Questions on notice from the House of Representatives Standing Committee on Communications

Inquiry into Cyber Crime

1. What is the effectiveness, uptake and upgrading of anti virus software and anti virus software services?

This question will be addressed by the Department of Broadband, Communications and the Digital Economy.

2. Does the current definition of criminality extend to embedded/latent functionality that can be activated by parties other than the technology owner in secret or to the detriment of the owner/user e.g. allegations/claims about Chinese broadband component vendors and BTs network upgrades?

Yes. Sections 477.1 (unauthorised access, modification or impairment with intent to commit a serious offence), 477.2 (unauthorised modification of data to cause impairment) and 478.1 (unauthorised access to, or modification of, restricted data) of the *Criminal Code Act 1995* (Cth) would cover a person exploiting inbuilt vulnerabilities in technology without the owner's knowledge. Sections 477.2 and 478.4 (producing, supplying or obtaining data with intent to commit a computer offence) could potentially cover deliberate placement of vulnerabilities in certain circumstances, such as a rogue employee placing a flaw in a program that with the intention of allowing criminals to exploit that flaw to steal data. However, it would not cover a computer program that was poorly made. Section 474.6 (interference with facilities) could potentially cover a person operating a device that results in the hindering of the normal operation of a carriage service.

Section 311 of the *Telecommunications Act 1997* outlines that carriers and carriage service providers must do their best to prevent telecommunications networks and facilities from being used to commit offences. Additionally, carriers and carriage service providers must also give the authorities such help as is reasonably necessary for the purpose of (a) enforcing the criminal law and laws imposing pecuniary penalties; and (b) protecting the public revenue; and (c) safeguarding national security. These requirements include giving help to execute warrants under the *Telecommunications (Interception and Access) Act 1979*.

3. To what extent does the current legal framework and the Government's stated policy ambition for 'achieving a just and secure society' support the personal security of individuals hurt by the use and application of ICT. In responding to this question, the Department(s) should focus on the current limitations of the law (i.e. unauthorised access to and modification of data) and apparent lack of safeguards to protect individuals from:

Information is provided below in response to the Committee's questions regarding the potential application of current criminal law to the various kinds of conduct of concern to the Committee raised in question 3.

We note, however, that there are also other avenues that could be utilised to address the conduct, other than criminal prosecution. These include, generally, classification regimes, defamation or breach of confidence lawsuits. Information on some of these areas is provided for the information of the Committee below, where they are specific areas of responsibility for AGD. AGD notes that

the information provided is in relation to Commonwealth law only – other avenues may be available under the relevant State or Territory laws.

AGD also notes that some of these issues relate more so to the Australian Government's programs for cyber-safety, for which the Department of Broadband, Communication and the Digital Economy is the responsible Australian Government agency.

Section 474.17 of the *Criminal Code Act 1995* (Cth) criminalises the use of a carriage service to menace, harass or cause offence. The maximum penalty for this offence is three years imprisonment. Section 474.17 is an offence of broad application and would generally cover online conduct such as stalking, bullying and harassment.

Section 474.14 of the Criminal Code criminalises the use of a telecommunications network with intention to commit a 'serious offence'. A serious offence is a Commonwealth, State or Territory offence with a maximum penalty of five or more years imprisonment. The maximum penalty for the offence in section 474.14 is determined by reference to the maximum penalty of the 'serious offence'. Similarly, section 474.14 is a broad offence that would generally cover the use of the Internet for conduct such as fraud or stalking.

Section 474.15 of the Criminal Code criminalises the use of a carriage service to make a threat. The penalty for this offence is determined by the nature of the threat that is made. Where a person has made a threat to kill, the maximum penalty is 10 years imprisonment; a threat to cause serious harm is punishable by a maximum penalty of seven years imprisonment.

Sections 474.19, 474.20, 474.22 and 474.23 of the Criminal Code provide criminalise dealing with child pornography or child abuse material online. The maximum penalty for these offences is 10 years imprisonment.

Section 477.1 of the Criminal Code criminalises the unauthorised access, modification or impairment or data with intent to commit a 'serious offence'. A 'serious offence' is a Commonwealth, State or Territory offence with a maximum penalty of five or more years imprisonment. The maximum penalty for the offence in section 477.1 is determined by reference to the maximum penalty of the 'serious offence'. Again, section 477.1 is a broad offence that would generally cover the use of the Internet for conduct such as fraud or stalking where it involves intrusion into a personal computer.

Section 478.1 of the Criminal Code criminalises the unauthorised access to or modification of data held on a computer which is restricted by an access control system. The maximum penalty for this offence is two years imprisonment. The offence in section 478.1 would generally cover hacking into password protected data, such as a Facebook account, and/or modifying that data.

Persons who suspect that such an offence may have occurred should refer the matter to the Australian Federal Police for investigation.

a. having identities assumed or created often involving new or manipulated images;

b. the distortion of the individuals personal interests, reputation or character;

AGD has participated in programs to raise awareness of the dangers of online identity theft, including the development of an ID theft kit and participation in the Australian Consumer Fraud Taskforce and ScamWatch initiatives. The Commonwealth, States and Territories are consulting to

publicise the dangers of identity crime and ensure that agency education programs use consistent messages based on up to date research and other information.

