Supplementary Submission No. 44.2

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

Inquiry into Cyber Crime

Civil Legal Liabilities

(Question taken on notice during the Committee hearing of 25 November 2009)

What is the potential for individual civil liability arising from a failure to remediate an infected PC causing nuisance to other Internet users?

The question of whether there is a potential for individual civil liability arising from a failure to remediate an infected PC which causes a nuisance to other Internet users is a matter of State and Territory law and it would not be appropriate for the Attorney-General's Department (AGD) to provide legal advice on the issue.

Private Sector Sharing Information with Government

1. The Cyber Security Strategy emphasises the business-government partnership. Symantec has pointed out that global IT companies have vast amounts of intelligence on Internet activity that is vital to the early warning and response capability of governments. The US has legislated (Critical Infrastructure Information Act 2002; Protected Critical Infrastructure Information Program) to give the private sector confidence that privacy and business sensitive data provided to government is protected:

a. How is the private sector's sensitive intelligence data protected from disclosure or possible use by regulatory authorities?

The Australian Government (the Government) places a high priority on protecting information provided in confidence by the private sector. Government officials who are provided with such information are bound by statutory and other legal and policy obligations for information handling. These include section 70 of the *Crimes Act 1914* (Cth) which deals with disclosure of information by Commonwealth officers, the Australian Public Service Code of Conduct set out in the *Public Service Act 1999* (Cth) and the Government's Protective Security Manual.

Government participants in business-government information sharing mechanisms such as the Trusted Information Sharing Network for Critical Infrastructure Protection (TISN) and the trusted cyber security information exchanges are specifically made aware of these obligations by signing a Government Representative Confidentiality Acknowledgement. In doing so, they acknowledge their legal obligations to retain the confidentiality of information and the penalties (which include criminal sanctions) that they may be subject to if they breach these confidences.

Private sector organisations that participate in these fora are expected to adhere to the terms of confidentiality agreements which set out their obligations regarding the use of confidential and commercially sensitive information provided either by Government or other private

sector stakeholders. This ensures that information is properly managed and reasonably protected from unauthorised disclosure or use.

Information that is provided to Government within the TISN is used for legitimate TISN purposes only. This information is not disclosed to other regulatory agencies, unless required by law. In such cases, the owners of the information would be given prompt notice and reasonable details of the circumstances involved should they wish to respond.

b. Is there value in adopting a specific and visible legislative regime to build private sector confidence in the Australian cyber security model?

AGD does not consider that further legislation is required in this area. Government employees are subject to statutory and other legal obligations which carry criminal and other sanctions for improper disclosure of information. In addition, the use of non-disclosure agreements for non-government organisations, which provide legal remedy in the event of a possible breach of confidentiality, often provides adequate protection for private sector information. The level of private sector participation in fora such as the TISN over recent years suggests that the vast majority of private sector stakeholders are comfortable with the current arrangements.

<u>Powers to implement technical responses to attack</u>

2. What, if any, legal impediment is there to taking ISP and Australian wide network wide action to combat malicious viruses? For example, what legal impediment is there (if any) to releasing software designed to disinfect PCs invaded by a widely distributed virus?

Part 10.7 of the *Criminal Code Act 1995* (Cth) contains offences that could cover the release of software designed to disinfect PCs invaded by a widely distributed virus if the software causes unauthorised access to or modification of data – for example, if it operates without the owner's consent.

For the offences in Part 10.7 to apply, the conduct in question must involve either a Commonwealth computer or the use of a carriage service (such as the Internet). In other cases, the conduct must be dealt with under relevant State or Territory legislation.

Under section 477.1, it is an offence to access, modify or impair data on a computer without the authorisation of the owner, with the intention of committing a serious offence. A serious offence is a Commonwealth, State or Territory offence with a maximum penalty of five or more years imprisonment. A person who is found guilty is punishable by a penalty not exceeding the maximum penalty of the serious offence.

