Response to discussion paper on electronic surveillance, by Glenn L. McGrath.

This partial response is solely based on my long term personal and professional interest in communications technologies, and its importance in facilitating trust.

1. Do the existing prohibitions and offences against unlawful access to information and data adequately protect privacy in the modern day ?

Protecting private information is increasingly difficult due to the commoditization of personal information, and digitisation of everything.

It is concerning that laws that exists to protect privacy may be effectively bypassed when information is gathered and made available by parties who are not be subject to Australian laws.

Lawful access to information and data should be consistent with that which can be lawfully gathered by the agency itself.

Harmonising laws between the states and the federal government is desirable, however consideration should also be given to how those laws relate to the importation of private information and data.

Problem Scenario: An app or program is installed by an Australian user, it gathers private information legally and exports it to another country, the data is then on-sold, and made available to Australian people or organisations who does not have lawful permission to gather that information.

There are competing goals between the commercialisation of personal data and protecting peoples right to privacy, an ideal solution would be one where users have control over who has and does not have access to their data prior to surveillance laws being used.

4. Do you agree with the proposed considerations for determining whether additional agencies should be permitted to access peoples' information and data? Are there any additional considerations that have not been outlined above?

Agencies should only be permitted to gather 'Information and data' on people suspected of committing a crime. Agencies should not be permitted to gather information on contacts of a suspect that are unrelated to the suspected crime.

Authorised agencies should limit the scope of private 'information and data' they seek to that which is related to the crime in which they are suspected.

Consideration should be given to the ability of an agency to be **publicly** accountable for their actions.

It is not enough to be privately accountable to adherence to these laws, maintaining trust with the public is essential in the long term to facilitate an agencies ability to covertly gather information.

- The passing of mandatory data retention laws resulted in a dramatic use of VPN's and encryption, because people don't trust law enforcement (or other 3rd parties) with their private information and data.
- Laws introduced to allow backdoors in software and services used by law-abiding citizens has also reduced trust in authorities and 3rd parties.

Weakening privacy laws further will surely result in increased privacy measure adopted by citizens, an escalation of the privacy arms-race between the government and its people.

5. Are there other kinds of information that should be captured by the new definition of 'communication'? If so, what are they?
6. Are there other key concepts in the existing framework that require updating to improve clarity? If so, what are they?
7. How could the framework best account for emerging technologies, such as artificial intelligence and information derived from quantum computing?

Communications should be defined in a technology-neutral manner, independently of the medium that facilitates it.

Mediums used to communicate other than 'electronic' include verbal (in person), written (on paper), physical (sign-language), visual (artistic), and probably others.

The labelling of this framework as specific to 'electronic' surveillance is burdensome, it suggests the need for surveillance of communications over an electronic medium differs to the need for surveillance over non-electronic mediums.

Where necessary, attributes of various mediums should be specified rather than referring to the name we give the medium, for example real-time communications, two-way, relayed, interpreted, broadcast.

e.g. What attributes of 'electronic surveillance' need to be addressed that distinguish it to other mediums.

Modern communications typically comprise a human oriented message, delivered by a machine, over an electronic medium, however both human and machines can comminate directly.

A distinction between the message and the carrier of that message is required to distinguish who is communicating, and who is carrying that communication.

The carrier of a communication should be treated as a different type of communication.

8. What kinds of information should be defined as 'content' information?
What kinds of information should be defined as 'non-content' information?
9. Would adopting a definition of 'content' similar to the UK be appropriate, or have any other countries adopted definitions that achieve the desired outcome?
10. Are there benefits in distinguishing between different kinds of non-content information? Are there particular kinds of non-content information that are more or less sensitive than others?

Distinguishing between different types of non-content is useful if different types of communications are recognised.

Content and Non-Content should be defined in a way that isolated it from the carrier of that content.

One type of non-content may be information about the end-party, a different type of content may be information about intermediate parties.

For example in layered communication, such as a VPN, non-content related to the end points of the communication should be recognised as a different type of non-content to intermediaries.

11. Should the distinction between ‘live’ and ‘stored’ communications be maintained in the new framework?
12. Do each of these kinds of information involve the same intrusion into privacy? Or should the impact of each be considered differently

The distinction should be between ‘delivered’ and ‘undelivered’ communications, rather than ‘live’ and ‘stored’, as a communication might be considered stored both before and after it has been delivered depending on the medium of delivery.

Undelivered communications should be considered more private. An old-school analogy would be between reading someones unopened and opened (snail-)mail, reading someones unopened mail should, be considered a greater intrusion into privacy.

Obtaining the content of undelivered mail should require extra consideration due to the greater breach of privacy.

13. What type of Australian communications providers should have obligations to protect and retain information, and comply with warrants, authorisations and assistance orders under the new framework?

Communications providers should be defined in a technology neutral manner.

Non-electronic providers such as Australia Post, Commercial Couriers and perhaps facilitators of in-person gatherings should also be recognised as communications providers (or communication carriers), and laws harmonised between them.

Justification should be provided where communication providers are treated differently under the law based on the medium of communication, with emphasis on the attributes of that particular medium that justify the distinction.

For example, should different laws apply if a message is sent via email, or a hand-delivered letter ?

The law should be principled rather than opportunistic, the cost of surveillance on different mediums should not influence the principles these laws seek to achieve.

If communications laws are stricter when using a modern communications medium, it creates an incentive to use old-fashioned communication methods, which might now considered more secure.