1 November, 2016

Mr David Monk
Inquiry Secretary
Joint Standing Committee on Electoral Matters
Parliament House
Canberra ACT 2600

RE: Authorisation of voter communication

Dear David,

We are writing to you in response to your enquiry (your email dated 26 October, 2016) regarding the authorisation of voter communication in text messages, phone calls and other forms of communications that may be facilitated by means of telecommunications.

In your email, you raise the question as to whether carriers/carriage services providers (C/CSPs) are or could be made responsible for ensuring that electoral content carried over telecommunications networks is appropriately authorised or whether they might have an obligation to assist authorities if communications are non-compliant. Our industry members have provided input to the following responses on the matters you have raised.

Legal assistance:

Industry fully recognises its obligations to assist national security and law enforcement agencies in accordance with Section 313 of the *Telecommunications Act 1997*. With regards to the issue at hand, Industry operates under the expectation that, upon receipt of a lawful request from a duly authorised officer within an organisation that has the legislated right to request customer information, it will make available the information of the service from which the message originates.

However, any proposal that our industry more broadly could or ought to 'police' the traffic that it carries over its networks raises fundamental concerns, including:

- a citizen's rights to communicate without surveillance by the State or other entities and the low likelihood that any legislative framework could be established to enable surveillance of customer communications;
- technical difficulties of mass surveillance of communications;
- high costs and regulatory burden which would have to apply to all forms of legacy and internet based communications, including social media; and
- relative ineffectiveness of such measures given the immediacy of the communication.

Authorisation of electoral content carried over telecommunications networks:

The issue raised goes to the role of C/CSPs in relation to the content of communications being carried by their networks/services. As distinct from print, television and radio broadcasters, C/CSPs do not exert any 'editorial' or 'programming' control over the content of communications carried by their networks/services. C/CSPs do not, in the ordinary course of

business, pre-approve, authorise or have any similar role in relation to third-party content carried by their networks/services, unlike print, TV or radio broadcasters who broadcast advertisements or community service announcements at the request of communicating parties and determine their content programming schedule.

It should also be noted that the real-time or near real-time nature of the communications under consideration means that non-compliance with any authorisation of voter communications legislation could often only be detected after the communication has taken place. This real-time nature constitutes a further difference to the TV or radio broadcasting of electoral matters which allows for inspection of the message to be broadcast for compliance with the legislation prior to the actual broadcast.

In general, it is always the responsibility of a communicating party to ensure that its communications comply with any applicable laws when carried over a telecommunications network/service. There is a range of laws already applying to various communications carried over telecommunications networks/services. These include, for example, the *Telemarketing and Research Industry Standard 2007*; the *Do Not Call Register Act 2006*, the *Australian Consumer Law (Competition and Consumer Act 2010)*; the *Spam Act 2003* or the *Commonwealth Electoral Act 1918*. However, irrespective of C/CSPs facilitating carriage or similar of the communications, it remains the responsibility of the communicating party to ensure its communications meet these obligations.

Consequently, the communicating party ought to bear the sole responsibility to ensure that its communications meet any legislative obligations, including any applicable voter authorisation or other electoral advertising requirements.

Protection of information:

The fundamentally different nature of communications over telecommunications networks/services (as compared with print, TV and radio communications) is demonstrated by the protections that C/CSPs are required to apply to these communications.

Under Section 13 of the *Telecommunications Act 1997*, C/CSPs are not allowed to disclose "the contents or substance of a communication that has been carried by a carrier or carriage service provider" (Section 13, 276(1)). Such disclosure is only authorised under a warrant or if authorised or required by law.

The content of a communications is also not required to be inspected or collected. The only requirement on C/CSPs is to retain customer and usage related data (commonly called metadata) under part 5-1A of the *Telecommunications (Interception and Access) Act 1979* (i.e. the data retention regime) which specifically excludes the content of a communication. The content of communications may only be copied if an interception warrant or a stored communications warrant is in place.

C/CSPs retain text messages for a short period for operational purposes, with individual text messages only being accessed by C/CSPs for the purpose of dealing with customer problem reports. The content of messages is not inspected. An inspection of the content of text messages would be highly impracticable, technically extremely difficult and costly, and impact on the delivery of the message. Furthermore, there is no legal basis for doing so. Broad community input would be required to determine whether such action was ethically or morally desirable.

A similar argument can be made for phone conversations. CSPs are only allowed to intercept phone conversations in accordance with the strict provisions of the *Telecommunications (Interception and Access) Act 1979*, i.e. under a warrant. Moreover, such interceptions are

specifically targeted and the content of communications is delivered to the requesting Agency for recording and analysis. C/CSPs do not have these capabilities and, given the daily volumes of communications, mass monitoring is impractical.

We are happy to assist the Committee further in this matter. Unfortunately, we both have other commitments in Melbourne on the afternoon of 11 November, 2016 but would be able to appear before the Committee via audio-conference. Please provide us with details closer to the date.

Yours sincerely,

John Stanton
Chief Executive Officer
Communications Alliance

Chris Althaus
Chief Executive Officer
Australian Mobile Telecommunications Association