Section 477.2 is intended to address the unauthorised modification of data on a computer that would impair access to, or the reliability, security or operation of the data – for example, by using the internet to embed software in a PC without the consent of the owner. This offence carries a penalty of 10 years imprisonment.

Section 477.3 criminalises the unauthorised impairment of electronic communication. It applies where a person causes any unauthorised impairment of electronic communication to or from a computer, knowing that the impairment is unauthorised. This offence is punishable by a maximum penalty of 10 years imprisonment.

Prosecutions

3. How many prosecutions and what sentences have been achieved under Part 10.6 and Part 10.7 of the Criminal Code Act 1995?

Please see statistics at Appendix A.

ISPs and Investigations

4. The AFP has said some telecommunications carriers are unable to provide accurate timely data and lack the capacity to discharge their obligations under the *Telecommunications (Intercept and Access) Act 1979*:

a. What steps will be taken by CERT Australia to ensure that the hundreds of ISPs in Australia are aware of and have the capacity to meet their legal obligations?

CERT Australia will not perform a regulatory role with Internet service providers (ISPs).

The responsibility for advising ISPs on their obligations under the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act) rests with AGD's Telecommunications and Surveillance Law Branch (TSLB). TSLB administers the TIA Act which enables law enforcement agencies such as the Australian Federal Police (AFP) to access telecommunications data from carriers. This information includes subscriber details, call log details and IP addresses.

The TIA Act creates a statutory position known as the Communications Access Co-ordinator (the CAC). The CAC is the first point of contact for both the telecommunications industry and law enforcement and national security agencies in relation to access to telecommunications information. The role of the CAC is currently performed by the First Assistant Secretary of the National Security Law and Policy Division in AGD.

TSLB supports the role of the CAC and is responsible for liaising with the telecommunications industry, providing education and ensuring compliance with the obligations imposed on industry by the TIA Act. To assist industry to comply with their obligations, they are required to provide an interception capability plan on an annual basis which is assessed by law enforcement and national security agencies before being approved by the CAC. These plans outline how industry will meet their obligations under the TIA Act. The plans for 2009 have been approved and carriers range from very large organisations such as Telstra or Optus to smaller operators like Clear Networks. While some carriers have less capability, the CAC works with carriers to ensure they improve their capabilities as they grow their business.

TSLB also administers an outreach program which provides extensive liaison and education for industry. The program involves the provision of legal advice to industry on their obligations under the Act. Additionally, TSLB provides face to face assistance for carriers, carriage service providers and ISPs. These programs enable AGD to assist industry meet their obligations under the legislation and provide a foundation of co-operation in the provision of assistance to law enforcement.

The responsibility for advising ISPs on their broader regulatory obligations under telecommunications legislation rests with the Australian Communications and Media Authority.

International Cooperation

5 The AFP has said it can sometimes take up to 18 months to get information and intelligence for forensic data analysis from overseas ISPs:

a. Would Australia's participation in the Council of Europe Convention on Cyber Crime help improve the speed of investigation cooperation?

There are several mechanisms available to law enforcement officers to obtain information and evidence from foreign countries. Mutual assistance is a formal government to government process for providing and obtaining assistance in criminal investigations and prosecutions, and in proceedings to recover the proceeds of crime.

Police-to-police assistance is direct cooperation that is provided by one country's police force to the police force of another country. Police-to-police assistance is often used in the investigation stage of a law enforcement operation, or to obtain general intelligence or information that would not require the exercise of coercive powers.

The timeframe for completing mutual assistance requests varies significantly in each case. It will depend on the type of assistance which is the subject of the request as well as the laws and processes for mutual assistance in the other country and applicable treaty requirements. Timeframes can vary from a few days or weeks in very urgent or less complex cases, to several months or years in cases which require the collection of extensive material, or which relate to complex investigations. In contrast, requests for police-to-police assistance can sometimes be actioned much more quickly.

