Universities and Colleges Information Systems Association

University of Oxford
13 Banbury Road
Oxford OX2 6NN

Tel: +44 (0)1865 283425
Fax: +44 (0)1865 283426
Email: admin@ucisa.ac.uk

www.ucisa.ac.uk

UCISA submission to the House of Commons Science and Technology Select Committee inquiry into aspects of the draft Investigatory Powers Bill

1. UCISA, the Universities and Colleges Information Systems Association, is a membership organisation representing those responsible for delivering information management systems and technology services in universities, colleges and other institutions. UCISA membership is institutional and the Association enjoys almost 100% coverage within the higher education sector and has a number of further education members.
2. UCISA's members, universities and colleges in the UK, provide a wide range of IT facilities to staff and students, including access to the wider internet through Janet, the UK's National Research and Education Network (NREN). Both the higher and further education sectors benefit from using Janet's connectivity to utilise shared and cloud services as part of institutions' ongoing drive to improve efficiency. In addition, international research collaboration is facilitated through Janet's connections to other NRENs.
3. Use of IT facilities within universities and colleges are governed by institutional regulations; many have derived their regulations from UCISA's *Model regulations for the use of institutional IT facilities and systems* (www.ucisa.ac.uk/modelregs). The Model Regulations set out the expectations of users of institutional facilities (i.e. staff and students) and also notes that the institution will log use of its systems and will comply with lawful requests for information from law enforcement and government agencies for the purposes of detecting, investigating or preventing crime, and ensuring national security.
4. The following are our views on the questions raised by the inquiry.

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

5. We note that the draft Bill gives the Secretary of State powers to impose a very wide range of obligations on any or *all* telecommunications operators. Previous legislation has limited the applicability of these obligations to public telecommunications services. However clause 193 allows them to be imposed on private telecommunications services including networks in businesses and homes. This brings the networks operated by our members in their institutions into scope and so duties to retain communications data (clause 71), install and maintain 'filtering arrangements' (clause 51) or 'technical capabilities' (clause 189) may be imposed on university and college networks. It is impossible to predict the feasibility and costs of meeting these obligations as it depends on the extent to which the Secretary of State chooses to exercise these wide powers.

6. We note that the Guide to Powers and Safeguards makes reference to CSPs (Communications Services Providers) throughout. This term has, in previous legislation, only been applied to public telecommunications services. This seems to be in contradiction with the scope defined in clause 193 which implies that the scope of the Bill (particularly the obligations outlined above) are also applicable to private networks.

The impact on communications service providers and related businesses

7. As noted above, the impact on UK universities and colleges depends on the extent to which the Secretary of State chooses to exercise the powers outlined within the Bill. We would note that universities and colleges already have established procedures for managing requests from law enforcement and government agencies. The existence of such procedures is noted in the acceptable use policies/regulations for use of IT facilities in each institution.
8. A number of universities have overseas campuses which will host similar IT services and facilities to the home institution. The extent to which the home institution 'controls' the network in a remote campus varies but clause 193 (10) (b) (ii) implies that those that are 'controlled' by a UK institution will be within scope. It is not clear what constitutes 'control' in this instance and so it is difficult to assess the impact implementation of the Bill may have on such institutions.

The likely consequences for citizen/consumer use of ICT services

9. We note that there does not appear to be any statutory limit on the scale or scope of any orders to deploy 'filtering arrangements' and 'technical capabilities' on telecommunications systems in case targeted interception or data access warrants might be issued in the future. Since such measures will have to be applied across the whole of the telecommunications systems an operator is responsible for (as the 'just in case' nature of the order cannot be targeted), they will affect all communications and hence all users.
10. It will be difficult, under the terms of the draft Bill, for universities and colleges to confirm that they are not subject to an order, as the Bill makes it unlawful for any telecommunications provider to confirm that they are. There is a high degree of trust between institutions collaborating on research (whether it is within the UK or international) that shared data will be kept confidential. We are concerned that the trust in UK institutions as safe places to hold sensitive data may be damaged by the inability of institutions (as telecommunications providers) to convince their partners that they have not been ordered to implement filtering arrangements or other technical facilities. We believe that this may be harmful to UK institutions looking to carry out collaborative research with overseas institutions.

Peter Tinson
Executive Director
UCISA

26 November 2015