually made. If the scope of these powers needs to be extended from the "public telecommunications services" to "telecommunications operators" then the impact on confidence might be reduced by regular publication of information about the number of orders made and the sectors to which they have been addressed.

We agree with the Government that public confidence in data security is vital for the UK to achieve the economic and social benefits of techniques such as big data. We are therefore concerned that applying the Bill’s full powers to its wide definition of "telecommunications operator" may involve a greater risk to that confidence than is necessary.

Links
[1] http://services.parliament.uk/bills/2015-16/investigatorypowers/documents.html

[2] http://www.publications.parliament.uk/pa/bills/cbill/2015-2016/0143/cbill_2015-20160143_en_1.htm
[3] http://www.publications.parliament.uk/pa/bills/cbill/2015-2016/0143/cbill_2015-20160143_en_8.htm#pt4-pb1-l1g78
[4] http://www.publications.parliament.uk/pa/bills/cbill/2015-2016/0143/cbill_2015-20160143_en_18.htm#pt9-ch1-pb3-l1g217
[5] http://www.publications.parliament.uk/pa/bills/cbill/2015-2016/0143/cbill_2015-20160143_en_19.htm#pt9-ch2-pb2-l1g223
[6] http://www.publications.parliament.uk/pa/bills/cbill/2015-2016/0143/cbill_2015-20160143_en_8.htm#pt4-pb4-l1g84
[7] http://www.publications.parliament.uk/pa/bills/cbill/2015-2016/0143/cbill_2015-20160143_en_18.htm#pt9-ch1-pb3-l1g218