To the Australian Minister for Communications and the Attorney-General,

With regards to the Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 - Consultation Paper – Access to Retained Data in Civil Proceedings

The metadata laws were imposed on the people of Australia under the guise of national security to protect the public against terrorist attacks.

From the beginning there has been a great deal of mistrust as to this information ever being used for these purposes and instead many believe that they were implemented for the eventual betrayal of the Australian public to foreign companies in exchange for campaign funding and other perks for our less altruistic politicians.

Security experts all state that this information is less valuable than the powers granted under a surveillance order previously granted by the courts. Target-less information on this scale held at the ISP level is only ever likely to be accessed after an event as there is too much content for continuous monitoring.

Most Australians had expected that this information would be available to just the AFP and ASIO as two trusted organisations protecting the people of this nation. Instead the purpose was corrupted almost from day one by access being granted to groups such as:

Australian Postal Corporation; Civil Aviation, Safety Authority (CASA); Clean Energy Regulator; Department of Agriculture; National Measurement Institute; Bankstown City Council, NSW; Greyhound Racing Victoria; Racing and Wagering Western Australia; Royal Society for the Prevention of Cruelty to Animals (RSPCA); Taxi Services Commission.

I will ask the obvious question here: what do any of these groups have with protecting Australians from malicious attacks?

It is well known that the co-chairman of Village Roadshow's Australian branch has had an inappropriate level of access to and influence on our elected representatives. This includes being involved in the push for meta-data retention along with the call for this review being on a delay so as to mislead the public that the true primary intent was not data gathering for civil litigation purposes all along. They have even been granted access to talk to young children at schools to engage in corrupt attempts at social engineering.

The co-chair himself has been publically quoted saying that movie pirates should be pursued to the same degree as terrorists and paedophiles showing complete disregard to national security, public safety and those among us that have been in any way affected by these very real and serious crimes.

Metadata information only reveals that a person has accessed a website and (from the stated parameters that are recorded) should provide no definite proof as to whether or not a person has performed a civil infraction. As far as my understanding goes, our courts still require actual proof of wrong-doing rather than weak circumstantial evidence that even basic malware could create without a user ever knowing the connection has been made.

However, this circumstantial evidence coming from surveillance that has been gathered under federal law would likely frame this data with a false legitimacy and very possibly result in unjust verdicts.

Many people do not understand the frailty of this proof including a number of our out-dated, technologically backwards magistrates and so opening up the information for civil proceedings would create an environment where greedy companies can attempt to profiteer off of this misunderstanding. In fact, the only civil use for metadata is circumstantial misinformation and so this access should never be granted.

As Australia is a democracy I see this information arbitrarily gathered on the citizens of this nation being available to anybody but the aforementioned AFP and ASIO that protect us as a breach of trust. To make it available to foreign owned companies for potentially use against our own citizens would be an act of treason and never to be tolerated or kept quiet.

Concernedly Yours,

Keith