Comments on the Australian Assistance and Access Bill 2018

Mark Nottingham <[redacted]>
7 September 2018

Thank you for the opportunity to comment.

I am an Australian citizen who is also active in the Internet standards community, having been Chair of the HTTP Working Group in the IETF for more than ten years, a member of the Internet Architecture Board, and a former member of the W3C's Technical Architecture Group (which serves a similar architectural function for the Web).

I had the opportunity to discuss this legislation with government advisors, department staff and members of the opposition on 21 August, after being a panel member at the Internet Society's event about encryption the previous night.

Those conversations left an impression that the government is taking a much more nuanced, thoughtful approach to this legislation that it and other governments (both in Australia and abroad) have in the past.

That said, I believe that several aspects of the proposed legislation need more careful consideration. I understand that you are receiving other submissions regarding transparency, oversight, and other issues, so I won't address those here. Likewise, as a member of the IAB, I will not repeat the arguments made in its submission.

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

Content of Communication vs Intercept Related Information

One of the primary protections relied upon in the proposed legislation is the existing requirement for an applicable warrant to obtain Content of Communication (CC). However, Intercept Related Information (IRI, aka "metadata") does not require an applicable warrant.

As I understand it, this distinction was designed for telephone intercepts; what I say or hear in a real-time voice call is protected and requires a higher level of oversight, whereas information about when and where calls are made has a lower bar. It reflects a balance between the need for lawful intercept and the need for privacy.

Over time, this approach has also been applied 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 the communication models (circuit switched vs. packet switched) have created some tensions in the past.

The proposed legislation applies to a much broader set of dedicated communications providers than the original legislation contemplated; it encompasses virtually all Web sites, apps, Internet-connected hardware and software. The services they provide are diverse, and often do not map to those provided by telecommunications services, and are often deeply entwined with people's personal lives. Despite this, it provides no guidance on this issue.

For example, is an Internet-connected fitness tracker's log of the times and places its user goes when CC or IRI? Their heart rate and blood pressure?

Is a person's private profile on a dating Web site CC or IRI?

Are the items I sell and buy on shopping and auction sites considered content, or metadata?

Are the times of day that my refrigerator was opened “intercept related”?

Besides the inapplicability of a telecommunications “data/metadata” duality to most Internet services, a significant issue here is that what might be considered IRI for Internet services 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 and apps is collected and analysed, it reveals significantly more about my life than merely knowing who I've called and texted, and when. Modern computing techniques such as machine learning magnify this effect, which will become even more pronounced over time.

This makes IRI (depending on how it is interpreted) an extremely powerful tool when applied to Internet services; much more so than current legislation and practices are calibrated for. While I and most Australians believe that our law enforcement officials should have powerful tools at their disposal, it should have appropriate controls over its use, and well-understood limits.

I would suggest that this could be addressed by assuming everything associated with these services is CC; i.e., there is 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.