# Comments on the Australian Assistance and Access Bill 2018

Mark Nottingham
11 October 2018

Thank you for the opportunity to comment.

I am an Australian citizen who is active in the Internet standards community. While I submit this in a personal capacity, I serve as Chair of the HTTP Working Group in the IETF, a member of the Internet Architecture Board (IAB), and a former member of the W3C's Technical Architecture Group (which serves a similar architectural function for the World Wide Web).

I believe that several aspects of the proposed legislation need more careful consideration, but understand that you are receiving other submissions regarding transparency, oversight, and related issues, so I won't address those directly despite my concerns in those areas. Likewise, as a member of the IAB, I will not repeat the arguments made in our separate submission.

Instead, I'll focus on one aspect of concern that may not be covered elsewhere.

## Content of Communication and Intercept Related Information

The proposed legislation balances the powers that it grants to enforcement agencies using the Telecommunications (Interception and Access) Act 1979 (hereafter, TIA)'s existing requirement for an applicable warrant to obtain *Content of Communication* (CC). From the explanatory memorandum:

> Under a technical assistance request or technical assistance notice, a provider cannot be asked to provide the content of a communication or private telecommunications data […] without an existing warrant or authorisation under the TIA Act.

However, Chapter 4 of the TIA describes what is often called *Intercept Related Information* (IRI) or "metadata." IRI does not require a warrant and includes such things as call times and destinations, subscriber information and so forth.

This is a reasonable and well-understood tradeoff for telephone intercepts; what someone says in a real-time voice call is protected and requires a higher level of oversight, whereas information about when and to where the call is made has a lower bar. It reflects a balance between the need for lawful intercept and the need for privacy.

Over time, governments have applied this distinction with some success to non-voice products of telecommunications providers, and then Internet Services Providers. In these cases, the endpoints of the communication, the subscribers' details and so on are IRI, whereas the actual payload is (usually) CC. Even so, the differences in communication models (circuit switched vs. packet switched) have created tensions in the past.

However, the proposed legislation nominates a much broader variety of communications providers than the authors of this distinction could have contemplated; it encompasses virtually all Web sites, apps, Internet-connected hardware and software. The services they provide are diverse, often with no clear mapping to those provided by telecommunications services, and are often deeply entwined with people's personal lives. Despite this, the proposed legislation gives no guidance regarding IRI.

To give just a few examples:

- Is an Internet-connected fitness tracker's log of the times and places its user goes considered Content of Communication or Intercept Related Information? Their heart rate and blood pressure?
- Is a person's private profile on a dating Web site CC or IRI — keeping in mind that it could be considered "subscriber information"? Could their connections to other users be considered analogous to who someone calls on the telephone?
- If I use "smart lighting" in my home, will that information be available without a warrant to any interested enforcement agency? A reasonable argument could be made that knowing when people are home helps them perform their duties — the bar set by the TIA.
- Are the items I sell and buy on shopping and auction sites considered content of communication, or metadata? Are the times of day that I open my refrigerator "intercept related"?
- Does anything stop an enforcement agency from using these powers to efficiently collect a cross-indexed database of all online accounts that Australians keep?
- If the Attorney-General requires Google to incorporate a machine learning model into Gmail to identify suspected terrorists amongst all Australian users, only supplying the "hits" but not their e-mails, will that require a warrant?

As written, the proposed legislation leaves these decisions open as a matter of interpretation, with the likely outcome being a body of secret administrative and judicial decisions. This leaves very little opportunity for the public to judge the processes' legitimacy or understand its impact.

Beyond the inapplicability of this "content/metadata" duality to Internet services, another significant issue is how what might be collected from Internet services using these instruments can "leak" a much larger amount of data about a person when taken in aggregate.

Simply put, if my activity on a number of Web sites, Internet-connected devices and apps is collected as "metadata" and analysed, it reveals significantly more about my life than merely knowing who and when I've called and texted.

This makes IRI an extremely powerful tool when applied to Internet services; much more so than current legislation, practices and public expectations are calibrated for. Modern computing techniques such as machine learning will only magnify this effect over time.

While I and most Australians believe that our law enforcement officials should have powerful tools at their disposal, there should be appropriate controls over their use — including oversight and transparency — and well-understood limits guided by legislation, not secret decisions.

This shortcoming can be addressed by defining everything obtained using these new powers as CC; i.e., there should be no metadata, as far as this legislation is concerned. If industry and government can agree to carve-outs for IRI (e.g., subscriber account information), that can be enshrined in this legislation or future law.

Kind regards,

Mark Nottingham