Australia can make a mutual assistance request to any country. However, in the absence of a treaty, whether the request is accepted will depend on the domestic laws of the country. Australia has over 25 bilateral mutual assistance treaties and is party to a number of multilateral conventions which contain provisions to facilitate mutual assistance between parties. Participation in the Council of Europe Convention on Cybercrime (the Convention) would further enhance Australia's ability to obtain international assistance from other parties to the Convention in investigating potential cybercrime offences, particularly in relation to accessing telecommunications.

b. Has there been a detailed review of the international mutual assistance legal regime to ensure current arrangements are comprehensive, up to date and responsive to the phenomena of online crime?

AGD has conducted a comprehensive review of Australia's mutual assistance and extradition laws. An exposure draft of the Extradition and Mutual Assistance in Criminal Matters Legislation Amendment Bill was released for public consultation in July 2009. A key intent of the reforms in this Bill is to streamline and modernise Australia's laws to ensure the mutual assistance regime is able to respond to advances in technology.

The Bill includes a number of proposals that would assist in gathering evidence in electronic form. For example, the Bill would enable Australian authorities to apply for a warrant to covertly access stored communications (such as email records) for foreign law enforcement purposes. This type of assistance is currently only available for domestic law enforcement purposes.

The Bill would also streamline the processes for providing other types of assistance to foreign countries. For example, existing telecommunication data, such as subscriber details and call charge records, can currently only be disclosed for foreign law enforcement purposes following receipt of a formal mutual assistance request from the foreign country. This process can be time-consuming. The Bill would remove the need for the foreign country to provide a mutual assistance request, instead enabling existing telecommunications data to be provided to a foreign law enforcement agency on a police to police basis.

The Government is considering submissions made in response to the exposure draft legislation, with a view to developing final reform measures for inclusion in a Bill to be introduced into Parliament.

c. To what extent does Australia's existing mutual assistance in criminal matters regime match the obligations of the Council of Europe Convention on Cyber Crime and what, if any, gaps are there?

Australia is able to meet some of the obligations under the Convention with respect to international crime cooperation through the existing mutual assistance regime. The exposure draft Bill included amendments which would further enhance Australia's ability to meet other obligations under the Convention (see response to part (b) above). The Government is assessing whether any additional changes would be needed to domestic legislation in order to meet the international crime cooperation obligations in the Convention.

<u>Evidence Gathering, Analysis and Admissibility</u>

6. The growth in cyber crime; increased reporting and full disclosure will increase the volume of data to be analysed by police. Encrypted data is a special obstacle:

a. How is the Government going to ensure that the AFP has the tools/systems necessary to store, review and analyse digital data?

The AFP continues to review work practices, technologies and engagement with industry to ensure it is in a position to advise on its needs now and into the future. The AFP has significant investment in networked analysis capacity across AFP offices. This capability is scalable and will continue to be developed in line with operational experience of technology use. The AFP is active in its exploration of science and technology for law enforcement purposes and brings forward proposals for Government's consideration where appropriate.

The Government has provided funding to assist in the analysis of data by the AFP under a number of New Policy Initiatives (NPIs).

The Enhanced Technical Surveillance NPI and the Maintaining Telecommunications Interception NPI provide funding for the AFP to collect data under the TIA Act and the *Surveillance Devices Act 2004* (Cth).

The E-Security National Agenda NPI will build investigative capacity to pursue cyber crime offences that have the potential to disrupt the national information infrastructure and critical infrastructure, including through enhancing technical tools and skills.

Under the Cyber-Safety NPI, the AFP is increasing research into the evolving digital landscape and emerging threats to better predict trends and capabilities. Additionally, work is being undertaken to develop and implement an Australian National Victim Image Library and a Child Exploitation Tracking System.

Under the Fighting Terrorism at its Source NPI, the AFP works to enhance its Australian based and regional criminal intelligence capacity. This incorporates intelligence tools developed and interconnected with the AFP information management system to enhance ability of intelligence teams to collect, collate, analyse and exploit intelligence.

7. The *Crimes Act 1914* (s.3LA) enables police to obtain a magistrate's order to compel a person to give police passwords and decryption keys:

a. Is the penalty of 6 months for refusing to assist police by giving them a password or decryption key a sufficiently strong penalty to achieve compliance with the order?

