This submission is made to the:

Inquiry into the gathering and use of criminal intelligence

There is a general consensus within the Australian community that the law enforcement tools available to our nation must be constantly improved, refined, and streamlined as just one means of being able to challenge and confront criminal organisations and terror networks.

Where sweeping and substantial changes are being considered, however, it is necessary to reflect deeply on their consequences, both intended and unintended.

In security and counter-terror theory, there are two factors to consider:

- ★ The motivational capacity.
- ★ The operational capacity.

That is, a man must have both the desire and the ability to commit a crime. Traditionally, law enforcement focuses on the latter, while it is up to the family and community to instil in a person a sense of responsibility and ethics such that they shall not aspire to a life of crime. Where a convicted felon is free, and remains criminally motivated, he will likely attempt another operation. This is known as recidivism. Focussing on the motivational capacity, therefore, is more efficient over the long-term.

When we propose legislation regarding law and order, we must analyse it from this perspective. While all Australians desire greater communication and interoperability between various law enforcement branches, the proposed ability of the authorities to access electronic data, stored, mandatorily, for two years, represents a disastrous paradigm shift for Australia's cherished and renowned democracy.

1. It does nothing to address the motivational capacity of terrorists and criminals.
2. The cost of the data retention will be massive. Vast multitudes of this data will be useless and inconsequential. A portion of this useless information will be 'false flags'. This is all grotesquely inefficient and a complete waste of time and money.
3. Circumventing such a system is, frankly, childishly easy. Encryption and stealth programs (and so forth) are easily available online, and are simple to use. With such circumventions available, it is difficult to conceive of a situation where such a scheme could in any way be of benefit to the fight against crime and terror.

4. It is an impossibility that the data would be secure. With several notable incidents of cyber-warfare and hacking having occurred recently, the potential for a breach is large, and this represents an unacceptable threat to the privacy of Australian residents and citizens. Worse, it represents a gold mine for hacker groups and foreign intelligence services.

5. Australia has a well-earned reputation as a free and fair democracy; an open and tolerant society. With similar legislation and proposals having been rejected elsewhere recently, Australia's international image and reputation will suffer tremendous damage.

6. The scheme represents a blanket, all-encompassing invasion of privacy for all Australians. That is, everybody is now a suspect, is under constant surveillance, and is deemed a person of interest. This would transform Australia into a police state by removing the presumption of innocence, promoting self-censorship, and, furthermore, removes the humanity of individuals. Each person will exist, not in their own right "in the image of God," but will be seen and judged on whether or not they are a state threat. The person who decides this is an unelected judge. Even if the benefits were enormous, I propose that many would rather live in a flawed democracy, than a perfect police-state.

Australia already allows for the observation, surveillance, and pre-trial detention of terror suspects. This represents an already significant security arsenal, and is a general framework that has not yet reached obsolescence (nor is it close).

It is OK for a policeman to view a man's mail, if there is reasonable suspicion regarding his activities. It is not OK for him to view everyone else's mail, with no exceptions and with a minimum of oversight, to find this person.

Since it does not address criminal motivations, will not be secure, will not help stop terrorists or criminals, and will transform Australia into a dark entity, it is my submission that this proposal for mandatory electronic and telecommunications data retention is irredeemably flawed and should not be considered as legislation by any government — Federal or State — under the sovereignty of the Commonwealth of Australia.