

The Section 12 Order

1. The Regulation of Investigatory Powers Act 2000 (RIPA) states that the section 12 order will define the reasonable interception capability a Communication Service Provider (CSP) will maintain **should they be served with a section 12 notice**. The notice will specify the services for which an interception capability is required and the steps and time-scale for meeting this requirement. The notice will be discussed with the CSP before it is issued and a plan of how the interceptions will be effected agreed.

2. The following paragraphs 3-4 relate to the contents of the section 12 order. The text in italics provide further explanation and clarification. Paragraph 5 deals with the contribution the government/intercepting agencies will make to the costs of the capability.

Requirement for Telecommunication CSPs

3. The capability must provide the following :

a. The implementation of interceptions within a reasonable time-scale.

b. The interception of the entire communication and the associated data going from or intended for a warranted person, and transmission to government/the intercepting agencies in near real time.

For stream-based services the stream shall be copied and forwarded as it happens. The emails of the warranted person will be forwarded as soon as they are available within the CSP infrastructure.

This requirement only applies if the warranted person can be associated with a specific telecommunications identifier.

Specific telecommunication identifiers include telephone numbers, email and IP addresses and log-on details.

This requirement does not include communications transmitted across a backbone.

c. The delivery to a hand-over point of the intercepted communication and its associated data so that the information can be unambiguously correlated.

Communication associated data may include:

- *Details of the cell site location for mobile telephones*
- *Caller line identification*
- *Signaling of access ready status*
- *The telecommunications address being contacted even if contact is not established.*
- *All signals emitted by the warranted person, including post-connection dialed signals.*
- *Beginning, end and duration of the connection.*

- *Actual destination and intermediate telecommunication addresses should a communication be diverted.*
 - *Information about the geographic location of the warranted person.*
- d. Filtering to identify the telecommunications of a particular warranted person if feasible, and transferal to government/intercepting agencies in an agreed format.
- e. Removal of any electronic protection applied by the CSP rather than anyone else.
- f. Simultaneous interception for at most 1 in 10,000 of the end users (if the CSP has fewer than 10,000 end users it will maintain an interception capability for one).
- g. A reliability at least equal to the service they offer to their customers.
- h. Audibility so that it is possible to confirm that the intercepted signals are those associated with a warranted person.

This may be required to demonstrate the correct operation of the interception and to prevent unauthorised interception of communications.

- i. Sufficient security so that the chance of a warranted person or other unauthorised persons becoming aware of any interception is minimised.

When the Government judges the security of an interception system it will adopt a risk management approach which takes into account the threat and technological limitations.

Requirement for Mail Communication Service Providers

4. If served with a notice a mail carrier will be required to have a capability to:
- a. Intercept and temporarily retain communications destined for addresses in the UK for provision to the interception agency.
 - b. Intercept and retain items sent by identified persons should they, in the course of their normal business, keep records of who sent which item.
 - c. To operate a system of clandestine opening, copying and resealing of any letters carried for less than £1.
 - d. Operate a-c in such a manner that the chance of the warranted person or other unauthorised persons becoming aware of the interception and interference is minimised

Costs

- 5 Government/intercepting agencies will pay the entire costs for the maintenance of an interception capability for small CSPs. In the case of larger

companies government/intercepting agencies will make a contribution depending on the resources of the company and the technology involved.