Retained data in civil proceedings consultation
Communications Security Branch
Attorney-General's Department
3-5 National Circuit
BARTON ACT 2600

17 Jan 2017

Dear Assistant Secretary,

Re: Access to telecommunications data in civil proceedings

Thank you for the opportunity to make the submission below.

I authorise its publication online.

Yours sincerely,

Justin Warren
Managing Director
PivotNine Pty Ltd

Summary

The mandatory data retention regime was specifically created, and justified, on national security and law enforcement grounds. Civil access to such data constitutes a major change in the intent and scope of the regime.

In justifying the need for the regime, the public was regularly re-assured that the regime did not involve the creation of new data, merely ensuring that existing data was retained for law enforcement and national security purposes. Logically, therefore, civil litigants already have access to the same kinds of data as retained in the regime.

The Parliamentary Joint Committee on Intelligence and Security (the Committee) was very clear in its *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (the Report) when making its Recommendations relating to access to data held under the regime:

> Nonetheless, the Committee considers that the proposed data retention regime is being established specifically for law enforcement and national security purposes and that as a general principle it would be inappropriate for the data retained under that regime to be drawn upon as a new source of evidence in civil disputes.[1]

Access to regime data should not be expanded to any civil proceedings or circumstances.

Discussion

Purpose of Data Retention

In justifying the creation of the mandatory data retention regime, the Attorney-General's Department and various supporting agencies were very clear that its purpose was to assist with law enforcement and national security.

Then Minister for Communications Malcolm Turnbull said at the time:

> This bill is critical to prevent the capabilities of Australia's law enforcement and national security agencies being further degraded. It does not expand the range of telecommunications metadata which is currently being accessed by law enforcement agencies. It simply ensures that metadata is retained for a period of two years.[2]

The threats to privacy of individuals were balanced against the need to combat serious crime and threats to the nation. The implicit assumption here is that the needs of the many outweigh the needs of the few, and thus some privacy must be given up in order to keep everyone safe. Whether or not the widespread collection and storage of surveillance data on the populace is effective or correct is a separate discussion. For now, Australia has decided to err on the side of mass surveillance.

However, this trade-off was made under specific circumstances, and a particular bargain was struck: personal privacy must be reduced, in exchange for the promise of greater protection from significant threats, and criminal, threats to a great many people.

Whether this bargain was well made is beyond the scope of this submission. If the terms of the bargain are to be altered, then all parties to the bargain should be given the opportunity to re-negotiate its terms.

1 Parliamentary Joint Committee on Intelligence and Security, 'Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014' (Commonwealth of Australia, February 2015), 223.

2 Parliament of Australia, 'The Hon Malcolm Turnbull, Minister for Communications' (House of Representatives Hansard, 30 October 2014), 12560.

Not New Data

If the data held under the data retention regime is—as we have been regularly told—not new data, then civil litigants already have access to the data in question.

The question then becomes whether or not the data civil litigants can access is

a) consistently created by all telecommunications providers, and

b) how long data is retained outside of the data retention regime.

Consistency

One feature of the data retention regime is to standardise the creation and/or storage of particular kinds of data across the industry. By prescribing a specific set of data that all providers must retain, the Government ensures that *all* providers create the same data types. Previously, if there was no business purpose for a specific provider to generate a particular kind of data, it may not have done so. Access to such data in a civil case could not be assured, because while one provider (say, Telstra) may use that data for standard business purposes, a smaller regional ISP may have no need for it, and thus wouldn't bother creating it or storing it because of the increased cost of doing so.

Now, because this data must be created and stored for data retention purposes, *all* providers have a common standard (for some loose definition of *standard*) of data to create and store. Providers are therefore far more likely to use this data for other purposes, because if they have to collect the data anyway, then they may as well get some business value from it as well. This is particularly likely for smaller providers with smaller margins who are less able to absorb the cost of implementing the data retention scheme.[3]

Since the data would then no longer be used "solely for the purpose of complying with Part 5-1A" of the *Telecommunications (Interception and Access) Act 1979*, it would no longer be covered by section 280 of the *Telecommunications Act 1997* and could be disclosed.

Civil litigants are therefore already likely to have increased access to data than they did prior to the introduction of mandatory data retention.

Civil Retention

A second major feature of mandatory data retention is the retention itself. Civil litigants do not currently enjoy a standard retention length across the industry; they must content themselves with whatever data a provider chooses to retain for its own purposes.

Extending access to the mandatory data retention regime to civil litigants would mean they come to enjoy the same two year mandatory retention period as law enforcement. But this retention period was justified on national security and terrorism grounds, not so that jealous men could stalk their ex-girlfriends[4], or so copyright holders could issue speculative invoices to people downloading fairly tedious movies.

If there is a strong enough case for a data retention period for civil purposes, then let it be debated and legislated separately from legislation designed to combat terrorism and serious crime.

Indeed, why should it be otherwise?

---

3 The cost of the regime is unclear, but is at least $100 million and may be as high as $700 million. 'Telecommunications data retention—an overview', *Parliamentary Library*, http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BN/2012-2013/DataRetention, retrieved 17 Jan 2017.

4 Richard Chirgwin, 'AFP Officer Abused Data Access to Stalk Ex', *The Register*, 3 June 2015, http://www.theregister.co.uk/2015/06/03/afp_officer_pleads_guilty_over_stalking/.

Limited Access

The Committee was particularly mindful of the existing access to Telecommunications data, as is clear from its comments in its *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (the Report).

The Committee understood that civil access to telecommunications data was already common practice, and that it would need to continue:

> The Committee is aware of the potential for unintended consequences resulting from a prohibition on courts authorising access to data retained under the data retention scheme. The potential for possible interference with judicial power was also raised in evidence.[5]

However, the Committee was also very clear that data retained under the data retention regime should not be accessible to civil litigants:

> Nonetheless, the Committee considers that the proposed data retention regime is being established specifically for law enforcement and national security purposes and that as a general principle it would be inappropriate for the data retained under that regime to be drawn upon as a new source of evidence in civil disputes.[6]

The Committee made recommendations that carefully avoided unintended consequences for interference with judicial power with the need to retain data for law enforcement and national security purposes. The recommendations maintained the existing ability for civil litigants to access data from telecommunications providers, but sought to enjoin them from using the regime data as "a new source of evidence in civil disputes."[7]

To remove restrictions on civil access to data held because of the mandatory data retention regime, as the Consultation Paper appears to suggest, would go completely against the recommendations of the Committee.

Such a position is particularly curious given the Government's enthusiastic support for all of the Committee's recommendations[8] at the time.

5 Parliamentary Joint Committee on Intelligence and Security, 'Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014', 223.

6 Ibid.

7 Ibid.

8 Brandis, G, Turnbull, M, 'Government Response to Committee Report on the Telecommunications (Interceptions and Access) Amendment (Data Retention) Bill 2014', 4 March 2015, http://www.malcolmturnbull.com.au/media/government-response-to-committee-report-on-telecommunications-amendment-bil, retrieved 17 Jan 2017