It is currently an offence under the *Crimes Act 1914* (Cth) for failing to provide assistance as is reasonable to a law enforcement officer to access data stored on a computer at a search warrant premises (for example, where the data is encrypted or password protected). The offence carries a maximum penalty of six months imprisonment. However this penalty is not sufficient when compared to the terms of imprisonment a person may be subjected to if the encrypted data provided evidence the person had committed a computer or other offence.

The Crimes Legislation Amendment (Serious and Organised Crime) Bill No. 2 will amend this offence by, among other things, increasing the applicable maximum penalty from six months to two years imprisonment. Given the serious nature of many of the offences for which assistance may be needed, it is appropriate that the penalty for failing to comply with an assistance order is increased to this level.

8. The NSW Police have argued that remote access under warrant would allow for surveillance at the point before encryption:

a. What are policy issues need to be considered in relation to this type of surveillance?

b. Is the matter currently under active consideration or is there any intention of doing so in the near future?

The issue of remote access under a warrant has been raised with AGD. This type of surveillance raises a number of complex legal, technical and privacy issues.

The use of surveillance technology in this manner needs to be considered against the existing legislative framework. It is necessary to ensure that remote surveillance does not amount to interception which is regulated under the TIA Act, rather than existing State and Territory and Commonwealth surveillance regimes. Other legislation such as the *Criminal Code Act 1995* (Cth) is also being considered in this context.

Further consideration of the existing surveillance legislative regime is also being undertaken. The TIA Act provides for a national regime in regards to a highly intrusive investigative power. However, the *Surveillance Devices Act 2004* (Cth) does not provide such a national regime. Accordingly, jurisdictional issues arise in the use of these types of surveillance powers where they can be deployed from one jurisdiction into another or to multiple jurisdictions.

The Telecommunications and Surveillance Law Branch of AGD currently has a working group which includes members from New South Wales law enforcement bodies, government and other relevant stakeholders to consider issues such as these.

9. The AFP have identified the need to 'demonstrate the chain of evidence handling of digital media' to meet court requirements' and the 'lack of an Australian wide standard for the display of electronic evidence to court' as two challenges to the prosecution of cyber crime (Response to QN 6b):

a. What special challenges does digital evidence pose for the prosecution of computer related crimes (legal and practical) in Australian courts?

Cyber crime, like other forms of crime, must be established by admissible evidence. This includes proving continuity of the digital evidence by presenting evidence of the chain of handling. Such evidence may be detailed given the involvement, for example, of computer forensic analysts, but this forms a necessary part of proving matters before criminal courts.

Presenting digital evidence to courts presents its own challenges and, like other forms of technical evidence, must be explained to the court by an expert witness. This process may be assisted by the use of aids such as diagrams and charts or electronic evidence setting out in detail the steps involved in the electronic processes. The way that evidence is presented may vary depending on the factual circumstances involved in the particular matter and the legal and evidentiary issues raised in that matter.

Digital evidence may give rise to issues regarding the practical handling of large volumes of complex material and the time taken to conduct the necessary analysis. There may also be issues such as dealing with and presenting evidence that has been subject to encryption.

b. Is the manner in which digital data is admitted the same in all the States and Territories? If not, what steps need to be taken to promote harmonised rules of evidence and court procedures?

Generally, the requirements for admissibility are prescribed by the evidence laws of the jurisdiction in which the proceedings are held. A number of jurisdictions have adopted a harmonised approach to evidence law, under the Uniform Evidence Acts regime developed through the Standing Committee of Attorneys-General (SCAG). This includes the Commonwealth, New South Wales, Victoria (once recently passed legislation commences), Tasmania, the Australian Capital Territory and Norfolk Island. SCAG oversees the implementation of the Uniform Evidence Acts and has an ongoing role in the harmonisation of evidence laws.

10. To prosecute a person running a botnet, police would need statements from potentially thousands of individuals that the perpetrator did not have authority to enter and operate their machine:

a. How is the criminal law going to respond to this practical issue, and what methods might be adopted that would make it easier for the prosecution to discharge the evidential burden in such cases?

