"Only to crime and only to the highest levels of crime": Individual Submission to the Consultation Paper "Access to Retained Data in Civil Proceedings"

I strongly support the prohibition of retained data being made available in connection with civil proceedings. There should be no change to s 280(1B) of the Telecommunications Act 1997 which prohibits the disclosure of data retained solely for the purpose of the Telecommunications (Interception and Access) Act 1979. Although I am opposed in principle to the data retention scheme that was introduced by the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, the protection against the use of the retained data in civil proceedings is important and should not be removed.

Civil Proceedings Would Not Be Impacted
Civil proceedings are not being negatively impacted because s 280(1B) is not removing their powers of discovery, but avoiding expanding the powers of civil litigants. No case was made for expanding the powers of civil litigants in Chapter 2 of the Parliamentary Joint Committee on Intelligence and Security’s (PJCIS) Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the “Advisory report”). The arguments made in this chapter were entirely about law enforcement needs to prevent and prosecute serious crime involving violence, terrorism and the sexual abuse of children. There has been no case made for a need for civil proceedings to have access to an expanded data set.

Notably, piracy lawsuits against individuals in Australia have failed due to the inability of plaintiffs to satisfy Court requirements, not due to a lack of access to telecommunications data. Dallas Buyers Club LLC v iiNet Limited failed in preliminary discovery because of the plaintiff’s unwillingness or inability to satisfy the Court that it would not engage in speculative invoicing. Therefore, even if data retained specifically for law enforcement to investigate serious crime and terrorism was made legally available to commercial litigants in piracy cases, it would have no effect because plaintiffs have not previously been granted preliminary discovery.

Data Collected Only for Serious Crime Should Not Be Used for Civil Proceedings
It is my position that no civil proceedings should be exempt from prohibition in s 280(1B) of the Telecommunications Act 1997. As noted above, the data retention scheme was specifically for the purpose of investigating the most serious crime. These were the only reasons that there was any support for the introduction of the scheme discussed by the PJCIS. Additionally George Brandis is on the record as saying,

“the mandatory metadata retention regime applies only to the most serious crime, to terrorism, to international and transnational organised crime, to paedophilia, where the use of metadata has been particularly useful as an investigative tool, only to as a tool, only to crime and only to the highest levels of crime. Breach of copyright is a civil wrong. Civil wrongs have nothing to do with this scheme.”
Australian Broadcasting Corporation Q&A, 3 November 2014
http://www.abc.net.au/tv/qanda/txt/s4096883.htm
To make data collected under the data retention scheme, where it is solely collected for compliance with that scheme, available to civil litigants is unjustified, inappropriate and unethical.

Not Consistent with Human Rights
The government may make laws that interfere with privacy rights and civil liberties that are for a legitimate purpose and are proportional to that purpose. The PJCIS report cites Professor Gillian Triggs, President of the Australian Human Rights Commission as saying, “In particular, we strongly support the bill’s proposal to confine the number of agencies that can access retained telecommunications data...” (29 January 2015). Additionally the PJCIS noted that it many individuals and organisations remained opposed to the data retention scheme, including many civil liberties groups like the Australian Privacy Foundation, Amnesty International, Blueprint for Free Speech, the New South Wales council for Civil Liberties and the joint councils for civil liberties as well as individual submissions “by and large” being in opposition to the proposal (2.4 & 2.8, Advisory report). Even when the data retention scheme was proposed only as a mechanism to combat the most serious crimes, it raised the concern of civil liberties groups, individuals and required limitation. Therefore, any expansion of access to address civil matters (which are minor relative to terrorism and child sexual abuse) would be completely disproportionate and inconsistent with human rights.

Raising the Cost of Living
The mandatory data retention scheme should not be opened up to civil proceedings because it would impose extra costs on telecommunications providers that would ultimately be paid by individual subscribers. In Chapter 6, the PJCIS Advisory report outlined submissions from the Communications Alliance and Australian Mobile Telecommunications Alliance arguing that making the data available for civil litigants would increase costs. They argued that the availability of the data would create a “honey pot” for civil litigants that “may start an industry” (6.98 -6.99). The importance of these arguments have not changed. If access is opened up to civil proceedings, it will raise the cost of living for everyone.

Scope Creep
The PJCIS noted that many civil liberties groups and interested individuals expressed concerns about scope creep with respect to civil proceedings. For example, Chris Berg of the Institute of Public Affairs cited the Polish experience about traffic and location data being used increasingly for divorce and alimentary disputes rather than combatting serious crime (6.101). The Australian Privacy Foundation also expressed concerns about the “honey pot” and its use in civil litigation (6.103) and the Law Institute of Victoria argued that the access to the data “should be limited to the purposes of the Bill, i.e. preventing, detecting and prosecuting crime and terrorist activities” (6.104). Making retained data available to civil litigants will demonstrate that the government is incapable of inhibiting its own growth and will reduce its credibility when asking for new, but limited, powers for legitimate purposes.

An Expanded Threat to Civil Liberty and Freedom
Making the data available in civil proceedings presents an expanded threat to civil liberties and freedom, including the rights of activists, journalists, academics and scientists. For example, a journalist could be sued for defamation and, as part of discovery, their
telephone metadata could be used to track down a whistleblower or activist. Scientists and academics may have the participants in their study identified because of legal action. In Canada, Marie-Ève Maillé has been ordered to provide a company with access to her data as part of civil court proceedings (Science, 22 November 2016, doi: 10.1126/science.aal0419). If telecommunications metadata were provided as part of discovery during such a lawsuit, many participants could be identified. As is the case for free speech, this could produce a chilling effect on research because guarantees of anonymity and confidentiality would be greatly weakened.

Expanding access to retained data also expands the risk that the data will be misused. Malevolent actors could use the courts to identify targets and related people for harassment. Civil litigants will not have as strong privacy and security controls as a limited number of government agencies and certainly not as strong as Australia’s police and intelligence agencies. Indeed, the use of retained data for family disputes will essentially have no privacy or security controls and individuals might discover things about their opponents that are unrelated to court proceedings but will nonetheless have negative consequences. For example, a couple that is going through a divorce following domestic violence may obtain each other’s telephone metadata records which would allow the violent partner greater insight into the victim’s behaviour. The risks of misuse are currently controlled by limiting access to a defined set of agencies, but if access is expanded then the risks of misuse grow very significantly for very little gain.

**Recommendation**

Expanding access to data retained under the *Telecommunications (Interception and Access) Act 1979* is not consistent with human rights, threatens civil liberties and demonstrates that the government cannot be trusted. It is an unjustified expansion of power that does not serve the purpose of the data retention program to enhance law enforcement’s capacity to investigate the most serious crimes.

I recommend that no change be made the s 280(18) of the *Telecommunications Act 1997*. 