Thank you for the opportunity to make a submission regarding the use of telecommunications data in civil proceedings.

Question 1

> *In what circumstances do parties to civil proceedings currently request access to telecommunications data in the data set outlined in section 187AA of the TIA Act?*

Executive Summary

The most likely circumstances are that a copyright holder, or someone acting on the holder's behalf, is seeking access to the contact details of ISP customers who it alleges have violated its copyright.

This would be with a view to sending threatening and extortionate demands to those customers.

Question 2

> *What, if any, impact would there be on civil proceedings if parties were unable to access the telecommunications data set as outlined in section 187AA of the TIA Act?*

Executive Summary

If these companies are not able to access telecommunications data today then there will be no impact on proceedings if that prohibition is maintained.

However perhaps that is not quite how the question is intended to be interpreted. So another answer would be: The proceedings would be less likely to continue. The companies involved would adapt their business models to the 21st century.

An equally important question – which the Committee should also be asking – is: What impact would there be if parties *are* able to access telecommunications data?

Question 3

> *Are there particular kinds of civil proceedings or circumstances in which the prohibition in section 280(1B) of the Telecommunications Act 1997 should not apply?*

Executive Summary

No

There should be no scope creep, no new mission, for telecommunications data retained in accordance with the Data Retention regime. The prohibition should always apply.

Detailed Commentary

Terrorism or Copyright?

In justifying the powers implied by the Data Retention amendment, the government was keen to stress that Data Retention would only be used in terrorism investigations and in the investigation of serious crime. While this was controversial enough, many people supported the goal, if not the method.

Abandoning this rationale so soon after the amendment passed into law, and indeed before the Data Retention regime is even officially up and running, is not a good look!

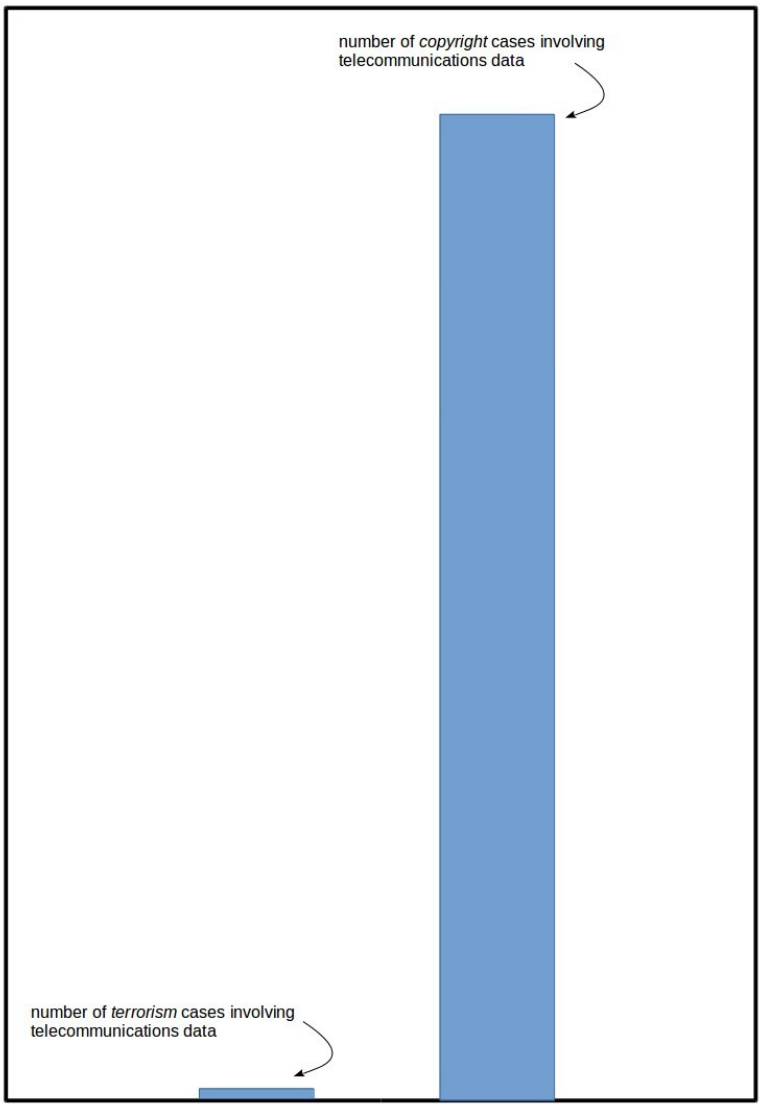
Attorney-General Brandis said on Q&A on November 3, 2014:

"the mandatory metadata retention regime applies only to the most serious crime, to terrorism, to international and transnational organised crime, to paedophilia, where the use of metadata has been particularly useful as an investigative tool, only to as a tool, only to crime and only to the highest levels of crime. ***Breach of copyright is a civil wrong. Civil wrongs have nothing to do with this scheme.****"* (my emphasis)

Link: http://www.abc.net.au/tv/qanda/txt/s4096883.htm#transcript

Abandoning this rationale could have the effect of undermining public support for Data Retention and thereby have the effect of undermining public support for anti-terrorism measures generally.