Alleged conduct regarding the use of a botnet may give rise to consideration of a range of offences, which will govern the evidence required for the purposes of a prosecution. In some cases, it may not be necessary to provide evidence in relation to every compromised computer. For example, it may be possible for the Commonwealth Director of Public Prosecutions (CDPP) to prosecute on the basis of representative charges which establish a course of conduct by the defendant together with forensic evidence to show how the botnet operated.

11. The NSW Police has suggested that proof of evidence would be facilitated if records from e.g. Microsoft and Gmail, which are 'business records' can be admitted in court by 'information and belief' rather than strict proof and witness evidence:

a. Is this an issue the Department has considered?

AGD's International Crime Cooperation Central Authority (ICCCA) works closely with the United States Department of Justice to ensure evidence obtained from ISPs through mutual assistance processes complies with the legal requirements for the admission of business records into evidence in Australian domestic proceedings. ICCCA has extensive experience dealing with its United States counterpart to facilitate requests for business records and considers that the majority of ISPs demonstrate a high level of cooperation and provide material within reasonable timeframes taking into account the requirements of US domestic law.

AGD is aware of concerns about the difficulties in adducing business records, such as internet records, obtained through mutual assistance into Australian domestic proceedings. Part 3 of the *Foreign Evidence Act 1993* (Cth) provides a means of adducing foreign evidence, obtained through mutual assistance, into Australian criminal proceedings. The Foreign Evidence Amendment Bill 2008, which is currently before the Senate, seeks to streamline the requirements for adducing foreign business records as evidence in Australian proceedings. The Bill would not enable business records to be admitted into court by 'information and belief'. However, the Bill would provide further flexibility in the testimony requirements that apply to foreign evidence adduced pursuant to the Act.

b. What are the pros and cons from a criminal law and law of evidence point of view?

Laws governing the admissibility of foreign evidence must strike an appropriate balance in ensuring safeguards are in place to protect individual rights, while providing sufficient flexibility in the law and judicial discretion to enable responsive and flexible measures in securing international crime cooperation.

Police Training

12. The NSW Police has suggested a Cyber Crime University or Cyber Crime Training Institute for law enforcement authorities and perhaps other arms of government:

a. What steps is the Federal Government taking to ensure that Australian police forces have access to effective training in the investigation or online crime?

The AFP also offers positions on various electronic crime based training courses to other Commonwealth and State and Territory law enforcement agencies. This includes the AFP's:

- Internet Policing Program which provides training in the tactical use of the internet including online conversations with suspects and advanced internet search techniques;
- Child Protection Operations workshop which provides training for investigating and managing of online child sex offences and child sex tourism internationally with a focus on the nexus between international law enforcement, the AFP and state and territory police; and
- Management of Serious Crime course, a multi-agency, multi-jurisdictional program provided to a range of senior law enforcement practitioners across the Commonwealth and the States and territories that includes a focus on cyber crime investigations.

The AFP is establishing a Technology Enabled Crime Centre of Excellence within its High Tech Crime Operations portfolio. This Centre brings together technical, legal and other subject matter experts to provide the AFP and its partner agencies with a single point of contact on issues of technology enabled crime. The Centre is being formed in recognition of the increasing complexity of technology enabled crime and the need to deliver contemporary, specialist advice to investigators working on these matters.

In June 2009, the AFP hosted the Australian High Tech Crime Conference in partnership with the University of Technology, Sydney and the Australian Institute of Criminology. The conference brought together cyber crime experts to establish and maintain links between law enforcement, the judiciary, the legal fraternity, academia, industry experts and government officials. The conference was successful in sharing information, ensuring a dialogue on key challenges, addressing investigative techniques and discussing legal and legislative issues relating to technology based crimes. The AFP will continue to host this conference annually.

