SUBMISSION NO. 51

Premier

Level 11, Executive Building, 15 Murray Street, Hobart TAS
GPO Box 123, Hobart, TAS 7001 Australia
Ph +61 3 6233 3464 Fax +61 3 6234 1572
Email Premier@dpac.tas.gov.au Web www.premier.tas.gov.au

Tasmania

31 JUL 2009

The Hon S Conroy MP
Minister for Broadband, Communications and the Digital Economy
Suite MG70
Parliament House
CANBERRA ACT 2600

Dear Senator Conroy Stephen,

I am writing in relation to the House of Representatives Standing Committee on Communications' (the Committee) Inquiry into Cyber Crime. I am pleased to provide the following submission from the Tasmanian Government.

By way of background, Tasmania Police is a relatively small organisation in national terms, comprising approximately 2.6 per cent of the total national policing resource and employing 1 252 sworn police officers, who serve the State's population of approximately 500 000 people.

Unlike larger jurisdictions, Tasmania Police does not have a centralised computer crime or major fraud area. Instead, such crimes are investigated by generalist detectives in the Criminal Investigation Branches across the State. The scale and resources of Tasmania Police limits its capacity for the specialist criminal investigation units that are a feature of many larger services.

Despite the absence of specialised units, in most areas Tasmania Police employs detectives with specific fraud and computer crime training and/or experience in the investigation of these crimes. These officers are supported by two full-time computer forensics officers, based in the Hobart Forensic Services area.

The above introductory comments provide the context for the following information that specifically addresses the inquiry's terms of reference.

a) ***Nature and prevalence of e-security risks including financial fraud and theft of personal information, including the impact of malicious software such as viruses and Trojans***

The extent of e-security offending in Tasmania is unable to be statistically determined due to difficulties in categorising the recording of e-security crime together with the under-reporting of offences.

CA 207936.

Tasmania Police's systems for recording reported crime are based on the crimes defined within the *Criminal Code Act 1924* (Tasmania) (the Act). Although the Act has been amended to include some specific computer crime offences, many of the offences committed by persons committing financial fraud or theft, including those facilitated by computer and communications technology, do not amount to such crimes, and are instead prosecuted as more traditional fraud offences or stealing. A consequence of such offending being 'mixed in' with general dishonesty offences is an inability to extract statistical data as to their incidence.

Further, anecdotal reports from Tasmania Police detectives indicate that the number of offences that fall within the scope of this inquiry are significantly higher than the official reports kept by police. Many victims of phishing-related offences report the matters to their banks, or other service providers in cases of non-bank phishing, but rarely do so to police. This is also true of many other computer-related crimes, such as unauthorised access to email accounts or other online services, especially in circumstances where the public believe there is little the police could do about the crime. Anecdotal evidence also suggests that many organisations, such as financial institutions, do not report every compromise they discover, or every compromise reported to them by customers, due to the reputational problems that widespread distrust in their electronic systems could produce.

Instances of malware infections are almost never reported, as most people now seem to accept this as a frustration inherent in computer use. Furthermore, it is doubtful whether police officers in any Australian jurisdiction would action such a report, as offences relating to malware tend to relate to its manufacture, use, or distribution, meaning individual end-user infections would rarely be considered to amount to an offence; many front line police would also consider such infections as an inherent part of computer use; and front line police officers generally are also untrained to deal with such complaints.

With regard to quantifying numbers of computer-specific crimes, during the 2007-08 financial year Tasmania Police received 58 reports of computer-related fraud and two reports of unauthorised access to a computer, while in the 2008-09 financial year 51 cases of computer-related fraud and five cases of unauthorised access to a computer were reported. However, as previously stated, these figures are considered to be unreliable indicators of the incidence of such crimes.

Anecdotal reports from Tasmania Police detectives indicate phishing-related offending, other online credit card fraud, and online action fraud are the complaints most commonly dealt with. Anecdotal reports, and information from other agencies involved in the investigation of phishing-related offences indicate that compromised data is now largely obtained through the use of malware, as opposed to the more traditional phishing emails and web sites.

b) The implications of these risks on the wider economy, including the growing economic and security impact of botnets

As the prevalence of cyber crime offending in Tasmania cannot be reliably determined, it is not possible to provide a reliable estimation of the impact on the wider economy, although some of the implications are obvious, such as actual theft and reputational damage to financial systems.

There are undoubtedly many malware infected computers in Tasmania that may include elements of botnets. However, Tasmania Police has not received any reports of botnet-related offences against Tasmanian entities, such as distributed denial of service attacks, nor any information indicating botnet offenders may be located in the State. Consequently no botnet-related investigations have been conducted.

c) Level of understanding and awareness of e-security risks within the Australian community

Anecdotally, Tasmania Police detectives indicate that although there appears to be a general awareness in the community of the need for some level of protection, such as that provided by anti-virus software, there is little understanding of the potential risks. As a result it is generally believed that most home and small business computer systems do not have adequate security, with very few having up-to-date security patches or anti-virus software.

d) Measures currently deployed to mitigate e-security risks faced by Australian consumers:

i) Education initiatives

Tasmania Police has not conducted any widespread educational campaigns, although from time to time particular issues have been highlighted by media releases. One example of this was the joint *'money mule'* media campaign with the Australian Federal Police and Australian Bankers Association, conducted in mid-2008.

