2010 - Home Office consultation on the Regulation of Investigatory Powers Act

This is JANET(UK)'s response to the Home Office consultation on Amendments to the *Regulation of Investigatory Powers Act 2000* [1]. JANET(UK) is the operator of the JANET network, which connects universities, colleges, research organisations and schools networks to each other, to education networks elsewhere in the world, and to the public Internet. As an operator of a large national network we are concerned that amendments to the Act should not unintentionally penalise activities necessary to operate such a network, nor unnecessarily limit the future development of network services.

1. Are you content with the way in which we propose to change section 3(1) of RIPA to make clear that interception will be lawful only where both parties to the communication give specific consent to the interception? What impact would this have on Communication Service Providers?

We regret that no draft has been provided of the amended text of this section, so it is not possible to comment on whether the amended text will be satisfactory. Although JANET does not currently make use of the "dual consent" permission to intercept that is provided by section 3(1), we are concerned that changes may make the section impossible to satisfy and therefore rule out future service developments that might depend on it.

For example, the current Act might permit the development of personalised services where the user positively consented to their service provider recording the websites they visit, in order to improve the relevance of suggestions or provide other benefits (an equivalent bargain to a supermarket storecard). However if the text is amended to require that both the sender and receiver of a communication have actually given their consent (rather than the current requirement that the service provider have "reasonable grounds" for believing that they have done so) then such a service would immediately become unlawful when a user who has consented passes the computer keyboard to one who has not. Given the significant penalties that we agree should be available for unlawful interception, it seems unlikely that anyone would take the risk of developing such a service.

2. Given that the Government accepts that it needs to make legislative changes to address the deficiencies identified by the Commission, do you agree with the recommended option?

As with the proposed changes to section 3(1), we very much regret that a draft amended text has not been provided. We are therefore unclear in what circumstances an "unintentional unlawful interception" might take place.

Section 1 of the current Act [2] states that "It shall be an offence for a person intentionally and without lawful authority to intercept..." and Section 2 of the Act clarifies that "a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if, he— (a)so modifies or interferes with the system, or its operation, (b)so

monitors transmissions made by means of the system, or (c)so monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system, as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication". Under this current text the offence appears to require both that the modification or monitoring must be intentional and that the person doing it must intend that their action will make the contents of the communication available. We presume that the act of "unintentional interception" will retain the same definition of interception, however it is not clear which of the two "intentions" of the current offence will be removed, or whether mistake in either of them will be sufficient.

All of these options appear likely to capture legitimate actions for which the imposition of even a civil penalty appears either inappropriate or disproportionate. For example turning on a wifi enabled laptop will result in many communications being made available to the owner, including those for other users in the same area, since wifi is a broadcast technology and not all networks are yet encrypted. Even a software bug can produce an "unintended interception", for example it has been reported [3] that one release of iPad software continues to use an IP address after its temporary allocation period has ended: this is likely to result in the iPad receiving communications intended for the next user of the same address: an unlawful interception, but by a blameless user.
The consultation paper states that a mistake in implementing an interception warrant under section 5 will not constitute an unintentional unauthorised interception. We believe the same protection needs to be given to mistakes in other authorised interceptions, for example those required for the operation of a telecommunications service that are currently lawful under section 3(3), otherwise an impossibly high standard of practice will be required.

Without much greater clarity on how the new offence will be defined and interpreted, therefore, we are unable to support the Government's proposal.

3. Are there any other options that the Government should consider or are there any changes that should be made to the recommended options?

As above, we do not feel the consultation paper gives sufficient detail of the proposed changes to say whether or not there may be better options.

4. Do you think the First-tier Tribunal (General Regulatory Chamber) is the appropriate appellate body to determine the appeals? If not, where do you think the appeals should be directed and why.

We have no view on the appeals body, however we consider that the Information Commissioner, rather than the Interception of Communications Commissioner (IoCC), should be considered the primary authority in these areas. Given the apparently wide scope of "unintentional interception", we would expect that most cases will be privacy breaches resulting from inadequate technical or procedural controls to protect digital information, not the interception and data access powers of public authorities that are the IoCC's current area of expertise under section 57 of the Act. The Information Commissioner is already being given powers to deal with breaches of personal data privacy in the implementation of the revised Telecommunications Directives: unintended interceptions seem to fit naturally within these powers and expertise.

5. What if any additional costs would these proposed changes impose on Communication Service Providers or others?

Whether costs are incurred by network operators of all kinds will depend on the extent of the new provisions so is impossible to predict given the current absence of detail. As well as direct costs, we see a significant risk of loss of opportunity to both service providers and their customers if the changes prevent the development of new, privacy-respecting, services.

Links
[1] http://www.homeoffice.gov.uk/publications/consultations/ripa-effect-lawful-intercep/ripa-amend-effect-lawful-incep
[2] http://www.legislation.gov.uk/ukpga/2000/23/contents
[3] http://www.net.princeton.edu/announcements/ipad-iphoneos32-stops-renewing-lease-keeps-using-IP-address.html