The Committee Secretary
House of Representatives Standing Committee on Infrastructure & Communications
PO Box 6021
Parliament House
Canberra ACT 2600

Section 313 of the *Telecommunications Act 1997* (Cth)

This submission responds to the Committee's invitation for public comment on government agency use of section 313 of the *Telecommunications Act 1997* (Cth) for the purpose of disrupting illegal online services.

In summary, there are substantive concerns regarding proportionality, effectiveness and appropriateness.

The section has such a wide scope, and appears to be so misunderstood by both law enforcement/national security personnel and telecommunications sector employees in the private sector, that a principles-based restatement is highly desirable.

Warrantless access to telecommunication content/metadata on the basis that connectivity providers are 'assisting' a range of law enforcement agencies is inappropriate and should be condemned by the Committee. Proposals for premptive action by agencies to take down online content on an extrajudicial basis should similarly be questioned.

Basis

This submission is made by Assistant Professor Bruce Baer Arnold.

I teach privacy, security and consumer law at Canberra Law School, ie the University of Canberra. My work has appeared in Australian and overseas law journals and practitioner publications over the past decade, for example *Privacy Law Bulletin* and *Melbourne University Law Review*. I have made invited submissions and testimony to a range of law inquiries at the national and state/territory levels during that time.

The following comments do not necessarily represent the views of the University of Canberra. They do not present what would be reasonably construed as a conflict of interest.

This submission initially offers general comments and then addresses specific concerns regarding the Committee's Terms of Reference.[1] It is based on familiarity with Australian and overseas data protection and telecommunications law, along with participation in a range of policy advisory bodies (for example regarding the Australian domain name system and the OECD global data protection guidelines) over the past fifteen years.

---

[1] The Terms of Reference for the inquiry cover (a) which government agencies should be permitted to make requests pursuant to section 313 to disrupt online services potentially in breach of Australian law from providing these services to Australians; (b) what level of authority should such agencies have in order to make such a request; (c) the characteristics of illegal or potentially illegal online services which should be subject to such requests; and (d) what are the most appropriate transparency and accountability measures that should accompany such requests, taking into account the nature of the online service being dealt with, and what is the best/appropriate method for implementing such measures.

Warrantless access and metadata

Recent controversy in which senior Commonwealth officials and ministers have given contradictory statements regarding metadata and regarding open-ended official access to communications demonstrates the important of clarity. It also demonstrates disquiet on the part of legal practitioners and academics, business and the broader community about

a) warrantless access to information, access that in practice is invisible and uncontestable and inappropriately bypasses the courts

b) the under-resourcing and hence regulatory incapacity of entities such as the Inspector-General of Intelligence & Security and the Office of the Australian Information Commissioner

c) the disregard of politicians and senior officials for human rights such as privacy, a disregard that is not justified through recourse to rhetoric about a 'hundred year war on terror' that requires abandonment of the liberal democratic values that differentiate Australia from totalitarian regimes such as ISIS.

Matters addressed by s 313 would be more appropriately addressed under other legislation, for example the *Telecommunications (Interception and Access) Act 1979* (Cth). As a liberal democratic state we should be wary of requirements to suppress websites merely on the basis that content is illegal overseas, for example a site that features criticism of the Syrian president or of egregious human rights abuses in Iran, Russia and Uganda.

We should also be wary about law that authorises preemptive action that is not justiciable – contrary to a fundamental principle of the Australian justice system – and that is so poorly documented as to lack transparency and thus eliminate the accountability that is a foundation of Australian government.

The section appears to be interpreted by officials in ways that blur

- law enforcement (ie instances where there is an expectation that evidence will be available and contestable) and
- national security (where action on occasion will be appropriate on a preemptive basis in the absence of an offence).

That blurring puts bureaucratic convenience (or misguided enthusiasm) ahead of justice.

It results in activity that is legally unsound and brings law enforcement into disrepute.

It is open to misuse – and to legitimate perceptions of misuse – by Commonwealth, state/territory and quasi-government entities.

As a society we legitimately expect connectivity providers, content hosts, publishers, authors and other entities to assist officials. Such assistance involves trust, a trust that is clearly absent in regimes such as North Korea, Syria and ISIS. Trust is founded on an expectation that governments and proxies will behave legitimately, ie will act in ways that are –

- authorised by law (rather than merely by employment as an official or

appointment as a minister)

- proportionate (ie are predicated on need rather than bureaucratic convenience, reflect impact rather than mere risk, respect rather than erode rights and responsibilities)
- accountable (an accountability that encompasses the transparency that enables a lawful challenge to arbitrary decision-making)

It is tempting for every Government and agency to claim that its circumstances are exceptional and require extraordinary action in the public interest. A succession of submissions by the Law Council of Australia, the law societies, law academics, industry representatives and civil society advocates over the past fifteen years have questioned the appropriateness of proposals for mandatory retention of telecommunications metadata on a whole-of-population basis. Irrespective of costs to connectivity providers and content hosts, which will of course be passed on to consumers, that retention is grossly disproportionate. Unsurprisingly it has been rejected by courts in Europe as grossly disproportionate.[2] It has been questioned by senior advisors to the US government as ineffective, a criticism consistent with independent assessments in other jurisdictions. Those proposals are of particular concern when coupled with suggestions that access to metadata should be provided to Commonwealth, state/territory, local government and other entities on a warrantless basis. Such provision is contrary to accountability.

