GlobalResearch
Center for Research on Globalization

Internet Privacy and Individual Rights: Australia's "National Data Retention Regime", A Fool's Paradise in the Land of Oz

By Dr. Binoy Kampmark
Global Research, February 22, 2015

Region: Oceania
Theme: Intelligence, Police State & Civil Rights

There should be nothing polite about it, whatever the curious start of the article in Gizmodo (Feb 3) suggests. The "future of privacy on the internet in Australia" is simply but one in a series of skirmishes being waged by a mishmash of authoritarian sentiments against the domain of private citizenry. At its heart is the nervous and nigh ridiculous desire that retaining data – that is to say, the metadata on individuals in the course of using various services – will somehow curb criminality, foil terrorism and keep deviance at bay.

The Australian angle on this is characteristically buffoonish, finding shape in the National Data Retention Regime. It demands that telcos and internet service providers retain data for a designated period of time – at this point two years – to be made readily available for law enforcement authorities to dip into. The drafters seem oblivious to the prospect that, in making such a pool of data readily available, malicious use of it is bound to happen. What is stored is bound to be accessed, however "secure" the systems in question.

What exactly that data constitutes suggests as much about the insentient authorities as it does about the cognitive deficiencies inherent in the entire effort to combat "threats" to the state. A "proposed data set" document that is doing the rounds says nothing about what exactly will be in the regulations, though it is predictably cumbersome.[1] The ghastly instrument that will enact the regime, the Abbott government hopes, is the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*.

The set does, however, seek to be as broad, and vague, as possible, making the reader drown in verbiage and tedium. (The most dangerous laws are often the most appallingly drafted ones.) In a section covering "Matters to which information must relate", an example in the data set includes information that covers names, addresses and "any other information for identification purposes" covering "the relevant service, being information used by the service provider for the purposes of identifying the subscriber of the relevant service".

Australia's Privacy Commissioner – whose post exists as a vague nod that the idea just might be important in the country – is concerned about the possibility of "breaches". Timothy Pilgrim fears that the scheme might result in ISPs collecting "more personal information than is necessary" for business purposes and "retaining that information for longer than is necessary for those purposes."[2] He proposes that internet and phone providers be required to disclose the fact of such breaches. Pigs, of course, might fly.

Then there is a lingering question as to whether this entire act of intrusive tomfoolery will even work. Earlier in the month, representatives from the Australian Attorney-General's department discussed the matter with Senators in Parliament House. The rather haphazard nature of the regime came to the fore, with Greens Senator Scott Ludlam probing Anna Harmer of the Attorney-General's section on "the wide variety of ways in which people could accidentally circumvent data retention by, for example, using a university network or logging onto the Parliament House Wi-Fi".[3]

A specific question related to the use of the Parliament's Wi-Fi network. "In this building, would the metadata be retained by anyone in particular or would that be out of the scope of the National Data Retention Regime?" Harmer's response suggested two "specific exemptions in the Bill" covering "services that are provided in a same place, and ones provided to an immediate circle. The immediate circle ones wouldn't be applicable here."

Leaving aside the pseudo-Ptolemaic madness regarding circles, Harmer's obtuse point serves to show how garbled and convoluted the regime is in draft form, notably over what constitutes a commercial service provider. This invariably affects public libraries, universities and various institutions. But might there be data collection from an individual using a Wi-Fi at a coffee store chain? Possibly not, as the "individual coffee shop provider does not need to disaggregate the data in respect of his or her individual customers".

The government, floundering before legislation that is ossifying on the Senate benches, is barking the usual reasons as to why this incompetent creation needs to pass: retaining such data is fundamental, despite the fact that the recent spate of attacks in Europe, not to mention the hostage situation in Sydney, would not have been prevented by such a data pool.

Prime Minister Tony Abbott, showing his characteristic immunity to reason, is convinced. "If we don't keep this data, our crime fighting agencies and the police are flying blind." Such deficiencies of sight are hardly likely to be cured by the data junkies, who, it seems, barely understand what it entails. What matters is that oversight and restriction to getting such data, most of it being superfluous to the agencies in question, can be accessed without warrant. The only requirement here is the signature of a faceless functionary.

The critics of the regime are not exactly screaming from the roof tops. An unnamed former police employee versed in the arts of metadata collection has told the ABC that, "The Australian people are being sleepwalked into a system the attorney-general cannot even articulate."[4] The source suggested a pertinent analogy: "asking a library to keep a history on their systems of who borrowed a book. [The library] don't care. They want to know who *has* a book; but that information is only required until it's returned. Data retention would force them to keep that info for two years."

The greatest danger of such an order of data retention is not even a dystopian one featuring corrupt police brutalising protesters and dissenters. Such totalitarian bestialities should never be deemed impossible, but in a materialist wonderland such as Australia, information retained by ISPs and telcos offers other rich prospects for abuse.

The transformation of a regime on data retention designed to circumvent terrorism or criminal activity easily becomes a bludgeon for the corporate sector keen to guard against copyright infringement. Now that must be music to those conservatives on parliament's benches. The long arm of the law becomes the brutish arm of the purse. The muddled,

even awkward words of the “source” suffice to show the seriousness of what is at stake: “[All it would take is] simple lobbying by a financial backer of political parties to make copyright seen as theft and bang so many Aussies caught up criminally”.

Not exactly *1984*, with its dark themes of technological enslavement, but certainly a nightmare of holed privacy, incompetent governance and sinister prosecutions. Freelance terrorists and lone wolf operators will have nothing to fear.

Dr. Binoy Kampmark was a Commonwealth Scholar at Selwyn College, Cambridge. He lectures at RMIT University, Melbourne. Email: bkampmark@gmail.com

Notes:

[1] http://www.ag.gov.au/NationalSecurity/DataRetention/Documents/-ProposeddatasetOctober2014.pdf

[2] http://www.smh.com.au/digital-life/consumer-security/australias-privacy--commissioner-tim-pilgrim-fears-telco-metadata-breaches-20150126-12ydmc.html

[3] http://www.gizmodo.com.au/2015/02/can-australias-proposed-data-retention--scheme-be-easily-circumvented-depends-on-who-you-ask/

[4] http://www.abc.net.au/radionational/programs/downloadthisshow/6145722

Articles by: Dr. Binoy Kampmark