However, AGD has identified certain limitations in the current arrangements:

1. Understanding the identity crime threat

The capacity of government agencies to develop a targeted response to online identity crime is limited by a lack of detailed information. This means that statistics do not provide meaningful information on the type of identity crime, including whether it was conducted in the digital or real worlds; and makes comparison of data sets from different sources and across jurisdictions difficult.

Improvements are underway with the recent identity crime offences being implemented as a result of the Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General (MCLOC) Final Report on Identity Crime. On 23 February 2009 the House of Representatives passed the Law and Justice Legislation Amendment (Identity Crimes and Other Measures) Bill 2008. The Bill is expected to be debated in the Senate in the second half of this year. The Bill implements the model identity crime offences and victims' certificate provisions recommended by the MCLOC.

The Bill inserts three new identity crime offences into the new Part 9.5 of the Criminal Code. With the exception of South Australia and Queensland, it is not currently an offence in Australia to assume or steal another person's identity, except in limited circumstances.

The offences include:

- dealing in identification information with the intention of committing, or facilitating the commission of a Commonwealth indictable offence, punishable by up to five years imprisonment
- possession of identification information with the intention of committing, or facilitating the commission of, conduct that constitutes the dealing offence, punishable by up to three years imprisonment, and
- possession of equipment to create identification documentation with the intention of committing, or facilitating the commission of, conduct that constitutes the dealing offence, punishable by up to three years imprisonment.

The identity crime provisions also contain measures to assist victims of identity crime. The amendments will allow a person who has been the victim of identity crime to approach a magistrate for a certificate to show they have had their identity information misused. The certificate may assist victims of identity crime in negotiating with financial institutions to remove fraudulent transactions, and other organisations such as Australia Post, to clear up residual problems with identity theft.

Victoria has recently introduced similar legislation into its parliament. South Australia and Queensland are the only two jurisdictions that currently provide for similar offences.

Equally, it is likely that an accurate picture of the scale of identity crime is hampered by inadequate reporting practices. In particular, it is clear that only a proportion of crimes are reported to police, while a larger proportion are reported to financial institutions. However, what is not known is how many crimes go unreported, nor how many victims of identity crime remain unaware that they have been victimised.

2. Support of ID theft victims

Supporting the victims of crime is more straightforward in cases of simple identity theft, such as the theft of credit card details. In Australia, victims generally suffer limited direct financial losses as costs are often covered by the financial institution under the Electronic Funds Transfer (EFT) Code of Conduct. Further damage is prevented by speedy action to cancel cards or stop accounts.

However, providing support to victims of more complex identity theft is more difficult. These more complex cases typically involve the use of various techniques, often computer based, to collect a range of identity information about the victim. This information can then be used for a wide range of criminal purposes including:

- creating false identities, which can involve applying for new credentials, such as driver's licences or opening bank accounts
- supporting serious criminal activities, including terrorism, money laundering, fraud, tax evasion, drug importation or people smuggling.

c. 'broadcasting' of personal data that is inaccurate, offensive, profoundly disturbing or intentionally damaging;

d. the use of ICT to bully or intimidate another party to act in a manner contrary to their will, free choice or interests, and/or

e. malicious and intentionally hurtful campaigns of retribution or character diminishment with no public interest or freedom of speech value.

Films, computer games and publications are classified under the National Classification Scheme (NCS), a cooperative scheme between the Commonwealth and the States and Territories. The Scheme is based around core principles:

- adults should be able to read, hear and see what they want
- minors should be protected from material likely to harm or disturb them, and
- everyone should be protected from exposure to unsolicited material that they find offensive.

Content broadcast over television or radio is regulated under the *Broadcasting Services Act 1992* (BSA). The dissemination of content online, or over convergent devices, such as mobile phones, is regulated under Schedules 5 and 7 of the BSA with reference to classification categories under the NCS.

Under the BSA, content available online or delivered over convergent devices, such as mobile phones, will be 'prohibited content' if it has been classified or is likely to be classified X 18+ or RC (Refused Classification) or R 18+ and it is not subject to a restricted access system. Content will also be prohibited if it has been classified or is likely to be classified MA 15+ and is provided on a commercial basis (i.e. for a fee) unless it is subject to a restricted access system. A restricted access system is a service that prevents persons under a particular age from accessing certain content.

The Australian Communications and Media Authority (ACMA) can take action to limit the accessibility of 'prohibited content' in Australia:

- either by issuing a take-down notice to the content service provider if based in Australia, or
- by arranging for the content to be filtered if the content is not hosted in Australia

Prohibited content is limited to content that has been classified or is likely to be classified Refused Classification or X18+ or has been classified R18+ or MA15+ without an appropriate restricted access system. A website reporting views that are racist but which do not specifically urge violence against another group of people would not be prohibited.

If ACMA considers that overseas hosted content is prohibited it must notify the content to Internet service providers so that the providers can deal with the content using technical means such as filtering technology.

Complaints about online content are made to ACMA. ACMA must refer content hosted in Australia to the Classification Board for classification if it considers the content is substantially likely to be prohibited.