"If you give me six lines written by the hand of the most honest of men, I will find something in them which will hang him". Cardinal Richelieu

To Whom It May Concern

I hereby wish to state that I strongly oppose the proposal to make retained data and or metadata available for use in civil proceedings.

My reasons for objecting include the following:

Smartphone data and metadata is used to constantly track user location. Although inherent in how the mobile phone service works, this data can also be used to determine where the user works, eats and sleeps. The location data can be used to determine whether the user goes to church, which church, how much time the user spends in a casino or a bar, and whether the user speeds while driving, even if only slightly. It can also be used to determine whom the user spends his or her days with, whom the user meets, as well as where and when, and, even who the user sleeps with, because the other people the user interacts with can also be reasonably expected to carry mobile phones, which produce similar data.

If the Government announced that everyone would henceforth be required to wear a tracking device so that it (the Government) and other organisations may track citizens 24 hours a day, 7 days a week, such a law would immediately be regarded as unconstitutional and as violating our basic human rights. The fact is, our mobile phones already produce all this tracking data - the only difference is that the data is not currently available to everyone seeking access to it as though they were tracking devices. Making it available for government agencies, private companies and available to civil litigation procedures would turn our mobile phones into the most efficient and the worst kind of tracking devices.

Our location information is very valuable. The police use it for helping with criminal investigations, and some governments have used it for social control. Organisations and companies may use it for location based advertising, and if it were to fall in the wrong hands, it may even be used for targeted attacks on individuals, and potentially evading the authorities. This is not as unlikely as people might assume.

There have been numerous cases where the Australian Government has admitted that security breaches of sensitive information had occurred, and they have no idea who has access to that data now. There was the blood donor data breach of October 2016, and the more recent gun owner address data breach in December 2016, which clearly evidences the fact that the Government does not have sufficient security measures in place to protect even limited amounts of sensitive information. Imagine the repercussions if legal litigation companies got hold of everyone's location and communication data. They would exploit any and every potential opportunity to monetize their find, irrespective of what collateral societal damage they might cause.

If health insurance companies had access to our health and fitness data, especially if it is coupled with information about our eating habits, heart rate during exercise and how frequently we exercise, to say nothing of DNA sequencing data, they could use that information to assess a person's overall health, and make business decisions based upon it. Doing so would allow them to discriminate against citizens whose data they have access to.

The Coalition used the threat of terrorism to justify introducing the metadata retention laws in 2014, vowing that people had nothing to fear from their introduction. The premise is that the government would relieve our fear of terrorism by having access to all our data. This wasn't as much a consultative process as a Government decision, and citizens have accepted it too easily and without really understanding the terms or its implications. There is no evidence that the mass surveillance and data retention laws introduced in 2014 have even resulted in any terrorism charges or convictions, instead the Government has just collected it and repeatedly demonstrated that it cannot keep our data secure.

The technology available to the Government allows it to conduct mass surveillance on a national scale.
["Mass surveillance makes it possible to discriminate based on almost any criteria: race, religion, social demographic, sexual orientation and political beliefs. It can be used to control what we see, what we do, and ultimately, what we say. It is being done without offering citizens any recourse or any real ability to opt out, and without any meaningful checks and balances. It actually makes us less safe. It makes us less free.

The data we generate is not limited to the mobile phone location data, it's also data about our phone calls, text messages, emails, web pages we visit, financial transaction data, etc. Many people don't realize that computers are integrated in everything we do, or that computer storage has become cheap enough to make it feasible to indefinitely save all the data we produce. Most of us also underestimate how easy it has become to identify us using data that we consider anonymous. History has repeatedly demonstrated the dangers of allowing governments to perform unchecked mass surveillance on their citizens. Potential harms include discrimination, control, impeding free speech and free thought; inevitable abuse and loss of democracy and liberty". A phrase often quoted by proponents of mass surveillance is "If you have nothing to hide, then you have nothing to fear". The Stasi in the the German Democratic Republic during world war 2 relied on it, and demonstrates a narrow conception of the value of privacy. Privacy is fundamental to being human and is an essential part of how we communicate to others and how we portray ourselves. We reveal different aspects of ourselves to our colleagues and boss than what we reveal to our partners. There is nothing dishonest about that. Denying people the basic right of privacy is dehumanizing and collecting and storing all the data we produce so that it may be extracted, perused and interrogated in intricate and impersonal detail at some later date is wrong. The fact that he Government wants to do this to its own citizens is terrifying.

