EURIM Consultation Response

Working Group on RIPA Implementation

August 2001

Response to Consultation on Section 12 Order

NOTE that this response was prepared by a working group and does not carry the status of being an agreed EURIM position as it has not yet been circulated for political approval.

General

In its current form this draft Order does little to expand on the inadequate level of information provided in the Act. EURIM accepts that the Order cannot contain all appropriate detail. For example, the role of the Technical Advisory Board is not mentioned. Much of the detail is provided in italics that will not be part of the formal Order. There is also no mention of how the contents of a specific Notice will be updated as the technology, products and services of the CSP change.

Given the advantages to industry of transparency in the process by which a Section 12 Notice is negotiated with a CSP, and the need to include in this Order only that information required by the RIP Act, we strongly recommend that the Order be accompanied by Explanatory Notes. The supporting information contained in italics in the Order could also be included in these Notes. We have identified in these comments some areas where such Notes would be of benefit.

EURIM notes with concern that all reference to how costs will be reimbursed has been removed. Such information is needed particularly by non-UK based organisations considering investment in the UK – who will expect to be able to assess the cost impact of such a move where they consider their business meets the definition of a CSP, and thus is potentially subject to a Section 12 Notice.

Specific Comments

Exception
While the explicit exception of services provided solely to the financial markets is welcomed, clarification is needed as to how this will be defined – as many such services increasingly include ancillary services (e.g. email, access to selected web sites or portals) to maintain a competitive advantage. We would welcome the opportunity to work with the government to agree the scope of such services.

Fundamental Principle for Public Telecommunications Services
This new section is to be welcomed as a means of bounding the requirement that could be placed on a CSP. However, standards, by their nature, change, and other standards bodies (such as the IETF for many protocols) produce relevant information. A formal list, under change control and publicly available, should be established where all such document references are held. Rather than mentioning specific standards bodies in the Order, we recommend that the TAB be made explicitly responsible for this list – which it will probably need anyway to carry out its designated tasks.

General Requirements
The paragraphs in this section refer more than once to “warranted person” – for example paragraphs 8b and 8i. The CSP can only intercept traffic related to specific telecommunications identifiers. Rarely can they can relate that identifier to the identity of the person actually using it any particular time. Given that the RIP Act unfortunately refers to “persons”, we recommend that it be made clear in the Explanatory Notes that in practice “telecommunications identifiers” will be used to identify targets.

Activation timescale (8a)
Explanatory Notes could explain that this would effectively be within one working day of *verification* of authenticity of a warrant (to reduce the chance of a CSP acting on a forged warrant). It could also make clear that all such warrants are executed through ISLU, further underwriting such authenticity.

Handling of Intercepted Data (8b) and Agreed Formats (8e)
The requirement to provide intercept in near real-time is closely linked with the requirement in paragraph *8e* to comply with hand-over standards “where they exist”. The responsibilities of the CSP

should be limited to handing off the intercepted data to an agreed point – it is likely that the CSP will have no direct control over the actual transmission mechanisms, and cannot be held responsible if they fail. We also note an inconsistency between 8(b) and 8(c). The former requires handover to "government/the intercepting agencies", while the latter seeks "delivery to a hand-over point"

On the interface standards, it is not clear what will happen where no such standards exist. Will they be government-mandated, possibly locking UK CSPs into the support of obsolete or proprietary formats to their commercial disadvantage. Where will the list of agreed standards be maintained – with the Technical Advisory Board?

Such issues could be covered in accompanying Explanatory Notes.

Traffic Data (8c)
The definition of communications data here is an improvement on that in the earlier draft. This statement also highlights the need for a formal change mechanism to allow changes to agreed definitions as services and the way they are offered by the CSP change (which they will do far more frequently than was historically the case for telcos).

Filtering Data Streams (8d)
The ability to filter out the telecommunications of a specific telecommunications identifier can have major technical and cost implications. It is not clear on what basis feasibility will be evaluated. This could be included in statements on costs (see later).

Interception rates (8g)
The value of 1 in 10,000 end users looks very high – depending on how "end user" is defined (e.g. registered user, connected user, registered mailboxes, registered accounts). We support the suggestion that the requirement would be better defined as the rate per number of "active communications channels" or "simultaneously active sessions".

Auditability (8i)
The statement that such information is not to be to evidential standards could be included in supporting Explanatory Notes.

Security (8j)
Again, this should be phrased in terms that allow a CSP to judge whether its standard systems need enhancement to meet the requirement. In particular, will the CSP be expected to conform to the Manual of Protective Security? There is also major concern over the numbers of people who may need formal vetting. Given the way CSP services are developed and managed. There will inevitably be significant numbers of people who will become aware of the existence of an interception capability even if they are not aware of specific interception targets. CSPs may not be prepared to remove such staff if they "fail" such a security vet. Such issues could be covered in supporting Explanatory Notes.

Costs

The lack of any information on how costs are to be reimbursed is a major issue. We understand that discussions are ongoing with specific CSPs to discuss the basis for cost reimbursement, but this does not help those contemplating investing in future CSP services. EURIM seeks transparency of the formulae that will be used for deciding what costs reimbursement levels might be. It is accepted that the detail should not be in the Order itself, but a commitment that the cost formulae used as the basis for individual negotiations with CSPs will be made public is essential.

Given that CSP services and infrastructure are continually evolving, there will also be a need for the interception capability to be upgraded from time to time. The cost formulae should include provision for such a maintenance capability.

Summary

Overall, this Draft still provides little useful information beyond that contained in the Act. For a CSP to be able to judge the potential investment demand resulting from the Order, far more precise information is needed. While we accept that this detail should not be included in the Order itself, the government should commit to such information being made available – for example in supporting Explanatory Notes. In particular, this EURIM Group seeks commitment to the availability of the formulae used as the basis for cost reimbursement negotiations and to the maintenance by the TAB of standards, and related bodies, that define the scope of interception requirements.

There are also a number of wording changes that need to be made to ensure the Order does not impose unreasonable demands on CSPs.