



Office of Hon Amy Adams

Member of Parliament for Selwyn

Minister for the Environment

Minister for Communications and Information Technology

Associate Minister for Canterbury Earthquake Recovery

24 SEP 2013

Don Christie
Director
Catalyst IT
PO Box 11053
Manners Street
WELLINGTON 6142

Dear Don

Thank you for your letter of 19 September 2013. In that letter you have raised concerns with the Telecommunications (Interception Capability and Security) Bill (the Bill), and specifically with the application of “network operator”, and the interception capability and network security requirements that apply to “network operators”.

The Bill is separated into two distinct parts – interception capability requirements (Part 2 of the Bill) and network security requirements (Part 3 of the Bill).

Interception capability requirements

As you are aware, the interception capability requirements amend and replace current requirements in the Telecommunications (Interception Capability) Act 2004 (the Act). That Act, which has been in operation for nine years, imposes a blanket interception capability obligation on all “network operators”.

Two points are worth noting. First, the definition of “network operator” (and therefore the companies that are caught by it) is unchanged in the Bill. The focus of the definition is on those companies who own, control or operate a public telecommunications network or, for example, those providing wholesale telecommunications services. Therefore, if your company does not have obligations attaching to network operators under the current Act, you equally will not have such obligations under the Bill. The Bill does not extend the reach of who is caught by “network operator”.

Second, for companies that are considered “network operators” (which I note captures different kinds of companies from those who count as “service providers” under both the Act and the Bill), the Bill reduces the nature of obligations that might apply to network operators. While the current Act requires all network operators to have complete interception capability, which is equivalent to the requirements in clause 10 of the Bill, the Bill additionally provides for reduced obligations to network operators with fewer than 4,000 customers, and network operators selling wholesale and infrastructure services.

The duty that you discuss (interception ready) represents a much reduced obligation from that which network operators of equivalent size would be required to comply with under the current Act. This will bring significant savings for small network operators.

You also raise a concern about the regulation making power in clause 110. The current Act provides that regulations may be made for “matters contemplated by this Act, necessary for its administration, or necessary for giving it full effect”. I note that no regulations have been issued to date. If regulations were ever issued, they could not provide for matters not anticipated by the scope of the Act.

Network security requirements

The network security requirements in the Bill apply only to “network operators”. The purpose of the requirements, as set out in clause 7, is to address security risks arising from the design, build and operation of “public telecommunications networks” (a term defined in the Bill), or interconnections with other networks. The Bill does not require companies to monitor their customers’ data on their networks to determine whether that data poses a threat to New Zealand’s national security or economic well-being. Further, the Bill does not give the Government Communications Security Bureau the power of veto, or the mandate to become involved in every business decision.

You have raised a concern about the operation of clause 46, and specifically in relation to the requirement for network operators to notify the government about changes to “any place in a network where data aggregates in large volumes”. I would draw your attention to changes made during the Select Committee process, and the clarifications that it:

- relates to a “public telecommunications network”, and
- that it is where data “belonging to a customer or end-user” aggregates in large volumes.

I also note that there is ability for the Director of GCSB to exempt network operators from notifying matters that will not give rise to a network security risk.

Finally, you raise concerns both about the consultation process, and about potential impacts to privacy. In relation to consultation, I note that a copy of the Bill was made public some four and a half months ago, and that it has been through a Select Committee process where everybody has had the chance to publicly submit.

As to concerns about privacy, I note that the current Act contains privacy protections for interception capability obligations, which remain unchanged in the Bill. Further, more secure networks from a national security perspective will have a positive effect on the privacy of individual and business information and communications.

Yours sincerely



Hon Amy Adams
Minister for Communications and Information Technology