30 July 2023

DITRDCA
Telecommunications Competition / Communications Infrastructure Division
coord@COMMUNICATIONS.gov.au

To Whom It Concerns,

IoT Alliance Australia submission – Regulation of LoRaWAN, issues paper June 2023

Internet of Things Alliance Australia (IoTAA) thanks the DITRDCA for the opportunity to submit feedback to the Regulation of LoRaWAN issues paper consultation.

IoTAA is the peak body for the Internet of Things (IoT) in Australia. A non-profit industry association, IoTAA was formed in 2016 to enable a data smart Australia, which advances society through trusted, accessible real-time data, powered by Internet of Things technologies. Communications technologies and networks are an integral part of the IoT technology suite, whether at the collection point in sensors, at the edge or in the core network for centralised intelligence – and at many points in the data chain across multiple entities.

Our members include LoRaWAN service providers, integrators, device providers and service users.

Our responses to the 10 questions raised in the consultation are in the appendix 1 of this document.

The IoTAA would welcome the opportunity to discuss any aspects of our submission in further detail.

Yours sincerely,

Frank Zeichner

Chief Executive Officer
IoT Alliance Australia
0408 233 762
www.iot.org.au

Appendix 1: Consultation questions

1) **Which parts of a LoRaWAN network should be regulated? Under the current regulatory framework, it is possible that all owners of gateways who provide use of the gateways to the public may require a carrier licence. The Department thinks that in general capturing individuals and entities that have little to no telecommunications technological capability would be undesirable?**

In general, we do not see a case for regulation of LoRaWAN networks, beyond that required by existing unlicenced band regulations.

As outlined in the consultation paper, Telecoms policy is driven by the need to drive services and encourage market development. Regulation plays an important role in reducing monopolistic behaviour especially where spectrum introduces market restrictions.

We see no clear market need e.g. competition issue to disrupt a thriving and growing LoRaWAN connectivity market. Moreover, the application of a carrier regulation would impose a stifling burden to most instances of existing LoRaWAN use in Australia.

Market development using LoRaWAN is evident, with over 80 Councils across Australia using LoRaWAN to provide community IoT data network access. This initiative has greatly increased economic development initiatives as well as aided in the post COVID recovery of communities and businesses in providing remote asset management for many popular tourism, trader, coastal and innovation hubs. For example:

City of Melbourne - https://www.melbourne.vic.gov.au/about-melbourne/melbourne-profile/smart-city/Pages/free-lorawan.aspx#:~:text=LoRaWAN%20is%20low%2Dpower%20networking,are%20used%20in%20a%20day.

City of Perth - https://www.iothub.com.au/news/perth-gets-a-community-lorawan-network-476560

University of Melbourne - https://www.iothub.com.au/news/how-the-university-of-melbourne-used-lorawan-and-iot-in-covidsafe-strategy-582055

LoRaWAN is also providing cost-effective and important data connectivity is an area of poor or no cellular coverage for many businesses and industrial applications including for farmers, utilities, asset management and for environmental monitoring.

   a) **How should sharing of network units by end-users be managed under the regulatory framework?**

LoRaWAN gateways shared or not should be exempt from the regulatory regime.

   b) **Could LoRaWAN Gateways be exempted from regulation as network units where the Core network is provided by a licensed carrier or is subject to a nominated carrier declaration?**

Yes. LoRaWAN gateways should be exempted.

This also simplifies/bypasses the "boundary issue" where gateways are personally owned but nevertheless may contribute to a wider access network. Policing "personal" gateways that might be required to have a carrier licence would be highly impractical.

None of the three case studies listed in the paper (personal, business or council pp12-13) should require a carrier licence, in our view.

2) **End-users vs businesses: Increasingly as we saw in the examples above, individuals and 'non- telco' businesses are entering the telecommunications network and providing services in the network. This raises questions around whether the relegations should recognise this and apply the laws differently.**

   a) **Should the type of owner of gateways and sensors affect the way the telecommunications laws should be applied?**

In general no.

   b) **For example, does the owners' status as an individual or business affect the applications of telecommunications specific obligations? What about their assumed technical ability?**

No

   c) **Should end-users have regulatory obligations if they are sharing gateways with others on a commercial basis? On a personal use basis?**

No.

   d) **Is it correct to assume that a portion of end-users will tend to own gateways?**

Yes, it is the case now for many networks, especially community networks.

   e) **Is it likely that an entity maintains ownership of the gateways as part of a LoRaWAN network?**

Ownership models for LoRaWAN are quite varied, including managed, outsourced, owned, shared etc.

