



**Australian
Privacy
Foundation**

<http://www.privacy.org.au>

Senate Legal & Constitutional Affairs References
Committee

**Inquiry into a Comprehensive Revision of
*Telecommunications (Interception and Access)
Act 1979***

Supplementary Submission, October 2014

Data retention proposals raise spectre of ‘thought crime’

Attention has been focused on legitimate concerns about the implications of mandatory data retention by telcos for privacy rights in general and for freedom of speech and association in particular. (as well as for the costs and who will bear them).

The focus has been on communications between at least two parties. There has been insufficient attention to the implications of the regime extending to communications that do not involve a second party – specifically on individuals’ use of the internet as a library or passive information resource.

The proposals (to the limited extent that they have been clarified) appear to include a requirement for ISPs to retain at least some information about internet content providers for sites visited (see note on the next page*), and the date and time of visits, by users identified at least to their IP address level – which in many cases will allow identification of the individual concerned.

To the extent that the regime will capture information about ‘what a user has looked at’, it represents a quantum leap in the level of insight it will potentially give law enforcement and intelligence agencies (and perhaps others – we do not yet know) into the concerns and interests of all Australians using the internet.

The closest ‘real world’ analogy would be if lending libraries were required to retain comprehensive records of all the books and other artefacts borrowed by their subscribers (a scenario which has already caused controversy, and litigation, in the US in relation to use of the PATRIOT Act powers).

Such surveillance potentially invites legitimate questions about where on the spectrum from interest to action it is appropriate for the state to have knowledge about individuals’ behaviour.

Consider the following scenarios:

- A. An individual consults a reference material on ‘bomb-making’ – motive unknown, and could as easily be benign as malicious?
- B. Two individuals communicate about ‘bomb-making’ – could be innocent but more likely to be reasonable grounds for suspicion? In some cases could amount to criminal conspiracy?
- C. One or more individuals attempt to make a bomb – very likely to be at least the precursor to a crime?
- D. One or more individuals make and attempt to explode, or succeed in exploding, a bomb – almost certainly a crime?

Few people would object to information about any of these scenarios (including A) being available to law enforcement agencies once they had established reasonable suspicion of a criminal offence, to the satisfaction of an appropriate authorising authority (important separate issue about thresholds and safeguards). Powers already exist for agencies to seek preservation orders on telcos in

possession of information about an individual's participation in any of the above scenarios, **once reasonable suspicion has been established**.

But what is at issue in the data retention debate is a different question – what information about an individual's participation in any of the above scenarios should be routinely retained and available to law enforcement agencies **as a general intelligence resource in order to generate suspicion**.

If the answer to this question includes Scenario A then we have crossed a major Orwellian threshold into potential 'thought crime' – where the burden of proof is reversed, and individuals are presumed to be guilty (of what?) unless they can prove themselves innocent.

Many thousands of individuals in any time period will presumably be exploring issues of crime and terrorism, whether out of academic research, journalism, general interest, or in some cases unhealthy obsession, misguided ideology or evil intent. Leaving aside who can or should judge what is unhealthy or misguided, it is clear that only a tiny minority of these individuals will ever prove a threat to others or to society in general.

The Parliament should think long and hard before facilitating, or mandating, routine surveillance that could readily (and almost inevitably) will be used to identify subjectively 'aberrant' behavior.

The 'thought crime' point has also been recently expressed by our chair, Professor Roger Clarke, in this way:

"The early years of the current century have seen technological change that embodies serious threats to a further dimension of human concerns. What an individual reads and views, and the ideas that they gain access to through meetings and other events, have been converted from unrecorded ephemera to stored data. That data is under the control of and exploitable by for-profit corporations, and available to government agencies. The privacy of personal thought may not yet be directly under assault, but the privacy of personal experience is a dangerously close proxy for it". Privacy and Free Speech, August 2014 <http://www.rogerclarke.com/DV/PFS-1408.html#PD>

We call on the Committee to take this important perspective into account in formulating its recommendations.

Nigel Waters
Australian Privacy Foundation

- See note on next page

***Q. Will the proposals require retention of any information about a user's 'destination' on the internet?**

The August 2014 AGD Confidential industry consultation paper, *Telecommunications data retention—Statement of requirements* repeatedly seeks to re-assure readers that:

'Category [x] does not apply to or require the retention of destination web address identifiers, such as destination IP addresses or URLs. This exception is intended to ensure that providers of retail and wholesale internet access services are not required to engage in session logging. **However, operators of such services remain obliged to retain network address allocation records (including Network Address Translation records) under category 1(b).**' (my emphasis)

However, category 1(b) is defined as:

‘... both present and past identifiers allocated to an account or service by the service provider (such as an IMSI, IP or email address, or other network identifier).’

It seems clear that this would include some information that would identify ***to at least some level*** the nature of a website visited.

[illegible]

Attachment – Two recent critiques of the metadata proposals

For a valuable technically informed critique of the government's metadata proposals, see this blog post from respected internet expert Geoff Huston - <http://www.potaroo.net/ispcol/2014-08/metadata.html>

Huston concludes that 'metadata retention to permit public IP address records to identify end users' is almost certain to 'morph from a simple log of assigned customer IP addresses into a comprehensive surveillance program that compels ISPs to capture and retain a comprehensive log of each user's online activity'.

Also this from Crikey:

Crikey says: rank incompetence from our new overlords

"As demolition jobs go, it is one of the more comprehensive ones you'll see: iiNet's response to the first paper circulated by the federal Attorney-General's Department to initiate discussions on the government's proposal for the mass surveillance mechanism known as data retention.

This isn't the first industry consultation process about data retention. As Crikey revealed last year, the department began pushing the Rudd government virtually the moment it was elected in 2007, but cruelled its own efforts by trying to rush the issue and failing to listen to the concerns of industry.

A recurring theme of previous AGD consultation efforts on data retention was its wholly unwarranted secrecy, and bureaucrats' poor understanding of some of the most basic issues around metadata. The latest consultation papers -- though widely available -- are still officially secret; judging by iiNet's response, AGD has barely improved its grasp of the basics, with many of the categories of the proposed data to be retained described as "vaguely defined" by the company. What we do know is that AGD has explicitly and bluntly contradicted both the Prime Minister and its own minister, Attorney-General George Brandis, who have both insisted -- in Brandis' case as recently as last week -- that data retention will not involve anything beyond what companies currently collect.

As iiNet notes, however,

"The Consultation Paper expressly states that data which falls within the defined data set will be required to be retained 'even if this exceeds business needs' and that 'the policy recognises that providers may need to modify some systems to ensure they meet the minimum standard'."

There's only three ways of reconciling this contradiction: either AGD has got it wrong, Brandis and Abbott don't have even a basic grasp of what data retention is, or Brandis and Abbott are deliberately misleading the community."

Between AGD's poor grasp of the technical basics and the huge gulf between what politicians say and what their bureaucrats demand, it's no wonder companies like iiNet -- regardless of their position on the benefits or otherwise of data retention -- are so utterly confused.

The AGD has had seven years to get this right. That they still haven't done so suggests rank incompetence, and that's hardly comforting when it comes to plans for mass surveillance."