Collecting metadata on people means putting them under surveillance. The former director of the US NSA and CIA, Michael Hayden remarked in 2014 that the US Government kills people based on their metadata. Phone metadata reveal a lot about us - the length, time and frequency of our calls reveal our relationships with others, our intimate friends, business associates. It reveals what we are interested in and what is important to us, no matter how private. Computers are more adept at processing metadata than actual data (content), and many experts have indicated that with enough metadata, you don't even need the actual data to find what you're looking for. Metadata is also ideal for discovering incidental findings, as it can apply a certain algorithm across everyone's metadata, as opposed to investigating only one person to find certain patterns. Computers are very good at establishing relationships and trends in data, which only become evident upon processing and "mining" the data. The more data (or metadata) there is to analyse, the better computers are at analysing it] Bill Schneier - Data and Goliath,The Hidden Battles to Collect Your Data and Control Your World.

Consider how being gay was illegal in Australia as recently as 1997. If the Government had access to the same data it currently holds on all people's location and communications metadata, it would have been very easy for them to prosecute individuals on the basis of the data or metadata they generated, and homosexuality would never have been decriminalised. We cannot grow or evolve as a democratic society in a world where everything we say and everywhere we go is recorded and analysed for signs of breaking the law. The data retention laws currently allow for retrospective analysis of our data, and making it available for civil litigation cases will undermine and erode any remaining sense of privacy people might still have.

Arguably some of the most important responsibilities of our Government are to keep its citizens safe while also protecting their freedom and liberty. A world in which we are under constant surveillance by an unseen authority is even more efficient than what Jeremy Bentham philosophised about in the late eighteenth century. In this infamous model, which he dubbed the Panopticon, prisoners would be observable by unseen guards at all times. The idea is that if the prisoners didn't know when they were being watched, but knew that it could be at any time, they would be compelled to conform at all times, reducing the number of guards needed, and resulting in cheaper prisons. We shouldn't have to feel like prisoners in a free country.

Targeted surveillance is fine. If a person behaves in a way that justifies surveillance, then by all means, have the police apply for a warrant and carry out the surveillance. But "fishing" for people who are not perfectly conforming to the police state dystopia a world of mass surveillance would create, by analysing everyone's metadata and combing it for irregularities is going too far.

In relation to the specific questions asked by the consultation paper, I would like to address questions 2 and 3:

Question 2: What, if any, impact would there be on civil proceedings if parties were unable to access the telecommunications data set as outlined in section 187AA of the TIA Act?

- Australian citizens would retain the last modicum of basic privacy that they are still currently (and should continue to be) entitled to. Even the metadata laws that are currently in place cause a wholly disproportionate amount of harm to citizens compared to the benefits of mass surveillance.
- By not allowing parties in civil lawsuits access to telecommunications data, lawyers and other operatives in the legal community would not be able to analyse all of the defendant's data and attempt to monetize their findings for their own benefit. In most civil proceedings the only real beneficiaries of financial compensation are the legal teams. Civilians, be they plaintiffs or defendants typically only end up with large bills, and are left feeling angry and stressed.
- Civil proceedings would proceed the way they always have. Just fine.

Question 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?

- Yes. It should not apply to any civil proceedings whatsoever.

Thank you for your consultation and consideration.

Best regards,
André de Lange