3) **Core networks: Core networks are responsible for much of the switching and 'intelligence' associated with LoRaWAN networks and would be considered a CSP under current regulations. The Department would like to know if any regulatory changes around Core networks should be considered.**

   a) **Should LoRaWAN Core networks be subject to carrier obligations?**

In general no.

There may be providers who represent themselves as carriers, in which case yes.

There is also a practical issue to be considered, if this were to be a requirement; namely that in many cases the 'core" control may not be through an Australian entity or managed in Australia. There may be ways in circumscribing this e.g. by forcing local control.

   b) **Would it be sufficient to protect the public interest in relation to LoRaWAN networks, if Core networks were captured as network units but gateways were exempted?**

We don't see what public interest is served by introducing regulation.

4) **National Interest: There is a general obligation on Carriers and CSPs to secure their networks and equipment from interference and do things to assist enforcement of the law. This requires Carriers and CSPs to have a certain level of sophistication and control of their equipment and service. Whether LoRaWAN technologies challenges these obligations should be considered.**

   a) **Can all parts of a LoRaWAN network be reasonably protected?**

In general, yes.

Interference is possible but hard at gateway level and with lower risk due to a relatively limited coverage and data flow.

The risk is higher at the network level, due to wider coverage and potential impact.

b) Is there anything about the set-up of LoRaWAN networks that make them particularly vulnerable to unauthorised interference?

LoRaWAN networks are not any more vulnerable than other types of Radio Frequency networks. In most cases they are less vulnerable as the LoRaWAN protocol has been designed with encryption as part of the standard. It is not possible to send unencrypted payloads over LoRaWAN.

- Most LoRaWAN end-devices (sensors) have no attack surface outside of their encrypted channel to the network as they don't rely on IP protocol.

- LoRaWAN Gateways relay LoRaWAN packets to the Network Server via TCP-IP. Gateways typically run embedded-Linux or another operating system. They are potentially more vulnerable than LoRaWAN devices, but no more so than other network appliances such as routers, switches, modems, etc.

- LoRaWAN Network Servers can be either cloud-based or on-premise software applications which communicate with the LoRaWAN Gateways and other LoRaWAN Network Servers. These should be secured and managed like any other Internet-facing software.

c) What are the security implications on individual households, unsophisticated businesses and government entities owning LoRaWAN gateways and other components? Should those entities have interception and data retention obligations?

As with Wi-Fi, no.

Definitely not. Gateway owners do not know identities of users and would have high difficulty in implementing interception.

d) Are the current national interest settings correct for LoRaWAN?

In general, these are not required.

There may be a case for security requirements in high-risk scenarios for services of national significance. (Critical infrastructure).

e) Would it be in the public interest for owners of gateways not to be subject to national interest requirements?

Yes, except possibly for those providing a service to services of national significance.

5) **Competition: One of the purposes of the telecommunications laws is to regulate the actions of individuals and businesses in the market, including to promote investment and control natural monopolies/bottlenecks. New technologies are likely to be disruptive to the competition settings in the regulations and a rethink may be needed if there is evidence to indicate a systemic issue.**

a) Could LoRaWAN conceivably be subject to access and competition monopoly issues? Can you identify any real-life examples? Could gateways be subject to those issues?

There is no evident market failure that we can identify.

Access issues we have seen, have resulted from poor use of the unlicenced spectrum e.g. Victorian energy meters occurred before the revised spectrum rules limited duty cycles and power output. Rogue gateway providers could breach power and duty cycle rules to disrupt.

b) Are there any access and competition monopoly issues that can arise with LoRaWAN networks that need to be addressed by specific telecommunications regulations?

No

c) Could a LoRaWAN provider, including the owner of a gateway, engage in anti-competitive conduct that could affect upstream and downstream telecommunications markets?

Yes, if they breached the power and duty cycle limits for unlicenced spectrum.

