

Subject: Data Retention Submission
Date: Tuesday, 2 December 2014 2:39:42 PM

Dear JCIS,

I hold grave concerns with relation to the data retention, as has been shown around the world you do not need content to build a profile of a persons life, who their friends are, what sports they like, where they like to shop, and eat, as a law abiding citizen in my near half century of life, I consider this proposal a gross invasion of mine, and everyone else's privacy, I did not realise you can be guilty through association in 2014 in Australia, but that sounds like exactly what this proposal aims to do.

I am a fairly private person, I avoid places like facebook for that reason, yet I commit no crimes and are a supporter of our Police who do a wonderful job in such trying circumstances, and the line that if you have nothing to hide you have nothing to fear, just doesn't wash, that's a cop out justification line.

I know the world is a different place post 9/11/2001, and that times have changed even since then, but the LEA's and Security Services should never have blanket access to the private information of the community en mass. I do accept law enforcement need tools to do their job, they have been using s262 of the Telco Act for some time and seems to work well, and the information they requested is pretty much what they want now, except perhaps with a few extras, and in times to come I'm sure even more.

However, my most grave concern is, it goes to great lengths to restrict Government access, yet as Federal Police Commissioner Colvin and The Hon Malcolm Turnbull have both publicly stated, the data is available to anyone civilly who can put a case to a court for the release of that information. This is absurd, there must be strict controls on the data access for only Law Enforcement and as the AG George Brandis has said, for "serious crime", therefore there must be amendments and safeguards to ensure it is only used in serious criminal matters and preventing a court ordering the release of this information in any civil matters.

I understand that there is at times good reason for an ISP to retain information to deal with spam or abuse complaints, or if you like, everyday ISP operational matters, this typically would be about a month to match IP to user, so I would not be concerned if a civil court was to order the release of a users details matching an IP Address if the incident was proved to be within 28 days, because it would be reasonable to expect an ISP to have Radius and Email Server logs for that period, but they must never be granted access to data that is old, like a blanket discovery for something months or a year ago.

That said, if this is to become law, I implore you to set in stone, law that restricts this data for serious criminal offences only, after 28 days of the alleged incident, preventing a court from ordering its release in civil cases after such time, further limiting its access.

Sincerely

Noel Butler