At the risk of pointing out the obvious, proceeding with this proposal will simply make life far more difficult for our various security agencies.

At the moment, very few Australian Internet users take advantage of secure proxy services (like TOR), or strongly encrypted IP tunnelling (through a plethora of private VPN's), or other application based (secure e-mail, routine browser based SSL connections, software update applications, gaming, proprietary - e.g.Apple, Windows etc etc - applications and protocols et alia) point-to-point encryption measures … but the proposal to make the already collected metadata available to non-government third parties for civil litigation (and possibly other purposes in future? Perhaps later on you could sell the data to the highest bidder?) will no doubt see an explosion of traffic on these high level encryption and data security services.

At present it only makes sense for either the nefarious or the more technologically informed to do so. (And at what currently amounts to between $3 and $5 per month, the economics of comprehensive encrypted data and communications security are within the reach of all.)

Threaten to make your data available to non-government third parties - and the incentives to use said anonymising and encryption services increases. And given that many packages to do same are much more available, advertised and user friendly than they were say even two years ago, said services are much more accessible to the average Internet user that you perhaps realise.

Which means that Joe Public will have an incentive to subscribe to 'secure communications' protocols, VPN's and secure applications protocols like never before. Strong encryption and data tunnelling will become de-riguer and increasingly common, rather than a manageable (by our security agencies) exception to the rule. And in the case of the services mentioned I might remind you what we are talking about is private keys assigned at the moment of establishing the socket by the secure remote server. (In other words, the client has no idea of how to decrypt the data, because they don't possess the keys and can't give same to security agencies no matter what they are threatened with.)

Now ask yourselves whether Australian security agencies have either the computing power and resources to track all this real-time 'false positive' encrypted traffic between 'innocent' clients and servers across the world, or whether their metadata analysis efforts would be severely impacted. Do they need to be monitoring a thousand times the encrypted traffic that they currently do? Do their packet traffic analysis techniques depend on examining data packet characteristics. Do they need to have even the metadata from the packet headers buried deep in encrypted packets between the local client and overseas based (in God knows what friendly and/or unfriendly jurisdictions) secure server on an effectively impenetrable encrypted link?

Because that is what will happen if the average Internet user activates even routine IP security. Ever more ubiquitous strongly encrypted real-time data communications means that our security agencies will be buried under data that is to all intents and purposes useless.

And the quality of the collected metadata will drop through the floor to the point of being unusable, whilst the quantity of 'junk' metadata increases astronomically.

… and that is what will happen if you carry through with this idea of making metadata available to non-government third parties. Australians trust their government with their metadata - especially in the current security situation, but they don't trust unelected anonymous private third parties. And they will take measures to secure their communications from eyes they don't trust.

Frank O'Connor
Rye VIC