If copyright holders are given ready access to telecommunications data then I forecast that the number of court cases per year relating to terrorism and using retained data versus the number of court cases per year relating to copyright infringement will look something like this. (diagram to scale)



This will make it difficult to maintain the fiction that Data Retention is about fighting terrorism, and thousands of Australians will have first hand experience of the reality.

Burden on ISPs

Another consideration is the burden on ISPs. The government originally said that it would meet the cost of the Data Retention regime. However it seems likely that the government did not ultimately fund 100% of the cost of the regime. This therefore leaves ISPs with a deficit for the provision of a service that is ostensibly a public benefit. The burden can only increase if telecommunications data is opened up to civil proceedings.

The distinction between data that is retained solely for the purposes of meeting the legal obligations implied by the Data Retention amendment and data that is retained both for those purposes and for the purposes of the ISP's business is not a solid one. An ISP could be tied up in court for months attempting to justify its classification of each individual piece of data.

I would suggest that the difficulties with this distinction be resolved by deeming that telecommunications data is *never* available to civil litigants. This is more consistent with the *Telecommunications Act*, which seeks to make this data strictly confidential and allow its release only in extreme circumstances, such as that the customer is suspected of being involved in a serious crime.

Protecting customers

In expressing my views here I am mindful of the great lengths that the judge in the Dallas Buyers Club case (*Dallas Buyers Club LLC v iiNet Limited*) went to in order to protect ISP customers from dishonest threats. It should not be up to individual judges to protect ISP customers from such threats. The legislation itself should do so.

Once telecommunications data is released to other parties there simply is no way to control what use is made of it or who will have access to it. This problem is bad enough in respect of the original rationale for Data Retention and it certainly doesn't get any better when the data is opened up to aggressive commercial litigants.

In this case we even had the extraordinary spectacle of the plaintiff demanding that ISP customers reveal their income details (perhaps because they intended to “fine” wealthier customers a larger amount). This shows how an entity with an appetite for private data should not be trusted with it, and should not have private data handed to it on a plate by the government.

The judge in this case proposed a $600,000 bond to ensure that the civil litigant, who had no assets in Australia, did not abuse the private data that would be released to it. It is unclear exactly how that bond was to work (i.e. under what circumstances it would be returned to the plaintiff) but this certainly raises two issues.

1. That a bond is even required or contemplated in this situation is a warning sign that telecommunications data should not be released to civil litigants.
2. You don't have to be too clever to see how such a system might be circumvented by disreputable plaintiffs.

Links: http://www.itnews.com.au/news/dbc-wants-alleged-pirates-income-download-details-405372

http://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2015/2015fca1437

The regulation change proposed here by the government can be seen as a continuation of the long-running war by copyright holders on ISPs and ISP customers, most notably as commenced in the original iiNet case (*Roadshow Films Pty Ltd v iiNet Limited*).

Links: http://www.austlii.edu.au/au/cases/cth/FCA/2010/24.html

https://en.wikipedia.org/wiki/Roadshow_Films_Pty_Ltd_v_iiNet_Ltd

Subversion by ISPs

One technique that ISPs could use to subvert the regulation change proposed here would be for ISPs to store the telecommunications data encrypted (which is a legislated requirement anyway) in such a way that authorised law enforcement and national security agencies could decrypt the data but the ISP itself could not. That would render any civil action to force the ISP to disclose the information irrelevant as the ISP would literally be unable to do so.

This would require the ISP to discriminate between

- telecommunications data that is collected and retained solely for the benefit of government agencies – it would be collected and immediately encrypted against ISP access
- telecommunications data that is collected and then retained for a short period (less than 2 years) for ISP business purposes and thereafter only for the benefit of government agencies – it would be collected, stored accessible to the ISP for a short period and then encrypted against ISP access
- telecommunications data that is collected and retained for at least 2 years for ISP business purposes – it would be stored accessible to the ISP for the lifetime of its retention

However it would seem that this change might force an ISP to make that distinction anyway.