6) **Enforcement: There is some evidence to suggest that the requirement for LoRaWAN providers to have a carrier licence is not uniformly enforced. This could result in an uneven playing field for current players in the market and reduces investment in LoRaWAN networks in Australia.**

a) Is this claim substantiated? If so, can you point to some examples?

A 'de facto" requirement for LoRaWAN providers to have a carrier licence is uniformly not being applied as far as we know, which we support.

There is little evidence of reduced investment in LoRaWAN networks as a result.

b) How does the lack of enforcement on carrier licence requirements reduce incentives for investments into LoRaWAN networks?

On the contrary, lack of enforcement has obviated the requirement for burdensome carrier requirements which has made it relatively easy for LoRaWAN networks to proliferate. In Australia.

c) Would better enforcement assist in supporting competition?

It would seem better if LoRaWAN was specifically exempted, as for Wi-Fi, rather that the market assuming this.

7) **Powers and Immunities: A carrier licence holder is able to utilise powers and immunities set out under Schedule 3 to the Tel Act, which are critical to the efficient construction and maintenance of telecommunications networks. The laws can mean that carrier licence holders deploying communications infrastructure are exempt from some state and territory laws, including planning laws, for:**

- **facilities that are determined to be low-impact facilities,**
- **temporary facilities for use by a defence organisation, or**
- **facilities for which the ACMA has granted a Facility Installation Permit.**

a) Are there any powers and immunities issues at play in LoRaWAN rollouts?

LoRaWAN gateways are relatively small and have low power requirements. There are local council issues to be managed, for example, in placement of gateways – these have been dealt with relatively well. We see no need for special powers and immunities for LoRaWAN providers.

8) **Consumer protection: Telecommunications specific consumer obligations are linked to the delivery of particular services e.g., broadband or voice services and issue around billing and level of service.**

   a) Are there any consumer issues that LoRaWAN raises that should be dealt with by specific telecommunications law?

None that are not already covered by consumer law.

9) **Taxation: Status as a carrier can attract an obligation to pay fees to contribute to the overall regulation of the sector and for universal service provision.**

   a) Should owners of LoRaWAN gateways and/or core networks contribute to telecommunications specific taxes?

No. It is likely, at any rate, that LoRaWAN providers in Australia are below the taxation threshold.

10) **Other:**

   a) Are there any other issues arising from the roll out of LoRaWAN networks that the Department should be aware of?

Unlicenced spectrum for LoRaWAN in not uniform across the world. The Australian market will to some extent better leverage LoRaWAN devices from Asia as a result.

   b) Is there any other information you would like to provide to assist with our thinking?

   c) Would there be issues arising from regulating LoRaWAN that may be better addressed in other Government regulation or as part of other reforms? If so, which ones and why?

In the case where LoRaWAN networks are used for services of national significance there may need to be adjustments made in the SOCI act, where there is today reliance made on a carrier licence to provide that protection.

   d) Are there any linkages in the issues raised in this LoRaWAN paper that could relate to other Internet of Thing's issues?

There may be a case for a broader view including other radio access technologies to be exempted, rather than being LoRaWAN technology specific.

Appendix 2: About IoTAA

IoTAA is the peak body for the Internet of Things (IoT) in Australia. A non-profit industry association, we formed in 2016 to enable a data smart Australia, which advances society through trusted, accessible real-time data, powered by Internet of Things technologies. Our broad membership of over 300 companies and 1000 participants collaborate to drive adoption though knowledge creation and sharing, building ecosystems and public advocacy.

Our focus

We focus on the three key areas that matter most for Australia:

- Sustainability: defining and promoting how organisations access the data they need to support their pathway to net zero and circularity
- Productivity: identifying use cases, highlighting leaders, codifying good practice, IoT/OT convergence and quantifying the value of IoT adoption
- Trusted technology: demystifying IoT technology, creating design and deployment tools and guides, setting the principles and good practices for trust in IoT and developing an IoT for Good charter.

What is IoT?

The Internet of Things (IoT) is a transformative suite of technologies that, if appropriately and sensitively implemented, can help address the great social and ecological challenges of our time. The Internet of Things encompasses Industrial IoT, which is fundamental to Australia's economy including critical infrastructure, manufacturing, cities and placemaking, construction, productivity and consumer IoT. Consumer IoT is growing exponentially and introducing a seismic shift in data use, trust and the balance in consumer and service provider interactions.