27/01/2017

Dear Assistant Secretary,

Re: Access to telecommunications data in civil proceedings.

Thank you for the opportunity to respond to this inquiry.

I do not believe that a strong case has been made for the existence of a regulatory power to make 'appropriate exclusions' to the prohibition on civil litigants accessing telecommunications data held as part of the mandatory data retention regime.

To address the particulars of the review, as I do not have the relevant experience, I will refrain from commenting on points 1 and 2.

In reference to point 3: *are there particular kinds of civil proceedings or circumstances in which the prohibition in section 280(1B) of the Telecommunications Act 1997 should not apply?*

No, I do not believe there are.

The mandatory data retention regime was originally introduced to prosecute serious and high-level crime, including terrorism. Attorney-General George Brandis is quoted as saying that 'Civil wrongs have nothing to do with this scheme.'[1] To expand access to this data would represent a significant widening in scope of the scheme that I consider unacceptable and dangerous given the already broad levels of warrantless access granted to authorised agencies and the intelligence community. Throughout the media coverage of this review which I have extensively followed, I am yet to read or hear anyone within the legal profession justify such an expansion. Instead, many have described it as unnecessary, disproportionate, and invasive.

Given the threat such access poses to Australians' privacy, I do not believe that civil courts should have access to data retained as part of the mandatory data retention regime.

I am also particularly concerned with the amendments to section 280 of the *Telecommunications Act 1997*, which prohibit the disclosure of telecommunications data in relation to civil proceedings when such data is collected solely for the purpose of complying with a providers data retention obligations under Part 5-1 A of the *Telecommunications (Interception and Access) Act 1979* (TIA Act). The prohibition in theory is a good idea,

[1] http://www.abc.net.au/tv/qanda/txt/s4096883.htm

however the ability for data that was *not* retained solely as a result of the data retention scheme (i.e. data ordinarily held for business purposes) to be subpoenaed or brought before a civil court has its own problems with regards to implementation and ambiguity.

As a hypothetical example, a telecommunications carrier might record the approximate location of a mobile device and the cell towers it connects to as part of its billing processes for calls and SMSs. Prior to the data retention scheme being implemented, it may have retained this information on a month-by-month basis as was necessary for billing. This would constitute such information being used for business purposes.

After the implementation of the data retention scheme, such information has to be retained for a minimum of two years. At this point, a data set that was originally used solely for business purposes is now also being retained due to the data retention scheme, but not *solely* for the purposes of the scheme.

If this cell tower data is also used for billing purposes – despite the fact that only one month of a minimum 24 months is used for billing – does that remove the prohibition (under the *Telecommunications Act 1997*, Section 280, (1B)) and render all 24 months of data available to civil proceedings?

There appears to be considerable ambiguity about how this might work, and it is not difficult to imagine practical issues emerging. Is only the first month of that data available for civil use, as that would constitute the data used for billing purposes? Or would the courts decide that because such information is not retained solely for compliance with the data retention scheme, that the entire two years should be available for civil proceedings?

Furthermore, the billing practices of telecommunications carriers and ISPs may change in unpredictable ways. Should a carrier or ISP expand their billing practices to require six months of data on an individual's phone and the cell towers it interacts with, could those six months of data then be subpoenaed by civil courts?

The current legislation around this issue is not clear, and crucially, it provides very little security, transparency, and clarity for Australian citizens, their data, and their privacy.

I urge the government to review this measure in consultation with civil liberty bodies, telecommunications carriers, and ISPs, to ensure that requirements are clear and explicit, and that there are strong privacy protections for individuals and their data. This could take numerous forms. At a bare minimum, requiring carriers and ISPs to disclose to customers

how much data they retain for business and billing purposes, so that individuals are then aware of how much of their information could be available to a civil court.

A more elegant and practical solution to the above issue would be to consult with civil rights bodies, carriers, and ISPs to discover where a reasonable overlap might exist between data sets being retained for both business purposes and for the purposes of the data retention scheme. Once meaningful consultation has occurred, certain data sets for specific time periods could be explicitly legislated to be made available to civil courts, only for the purposes of preserving the manner in which such data has been available in the past. This would reduce the need for a regulation-making power to make exceptions to the prohibition being reviewed. For example: it may be discovered that in general, carriers retain an individual's cell tower location data for billing purposes for between one to two months. To then legislate that civil courts can only ever access, say, the most recent month of that data, would at the very least provide transparency and clarity for citizens and consistency across the industry, which is much more than the current system appears to provide.

If the government is serious about retaining citizens' data to prosecute high-level crimes like terrorism, while also making sure that data retained for business purposes is still available to civil courts, a full review and consultation with industry and civil rights bodies about how this could strike an effective balance between access and privacy is necessary.

Overall, I recommend that rather than widening the scope of access to data retained through the data retention regime, the government consider whether or not an already revealing and invasive system such as this should be further limited, rather than expanded.

I recommend that access to the retained data is not expanded for use in any civil proceedings, that no regulatory power is legislated for or used to make exceptions to the prohibition, and that the current mandatory data retention regime is reviewed as soon as possible. I further recommend that a rigorous, mandatory data breach notification scheme be put in place, as such a scheme is paramount to Australian citizens, their data, and their privacy.

Yours sincerely,

Jeremy Stevens