Policy Coordination with States and Territories

13. What is the Government's view of the suggestion by NSW that a National Cyber Crime Working Group be established to inform cyber crime policy? The proposal is to include prosecutors, policy developers, members of the private sector, and police including AFP High Tech Operations.

The Government agrees that greater cooperation and coordination between the Commonwealth and States and Territories on cyber crime would be beneficial and is supportive of the concept of a National Cyber Crime Working Group. The proposal was originally put forward by New South Wales but following the National Justice CEO's meeting on 5 November 2009, it is now being further scoped by Victoria, in consultation with the Commonwealth and the other States and Territories. This is important to ensure that such a working group does not duplicate work already being undertaken by the Commonwealth, including in consultation with other parts of State and Territory governments. The proposal is to be considered by SCAG in April 2010.

Unauthorised installation of spyware or other software

14. The Cyber Space Law and Policy Centre has said the legal regimes covering cyber crime are complex and convoluted, and the installation of unwanted software without the user's informed consent is not expressly illegal in Australia:

a. Is it a crime to install software without the informed consent of the PC owner?

Part 10.7 of the *Criminal Code* (Cth) contains Commonwealth offences which criminalise the misuse of computers. These offences would generally apply in cases where software, such as spyware, is installed in a PC without the owner's informed consent.

For Part 10.7 offences to apply, the conduct in question must involve either a Commonwealth computer or the use of a carriage service (such as the Internet). In other cases, the conduct must be dealt with under relevant State or Territory legislation.

The offences that apply under Part 10.7 focus on the result of the conduct by defendant, rather than the nature of the conduct itself. Therefore, the conduct described above may be covered by one of several offences under Part 10.7.

Under section 477.2, it is an offence to modify data on a computer without the authorisation of the owner in a manner that would impair access to, or the reliability, security or operation of the data – for example, by using the internet to infect a computer with spyware. This offence carries a penalty of 10 years imprisonment.

Section 477.1 covers unauthorised access, modification or impairment of computer technology where the offender does so with the intention of committing a serious offence. A serious offence is a Commonwealth, State or Territory offence with a maximum penalty of five or more years imprisonment. A person who is found guilty is punishable by a penalty not exceeding the maximum penalty of the serious offence.

It may also be an offence under Part 10.7 to prepare to engage in any of the above conduct. It is an offence under section 478.3 to possess or control data with intent to commit a computer offence under Division 477. For example, it would be an offence under this section to possess spyware with the intention of impairing the security of data, even if the spyware was never installed. This offence is punishable by a maximum penalty of three years imprisonment

It is also an offence under section 478.4 to produce, supply or obtain data with intent to commit a computer offence under Division 477. This offence is designed to cover the

production and/or supply or data to be used in a computer offence. This offence is punishable by a maximum penalty of three years imprisonment.

High level policy advice to Government

15. Some IT vendors have suggested a Cyber Crime Advisory Group to bring knowledgeable stakeholders into high level dialogue on policy development:

a. Is there any reason why a Ministerial Advisory Committee on Cyber Crime should not be established?

The Government has a range of mechanisms for consulting with private sector, academic and other stakeholders on cyber security issues, including:

- the TISN which includes an Information Technology Security Expert Advisory Group (ITSEAG). The ITSEAG provides support and guidance on emerging and future medium to long term IT security issues impacting Australia's critical infrastructure. Its membership includes representatives of major IT vendors, academics and other industry stakeholders such as the Australian Computer Society

- the trusted cyber security information exchanges that have been conducted under the auspices of AGD's GovCERT.au team. From 2010 these will be conducted by CERT Australia, and

- a range of memoranda of understanding and other bilateral agreements with major vendors and tertiary education institutions for the sharing of information and provision of advice and assistance on cyber security issues.

CERT Australia will build on these mechanisms in further engaging vendors, ISPs and other IT and broader industry stakeholders in its role as the Government's coordination point for the coordination of information exchange between the Government and the private sector on cyber security issues.

The Government also consults widely in major reviews of cyber security policy, for example the 2008 *E-Security Review*. The AGD-led review team conducted targeted consultations with a range of private sector, academic, state and territory and Commonwealth stakeholders. These consultations were one of the key inputs into the review which in turn informed the development of the Government's Cyber Security Strategy.

