CHAIR—I am very interested in your portal for the reporting of e-crime. How extensive is it? Where have you done it before? How effective is it? How does it work?
CHAIR—So it does not just collect the data; it actually provides the person who has made the report with information about where they go? Does it actually refer the complaint, or does it just get back to them and say, 'You should go here,' or, 'You should go there'?
CHAIR—How is the cost of that process borne?

McAfee has proposed the establishment of an Australian e-security portal that provides a central gateway for reports to be made about incidents of cyber crime. The benefits of such a resource would include:

- a central place for receiving information from the public and then performing analysis to be used by law enforcement and regulatory agencies about specific cybercrime tactics used and potentially data to be used to arrest and prosecute offenders,
- the ability to coordinate a cross-jurisdictional response to cybercrime, and
- enhanced cyber crime intelligence overall about new and evolving cyber security threats that can be distributed to participating public and private sector parties (state police services, financial service providers, telecom service providers, and so on).

McAfee is not aware of an existing resource of this specific nature in Australia.

In the United States, McAfee developed a predecessor, of sorts, to this type of portal. In the United States, numerous authorities (including the Internet Crime Complaint Center (IC3), Federal Trade Commission (FTC), credit agencies and so forth) exist yet there is no *centralised* knowledge centre for victims to understand what types of assistance they need – from reporting intellectual property theft to identity theft to cyberbullying and auction fraud to how to request a fraud alert on their credit reports.

Known as the Cybercrime Response Unit (CRU) portal, it also houses a customised tool developed for the CRU by McAfee experts to evaluate a victim's online history at a cursory, non-intrusive level, and identify the online risky behaviour of which the victim may not have been aware. The scan performs a 'light' non-intrusive check of their PC to determine if they've visited malicious websites, their anti-virus is running and up-to-date, and other nominal checks. The scan then produces results and recommendations on what users can do to protect themselves from the specific threats identified. The site contains information about various cyber crime threats including identity theft, online fraud, scams, cyber bullying and provides safe transactional practices related to shopping, search, auctions, social networking use and other relevant matters. It is located at www.mcafee.com/cru

The objectives of the CRU are to:

- support victims of cyber crime by directing them to the appropriate law enforcement agency, credit reporting agency or complaints mechanism,
- provide valuable insights about today's online risks and how to improve their risk posture as a business or consumer to avoid becoming victims, and
- provide education about protection mechanisms such as free safe search software, the use of captchas, and other tools at their disposal.

McAfee provides both a preventative and a responsive approach to cyber crime through the CRU, as once victims use the online risk assessment and receive their feedback, they can call a McAfee specialist to answer further questions and guide them in reporting online crime.

McAfee provides all aspects of this portal: hosting the online help centre, providing an online scanning tool for identifying potential security threats for individual users, and providing CRU agents to help answer victim questions and clarify where to report the crime or request credit reports. The CRU is not intended to have investigative powers in its own right – rather it refers victims to the right agency for assistance and effective follow up.

In addition to providing victims with this portal, McAfee has developed a close working relationship with US and EU enforcement authorities including the Federal Bureau of Investigation (FBI) and the Serious Organised Crime Agency (SOCA), and shares intelligence with these agencies in order to ensure they not only have the latest threat information and advice, but also provides specific case support, and that the community is otherwise assisted in the most effective way.

The CRU is funded solely by McAfee.

McAfee has proposed a similar, but more advanced, e-security portal for Australian families and businesses. Like the U.S. CRU portal, the Australian portal would provide a central gateway for learning more about specific cyber threats and notifying appropriate agencies of incidents of cyber crime. But McAfee is willing to provide additional resources to ensure that law enforcement, financial service providers, and telecom service providers have the intelligence from this portal that they need to use the information effectively.

Centralising this reporting function could greatly enhance law enforcement's ability to respond to only the immediate crimes and not spend as much time fielding general questions and following information that is not necessarily in and of itself, an online crime or one in which no usable information is available.

McAfee believe government participation would be required to ensure it is an effective resource. This includes the, Australian Communications and Media Authority, Department of Broadband, Communications and the Digital Economy, Australian Federal Police, and other state and territory authorities).

McAfee has had very initial discussions with government and industry where it has advised of the proposal in broad terms and without seeking formal commitments at this early stage. However, McAfee intends to engage government and industry further to build on this proposal, and identify government and industry partners willing to formally participate in this important initiative.

CHAIR—You seem to suggest in your submission that Australia's investigation and prosecution of cybercrime could be improved. Do you want to provide any more details about that or any suggestions?

The challenge in relation to laws dealing with cyber crime is ensuring they keep pace with rapid changes, and that adequate resources are dedicated towards investigating and prosecuting the perpetrators of cyber crime. Much of this comes down to effective resourcing.

McAfee submits that a central e-security portal may assist in the reporting, investigation and successful prosecution of cybercrime by allowing for cross-analysis of victim reports across Australia's jurisdictions, combined with our Global Threat Intelligence of reputation-based scoring of cybercriminals and their websites globally, thus enabling more effective use of resources, quicker responses and better awareness of users overall.

While the portal provides the technical solution for reporting security breaches and finding out options for action when such incidents occur, collaboration between policing authorities at a federal and state level is also critical to ensure that suitable action is taken when a breach is reported. McAfee has not defined the specifics of these mechanisms and is open to guidance of other models that may

be useful for this scenario, including modelling the Queensland Police Service portal or others which the Australian government may find useful for this particular requirement.

In order for telecom service providers, in particular, to make effective use of the intelligence provided through this portal and other mechanisms, McAfee and telecom service providers recognise that safe harbour must be granted to these providers to be effective in chasing and taking down the operations of cybercriminals and their use of zombies and other tools to orchestrate cybercrime globally.

McAfee is active in its support of privacy initiatives such as Privacy by Design (www.privacybydesign.ca) and as such, intends to work with Australian authorities including the Privacy Commissioner to ensure such a portal would follow the best privacy practices available when gathering cybercrime victim data to assist in the analysis of the crime committed. It will be a fundamental necessity to ensure the utmost privacy protections to consumers or even businesses for the success of such a portal.

CHAIR—I would like to know, in respect of cloud computing, a little bit more about how it actually works. I have sort of an idea but not a clear one.

The topic of cloud computing – its many benefits and the precautions of retaining data in the cloud - is indeed one of great conversation globally. As such, McAfee has recently released a White Paper in October 2009, which explored the nature, risks and benefits of cloud computing. As companies and governments globally consider this option for their business needs, it is important to fully understand how to vet the companies with whom they choose to outsource to ensure the utmost security considerations are in place and regularly enforced and audited. McAfee includes numerous security best practices to assist in the decision-making process in the attached copy of the McAfee Cloud Computing whitepaper for the Committee's reference.