26 February 2020

Productivity Commission
4 National Circuit
Barton ACT 2600

By online submission

Dear Commissioners,

RE: Inquiry into the Right to Repair

Communications Alliance is the primary telecommunications industry body in Australia. Our membership is drawn from a wide cross-section of the communications industry, including carriers, carriage and internet service providers, content providers, equipment vendors, IT companies, consultants and business groups.

We are writing this letter in support of the Australian Mobile Telecommunications Association's (AMTA) submission to the Right to Repair inquiry. Their submission thoroughly addresses the matter of consumer access to repair and management of e-waste in Australia. We agree that Australian consumers are well served by the existing regulatory framework in regards to mobile phones and devices, and that there is no need to add further regulation on these matters beyond the rights already included in the ACL.

Additionally, the Commission should take into account the security implications of any changes that would increase access to communications equipment by unauthorised repairers. With the number of devices connected to the internet predicted to reach anything between 25-30/household in 2021 (mobile phones, routers, modems, IoT devices) and forecast to increase even further over the coming years/decades, it is critical to ensure that no additional sources of vulnerabilities are being introduced into the system.

These devices have replaceable firmware to allow suppliers to maintain and update the device software and to plug security holes, in addition to a range of physical parts that are accessed by a (licenced) repairer. However, we see the risk that unauthorised repairers may use uncertified (cheaper) parts or install uncertified firmware on devices – both of which can make these devices vulnerable to hacking and illegal interceptions. In fact, many large businesses prohibit the connection of phones without their original firmware ('rooted' phones) to corporate intranets because of the seriousness of these security issues and possible privacy implications. Private households, however, would be unlikely to be aware of any security compromises.

Beyond the security implications, firmware implication arise, particularly in the context of mobile phones. If an Australian firmware set is wrongly replaced with a foreign firmware set by the same manufacturer or by a generic set, the phone might mis-operate (or not operate at all) in Australia by activating on the wrong spectrum, or possibly would not comply with other legal requirements such as Standard AS/CA S042.1:2020 *Requirements for connection to an air interface of a Telecommunications Network – Part 1: General*, which requires that emergency calling remain available even if a phone is locked or has an expired SIM. This could place consumers at risk in emergency situations.

Allowing unauthorised 3rd parties to repair communications equipment could have implications for the security of home and work networks and the broader Australian telecommunications infrastructure, including the possibility of opening backdoors for fraudulent access or illegal interception.

We would be pleased to further discuss this matter with the Commission if there are any questions.

Yours sincerely,

John Stanton
Chief Executive Officer