The Tasmanian Office of Consumer Affairs and Fair Trading in the Department of Justice has produced some public education material in this area.

The Australian Competition and Consumer Commission appears to have been the most active in this space, however, it is likely that there has not been significant public awareness of this work. Anecdotal reports from Tasmania Police detectives indicate most consumers have very little awareness of cyber crime until they fall victim to it.

ii) Legislative and regulatory initiatives

There has been limited legislative reform within Tasmania in relation to e-security risks. However, in the last few years there has been some reform to enhance the investigative powers of Tasmania Police.

In 1999 the *Telecommunications (Interception) Tasmania Act 1999* (Tasmania) was passed to provide Tasmania Police with the ability to conduct telecommunications intercepts as part of serious criminal investigations. As a result of this legislation Tasmania Police now has the ability to utilise data communication intercepts, where necessary, in addition to the more traditional telephone intercepts. To date some data intercepts have occurred, but none have yet involved the investigation of e-crime related offences.

In addition, on 1 January 2009 the *Police Powers (Surveillance Devices) Act 2006* (Tasmania) commenced, providing Tasmania Police with the authority to utilise data surveillance devices in certain circumstances. Tasmania Police has not yet developed a capacity to deploy such devices.

As most e-security threats involve the use of communications technology, which is regulated by the Australian Government, the majority of legislative and regulatory reforms have been at this level.

iii) Cross-portfolio and inter-jurisdictional coordination

Between 2004 and 2006 Tasmania Police partnered with other Australian jurisdictions to form the Australian High Tech Crime Centre (AHTCC), which involved the out-posting of a Tasmania Police staff member to AHTCC. Since the closure of the AHTCC there has not been significant cross-jurisdictional coordination in relation to e-security risks.

Inter-jurisdictional coordination now rests with the Australian New Zealand Police Advisory Agency (ANZPAA). The Tasmanian Government is unaware of any significant developments in this area by ANZPAA at this point in time.

In the meantime coordination has largely occurred on a case-by-case basis. For example, the Tasmanian Government is aware that the Commonwealth Attorney General's Department has provided assistance to Australian law enforcement agencies with regard to obtaining information from foreign companies operating in Australia, such as Microsoft and Google, under the *Telecommunication (Interception and Access) Act 1979* (Commonwealth).

Queensland Police, in partnership with other jurisdictions including Tasmania Police, has also taken some initiative with regard to online auction fraud by providing a facility for complainants, regardless of jurisdiction, to report such matters online direct to the appropriate Australian police service.

Similarly, Tasmania Police has partnered with Victoria Police regarding telecommunication interception capacity, as the cost of implementing a stand-alone capacity was prohibitive. This partnership arrangement allows the use of Victoria Police infrastructure on a cost-recovery basis.

Pending the development of more formal coordination regarding e-crime issues, several Tasmania Police investigators have joined the AUSPOL email list, hosted by the Australian Computer Emergency Response Team. This list allows investigators involved in e-crime matters, in any jurisdiction, to post queries and information to their colleagues across the country.

Police services across Australia regularly cooperate with regard to criminal activities, and provide assistance or referrals to one another. Enlisting foreign cooperation tends to be more difficult however, and Tasmania Police makes regular use of Interpol where such assistance is required.

iv) International co-operation

Tasmania Police is not currently involved in any international activities with regard to e-security. Where necessary the Interpol network is utilised to request assistance, but success in this area has been limited. Many countries are not adequately positioned to provide assistance, or have domestic privacy laws that hamper information sharing. Even where formal mutual assistance provisions can be relied on, these have largely proved to be slow and ineffective with regard to e-crime issues.

In the past Tasmania Police has relied on the activities of other agencies, such as the Commonwealth Attorney General's Department and Australian Federal Police, to engage internationally on behalf of Australian law enforcement.

e) Future initiatives that will further mitigate the e-security risks to Australian internet users

Tasmania Police is currently not involved in the development of any future initiatives in this space. Although e-security risks do pose a serious problem for internet users, the current demand from the public, coupled with our limited specialist capacity in this area, have been unable to justify significant investment by Tasmania Police.

Tasmania Police believes that e-security issues can only be properly addressed at the national level. Many e-security issues affect consumers across Australia and internationally, and consequently it is not practical for State agencies to address them individually. Further, responses by individual states risks significant duplication of resources, which can be ill-afforded by small jurisdictions. This is especially the case with regard to highly technical problems such as those posed by the increasing criminal use of malware.

f) Emerging technologies to combat these risks

Tasmania Police is unable to contribute knowledge in this area.

The Tasmanian Government looks forward to learning the outcomes of the inquiry. Should there be any queries in relation to this submission the contact in Tasmania Police is Ms Sandra Lovell. Ms Lovell can be contacted by email at sandra.lovell@police.tas.gov.au or by telephone on (03) 6230 2461. For your information I have made arrangements for a copy of this submission to be forwarded to the Committee's Secretariat.

David Bartlett MP
Premier