



18 October 2016

Mr. Mark Fitt  
Committee Secretary  
Senate Economics References Committee  
PO Box 6100, Parliament House  
Canberra ACT 2600

**By email:** economics.sen@aph.gov.au

Dear Mr. Fitt

### **NEXTGEN'S RESPONSE TO SENATE INQUIRY INTO 2016 CENSUS**

Thank you for your letter dated 14 October 2016 relating to the Senate inquiry into the 2016 Census, and giving Nextgen Networks Pty Ltd (**Nextgen**) the opportunity to respond to IBM Australia Limited (**IBM**)'s submission to the inquiry (**Submission**).

Nextgen is a leading provider of telecommunications networks in Australia and is a licensed carrier under the *Telecommunications Act 1997* (Cth). As certain matters raised in IBM's Submission refer to Vocus Communications Limited (**Vocus**), we wish to note that the shareholders of Nextgen Group Holdings Pty Limited (**Nextgen Group**) accepted an offer from Vocus on 29 June 2016 to acquire a number of Nextgen Group companies, including Nextgen Networks Pty Limited. The proposed acquisition is yet to complete, subject to customary completion completions (ACCC approval having been granted).

We would like to respond to several comments in the Submission, in particular to paragraphs 12, 13, 14, 16, 66, 67, 73, 75, 76, 77, 78, 82, 83, 86, 95 and 96. Instead of responding to and addressing these paragraphs one-by-one, below is our response in relation to Nextgen's role and participation in the matter (subject to Parliamentary Privilege). We also note that in keeping with IBM's submission, we have kept our response at a high level, and not responded with detailed technical arguments about the solution developed by IBM.

1. **Nextgen's offer of DDoS protection rejected:** In accordance with IBM's order, Nextgen supplied IBM with a standard internet service, and met all of its service levels on that product. Although Nextgen strongly recommended to IBM to take up an internet DDoS (Distributed-Denial-of-Service) protection option for the purposes of the 2016 census, it was declined by IBM (see **Annexure 1** – Nextgen's commercial proposal to IBM dated 12 January 2015, and email confirmation of rejection of Nextgen's DDoS protection dated 24 May 2016). This additional feature offered by Nextgen is designed to effectively detect and defend against DDoS attacks.
2. **Nextgen implemented IBM's "Island Australia" strategy – which is tested by IBM:** Although Nextgen provided IBM with its commercial proposal on 12 January 2015, it was not privy to the IBM "Island Australia" strategy until 20 July 2016, just 6 days before the eCensus site went live on 26 July 2016. Nextgen provided all possible assistance to IBM



(which is well beyond what is provided for a standard internet service) to put in place "Island Australia". Nextgen complied with the IBM "Island Australia" framework requirements provided by IBM, which was activated for testing on 5 August 2016 by IBM. IBM advised Nextgen that the test results were successful and positive. IBM's intention was to activate IBM's "Island Australia" only when there was a DDoS attack and would accordingly instruct Nextgen to do so when needed. Below are further details of the "Island Australia" framework requested by IBM:

- a. IBM had earlier in June 2016 requested Nextgen to provide a specific IP address range (due to a requirement to advertise the IP addresses to both Nextgen and Telstra), without providing any context to Nextgen regarding IBM's "Island Australia". After becoming aware of "Island Australia", Nextgen advised IBM that the IP address range requested by IBM was part of a larger aggregate network, and therefore it was not possible to provide specific international routing restrictions for this range. Nextgen recommended using an alternative IP address range, which would give IBM better control, but this was rejected by IBM.
  - b. IBM requested Nextgen to apply IP address blocking filters by Nextgen's upstream suppliers, and international remote black holes for 20 specific individual host routes, which Nextgen complied with. Nextgen believes that the individual host routes picked by IBM may not be exhaustive, and DDoS attacks could come from other routes in the IP address range (which they did in the 3<sup>rd</sup> DDoS attack on Census Day).
  - c. **Testing of "Island Australia" by IBM prior to Census Day:** IBM instructed Nextgen to activate "Island Australia" for testing by IBM on 5 August 2016 at 6am, and IBM advised Nextgen that the testing was successful soon after. The same configuration used on 5 August 2016 was to be used if IBM was ever to instruct Nextgen to activate "Island Australia". Nextgen cannot comment on the testing conducted by IBM as it was not involved with it.
3. **Census Day DDoS attacks:** On 9 August 2016 (**Census Day**), the eCensus system experienced its first DDoS attack at approximately 10.10am and Nextgen alerted IBM to it. The attack subsided by itself at 10.20am. At approximately 11.45am it experienced its second DDoS attack, and IBM instructed Nextgen to activate IBM "Island Australia", which was put in place within 2 minutes (using the same pre-configuration that had undergone testing on 5 August 2016), and the eCensus site returned to normal by 11.49am. At all times Nextgen was in contact with IBM, and IBM's "Island Australia" remained in place after the second DDoS attack. At approximately 4.52pm a third DDoS attack occurred which did not impact the eCensus availability. At approximately 7.27pm, there was a fourth DDoS attack, which resulted in the eCensus site being unresponsive and unavailable.

Nextgen can show that the fourth attack affected both links (see **Annexure 2** – using traceroutes provided by IBM. There were a number of routes without geoblocking during the fourth DDoS attack, and which were not identified during testing, along with the Singapore link mentioned in paragraph 95 of IBM's Submission).

IBM's router facing the Nextgen link was rebooted soon after the attack and IBM kept the Nextgen IBM link down until it was comfortable there was no data breach. After the fourth DDoS attack, Nextgen offered to implement the DDoS protection option, mentioned in



item 1 above on the internet service it provides to IBM, which it did when it received instruction from IBM to do so on 13 August 2016. This was provided at Nextgen's cost and continued to provide full support to IBM on the service.



**Annexure 1: Nextgen's commercial proposal to IBM and IBM's rejection of Nextgen's DDoS protection option**

[Redacted as commercial in confidence]



**Annexure 2: Traceroutes**

[Redacted as contains names of employees and security information]