

Regulation of Investigatory Powers Act Code of Practice for Part 1 Chapter 1

EURIM members have responded individually to the Code of Practice for Part I Chapter 1 of the RIP Act in some detail. This response highlights major issues that need to be addressed if this Code of Practice is to reassure industry that the Act will be applied fairly and reasonably. Failure to provide this level of guidance will inevitably revive concerns on the effect of the provisions of the Act on investment in e-commerce in the UK.

It may be that some of the issues raised below are to be covered in other documents. If this is the case, a list of those documents should be included in this Code of Practice, with references to them in the body of the text where appropriate. Informal discussion suggested that a framework document explaining the scope of the Codes of Practice and supporting documents would be useful both to those raising warrants/notices and to industry. In the absence of any such document, we expect all relevant information to be contained within the Codes of Practice.

General Comments and Issues

1. Overall, this Code of Practice seems to concentrate on the various warrant processes, while giving only cursory guidance on other, no less important processes associated with creating and maintaining an effective intercept capability. It seems that this Code of Practice has yet to reflect the very different environment in which there are many communications service providers who could become involved in interception requests.
2. The omission of any discussion of the process of establishing an intercept capability, and of any reference to the Technical Advisory Board is surprising. Section 3.15 does not even recommend that discussion take place with a service provider before any Notice is served under Section 12(2), nor does it mention the role of the Technical Advisory Board or what happens if the service provider decides the requirements of the Notice are unreasonable. The form of Notices described in Section 3.16 contains no means of independent verification. The Code of Practice seems to assume that interception capability will be provided on demand without prior discussion. There are also major issues relating to the obligation to maintain an interception capability once installed. The responsibility for, and who pays the cost of, installation, upgrade on changes to infrastructure, error reporting, commitment to test the capability still works, etc, all need to be spelt out.
3. Section 3.13 talks about requiring a service provider being asked only to take reasonable steps, but provides no guidance on what steps should be taken if there is a dispute as to whether the request is reasonable. We would expect at least a

requirement to refer the matter to the Technical Advisory Board. Further, other than as footnotes in Section 4, there is no reference anywhere to the need to agree with the service provider what is reasonably achievable.

It is strongly recommended that the Code of Practice contain much more information about how an intercepting agency can and should help an innocent CSP to comply to the best of their ability with a warrant or notice.

4. There is no discussion of the basis upon which costs are to be agreed and of the set-up and ongoing costs that the service provider should bear. This was debated at length during the progress of the Bill, and the lack of any positive statements in this Code of Practice is disappointing.
5. There are still major concerns over the method of authentication of warrants/notices. Where the form of warrant/notice proposed in the Code of Practice contains verification details, these are not proof against spoofing or forgery. For example, a contact telephone number on the warrant itself is not effective - there is no guarantee that it has not just been provided by the presenter of the warrant. Industry is already experiencing attempts to use similar processes to gain illegal access to privileged information (including personal data). Some uniform means of independent verification of the validity of all warrants/notices is required. The Code should grant a reasonable time in which to do this and provide for the case where the operator is not able to complete the verification for reasons beyond his control.
6. Where a warrant or notice is served under a mutual assistance agreement, all contact with the UK-based CSP must be through a UK based authority which accepts full responsibility and liability for ensuring that the access requested conforms with the legal requirements of the Nation requesting the assistance. No CSP should be asked directly by a non-UK organisation to provide information.

Chris Sundt
Chairman, EURIM Secure E-commerce Working Group
10 November 2000