Few privacy advocates would disagree with the need for law enforcement or national security personnel to engage in surveillance in particular circumstances. It is an accepted and fundamental principle, however, that such surveillance can only be undertaken on a legitimate basis. There is no reason why law enforcement access to telecommunication content and metadata should take place outside a legal framework per se and without a warrant. Law enforcement personnel have recurrently sought warrantless access on the basis of convenience. Law enforcement is a matter of justice rather than official convenience.

In the absence of any indication that legitimate requests for warrants are being refused by the courts the Committee should question whether there is a need for warrantless access under s 313. I suggest that the Committee should resist proposals based on what is convenient for Commonwealth officials and peers in other governments. The Committee should instead call on the Government to reconsider s 313, restricting rather than extending warrantless access to both telecommunications content and metadata about that content.

The Government will presumably note that a requirement for warrants will impose a financial burden and even result in delays. Both claims lack substance. A warrant regime provides an essential and appropriate discipline. Costs will be involved, but as a society we accept that the justice system necessarily involves costs. Those costs are legitimate and historically have been embraced by the community when Governments have made an effort to explain why and how taxes are spent. If savings are essential – and there is evident disagreement within government regarding the basis for budget cuts – they might most appropriately be found through cutting handouts to special interests (such as the millions allocated in the latest Commonwealth Budget to accommodation for students at a ballet school in

[2] Contrary to hyperbole by a senior Australian Federal Police officer several years ago, that condemnation has *not* resulted in the end of 'law and order' in Germany or other parts of Europe and has been endorsed by EU governments and voters, providing a reality test for Australia's parliaments.

Melbourne) rather than eroding the capacity of the OAIC or skipping warrants on the basis that the Australian Federal Police cannot afford to engage with the courts.

More broadly as a society we should expect that access will be contestable. If law enforcement personnel are acting appropriately they have nothing to fear. If they are acting outside the law or are misinterpreting the law they should be held to account. Accountability may, again, be inconvenient but it is consistent with Australian values – it is one of features of life that differentiates us from terrorists (and from entities such as Wikileaks), something that we should zealously preserve and that is more important than the opportunism evident in media releases from both major political parties over the past decade.

A bureaucratic 'kill switch'

Government officials concerned with consumer protection, crime and other matters are typically diligent and conscientious. Regrettably, however, some are uninformed and blinkered. A recurrent feature of discussions with industry over the past fifteen years has been calls by Commonwealth and other agencies for what critics characterise as a 'kill switch', ie the ability to require internet service providers and internet content hosts to deny public access to online content on the basis of a direction by an official.

Those calls encompass deletion of content from a server or removing internet address information so that the content cannot be found. The latter action might amount to the suppression of legitimate content that is independent of illicit material published online by another entity, with for example officials regarding the disappearance of hobby or commercial sites as acceptable collateral damage attributable to suppression of sites used for financial scams, retailing of fake pharmaceuticals, the promotion of hatespeech and so forth.

The scale of such suppression may be large. One indication is the advice by ASIC to a Senate committee last year that it had caused blocking of some 250,000 websites – blocking those sites in error, without compensation and without a substantive commitment to learn from its error.

A legal axiom is that 'just because you can do something doesn't mean that you should'. We should be wary about authorisation of officials to act as a prosecutor, judge and executioner in requiring the takedown of online content under s 313. Action should be undertaken specifically rather than through a broad 'requirement to assist' provision, particularly a provision where

- law enforcement is being conflated with national security
- there is no compensation for error
- there is no appeal mechanism
- content owners need not be notified by a government agency or by an internet service provider/content host that a site has been taken down
- there is, at best, uncertain accountability for error.

Open-ended assistance

In an independent submission to the Committee the Australian Privacy Foundation has highlighted specific privacy concerns regarding s 313. Those concerns are worthy

of consideration and are consistent with representations over the past decade by bodies such as the Law Council of Australia.

In particular there is concern regarding the open-ended nature of assistance to government agencies, for example perceptions that assistance involves a requirement to store and provide access to a range of information in a way that

- erodes privacy protections
- is not transparent
- is not justiciable.