At the ministerial level, the Attorney-General chairs the Business Government Advisory Group on National Security. This is a high level group of CEOs and other business leaders which considers a range of issues relevant on national security, including cyber security.

The question of whether a further Ministerial Advisory Committee on Cyber Crime is required is a matter for the Attorney-General.

Judicial Education

16. Several witnesses have raised the issue of judicial and prosecution education about cyber crime:

a. What action is planned to increase the level of knowledge about the nature and seriousness of online crime?

The Government's Cyber Security Strategy highlights legal and law enforcement issues as one of seven strategic priorities to be pursued. As suggested in earlier answers five and twelve, this is a multi faceted process. The Government is undertaking a range of measures to maintain an effective legal framework to prosecute cybercrime. This includes providing the legal profession with access to information and resources to provide them with the requisite level of technological knowledge and understanding to effectively administer these laws.

For example, specialised training for police prosecutors is currently being conducted by the AFP and the CDPP.

AGD is consulting with a range of stakeholders, including the AFP, CDPP, the Courts, the Judicial College of Australia and law societies to scope the requirements of each target group and identify suitable programs for implementation.

Appendix A

The following Tables represent the number of prosecutions and penalty types under Part 10.6 and 10.7 of the *Criminal Code*, from 2004 to 2009.

Please note that some prosecutions in 2008-2009 have not yet been completed.

PROSECUTIONS UNDER PART 10.6 CRIM CODE ACT 1995, by date received and outcome

Number of prosecutions under Part 10.6 of the Criminal Code Act 1995, by date received & outcome						
	2004-05	**2005-06**	**2006-07**	**2007-08**	**2008-09**	**Total**
Offence proven, highest penalty: Gaol	3	33	36	72	50	**194**
Offence proven, highest penalty: Gaol (Fully Suspended)	1	8	22	45	38	**114**
Offence proven, highest penalty: Periodic Detention	0	1	2	3	3	**9**
Offence proven, highest penalty: Fine	3	11	10	8	16	**48**
Offence proven, highest penalty: CBO / CSO	0	1	7	9	3	**20**
Offence proven, highest penalty: Recog Order/Bond/TBGB	1	17	20	26	24	**88**
Offence proven, highest penalty: Other	0	3	2	5	8	**18**
Prosecution discontinued	1	10	19	33	26	**89**
Outstanding warrant/Defendant not served	2	2	4	3	8	**19**
Not guilty/Acquitted	0	2	4	3	2	**11**
Not yet sentenced/Matter still open	0	0	2	22	91	**115**
Total prosecutions	**11**	**88**	**128**	**229**	**269**	**725**

PROSECUTIONS UNDER PART 10.7 CRIM CODE ACT 1995, by date received and outcome

Number of prosecutions under Part 10.7 of the Criminal Code Act 1995, by date received & outcome						
	2004-05	**2005-06**	**2006-07**	**2007-08**	**2008-09**	**Total**
Offence proven, highest penalty: Gaol	0	2	2	1	0	**5**
Offence proven, highest penalty: Gaol (Fully Suspended)	0	1	1	1	1	**4**
Offence proven, highest penalty: Periodic Detention	0	0	0	0	0	**0**
Offence proven, highest penalty: Fine	1	4	3	1	1	**10**
Offence proven, highest penalty: CBO / CSO	1	3	0	2	1	**7**
Offence proven, highest penalty: Recog Order/Bond/TBGB	1	2	3	3	1	**10**
Offence proven, highest penalty: Other	0	1	0	0	0	**1**
Prosecution discontinued	0	0	1	0	0	**1**
Outstanding warrant/Defendant not served	0	0	1	0	0	**1**
Not guilty/Acquitted	0	0	0	0	0	**0**
Not yet sentenced/Matter still open	0	0	0	0	2	**2**
Total prosecutions	**3**	**13**	**11**	**8**	**6**	**41**