HOUSE OF REPRESENTATIVES STANDING COMMITTEE ON COMMUNICATIONS

Inquiry into Cyber Crime

AUSTRALIAN FEDERAL POLICE

The Committee asked the following questions on notice at the hearing of 9 September 2009:

1a. Does the current description of cyber crime or technology enabled crime go far enough? Should it include damage to personal safety and wellbeing, for example, cyber bullying, stalking, and vilification, sim stalking, misuse of information and communications technology, damage to reputation and assumption of identity?

1b. How can legislation be future proofed to accommodate the changing nature of cyber crime and new technologies?

2a. What recourse do individuals have when they receive unsolicited pornographic photographs?

2b. What recourse do adults have if photographs of themselves are compromised and distributed without their knowledge?

3. Five areas of concern: (i) having identities assumed or created, involving new or manipulated images; (ii) the distortion of a person's personal interest, reputation or character; (iii) the broadcasting of personal data that is inaccurate, offensive, profoundly disturbing or intensely damaging; (iv) the use of ICT to bully or intimidate another party, to act in a manner contrary to their will, their free choice or interest; (v) and maliciously and intentionally hurtful campaigns of retribution, of character diminishment with no public interest or freedom of speech value.

4. What are the key messages for an education campaign to motivate consumers to protect themselves from cyber crime?

5. What are the take-home messages that the AFP would like to see the Committee consider? (in compiling a report on Cyber crime)

6a. What are the key challenges the AFP face in obtaining electronic data during an investigation into cyber crime, in particular, where that investigation crosses national borders?

6b. What are the key challenges the AFP face in relying on electronic data, which is evidence of a cyber crime, in Australian courts?

The answers to the Committee's questions are as follows:

1a. Does the current description of cyber crime or technology enabled crime go far enough? Should it include damage to personal safety and wellbeing, for example, cyber bullying, stalking, and vilification, sim stalking, misuse of information and communications technology, damage to reputation and assumption of identity?

Law Enforcement Agencies (LEA's) such as the Australian Federal Police (AFP) are bound by the definition of cyber or computer crimes as provided by legislation, particularly the *Criminal Code Act 1995* (Cth).

Cyber crime is a generic term often utilised to describe offences undertaken using information, communication and associated technologies and incorporates two distinct categories:

1. Crimes committed utilising Information and Communications Technology (ICT) as a 'facilitator' in the commission of the crime. This includes harassment, possession of objectionable material (child pornography), fraud and identity theft; and

2. Crimes committed that would otherwise be unable to be committed should the ICT not have existed. For example, Denial of Service (DOS) attacks and system intrusions, etcetera.

It is common for terms such as 'cyber crime' and 'Technology Enabled Crime (TEC) to be used interchangeably. As outlined above, they generally refer to criminal activity where the computer or network is the source, tool, target, or location of a crime. TEC also describes traditional crimes facilitated by technology (category one described above). These crimes are not new, but utilise technology to plan, enable or hide the crime and may include:

- Offensive or prohibited content, such as online child exploitation (child pornography);
- Threats, harassment and stalking;
- Extortion;
- Fraud;
- Sale of illegal items or services via the Internet; and
- Mule recruitment.

These offences are investigated under a variety of State, Territory and Commonwealth Acts.

It is envisaged that, given the increasing proliferation of ICT, the number of offences committed or facilitated through the use of ICT will increase. This does not mean that these offences should be considered as being 'cyber' crimes per se[1]. A differentiation

[1] The US Government Accountability Office report GAO-07-705 "CYBER CRIME – Public and Private Entities Face Challenges in Addressing Cyber Threats" contains an illustration on page 6 of traditional crimes that utilise ICT as a facilitator. http://www.gao.gov/new.items/d07705.pdf

between actual 'cyber' crimes as opposed to the underlying offences such as harassment or fraud should be made in a manner that clearly identifies the underlying act.

1b. How can legislation be future proofed to accommodate the changing nature of cyber crime and new technologies?

Due to the evolving nature of technology, it would be very difficult to future proof legislation to pre-empt the development of ICT. It is important, however, to understand the time sensitivity surrounding the nature of cybercrime and ensure that legal frameworks support this – especially relating to cross jurisdictional and transnational criminal activity.

The adaptation of legislation that reflects the use of ICT to commit predicate offences would ensure that new technologies would be encapsulated where 'real world' offences are committed using emerging technologies. That is to say, the insertion of an offence in the Criminal Code that stipulates any other offence can be committed "by virtue" of the use of ICT.

2a. What recourse do individuals have when they receive unsolicited pornographic photographs?

Adult Pornography

The receipt of unsolicited adult pornographic images may cause particular offence to individuals depending on age, race, religion or other characteristics. If the individual receiving the images is offended, they have the option to report the conduct to their local police station as the conduct could potentially amount to an offence under s474.17 of the *Criminal Code Act* 1995 (Cth). Matters of this nature would be decided on a case-by-case basis. Please note that in Australia, the Office of Film and Literature Classification (OFLC) are responsible for the classification of films, including pornography. Such films are subjected to the *Classification (Publications, Films and Computer Games) Act* 1995 (Cth*).*

There are specific rules governing dealings with films that are unclassified, exempt from classification, RC, M15+, R18+ and X18+ and the relevant offences in the Australian Capital Territory in relation to the Commonwealth Act are outlined in the *Classification (Publications, Films and Computer Games) (Enforcement) Act* 1995 (ACT). Other states and territories of Australia have similar enforcement legislation. Offences contained in these Acts appear to be more applicable in the commercialisation of films rather than the private sector, however depending on the conduct these Acts may apply.

<u>Practical Options</u>
If the individual does not wish to possess the image, they have the option of discarding it. Additionally, the individual could either:

1. Ask the individual providing the images to stop; and/or
2. Change their personal email account and telephone numbers.

Should such incidents continue, the individual may also request their service provider block the sender's number.

Child Pornography

If the photographs contain child abuse material, the *Criminal Code Act 1995* (Cth) could be applicable. Possible offences include:

474.19 Using a carriage service for child pornography material

(1) A person is guilty of an offence if

(a) the person:

(i) uses a carriage service to access material; or

(ii) uses a carriage service to cause material to be transmitted to the person; or

(iii) uses a carriage service to transmit material; or

(iv) uses a carriage service to make material available; or

(v) uses a carriage service to publish or otherwise distribute material; and

(b) the material is child pornography material.

Penalty: Imprisonment for ten years.

474.20 Possessing, controlling, producing, supplying or obtaining child pornography material for use through a carriage service

(1) A person is guilty of an offence if:

(a) the person:

(i) has possession or control of material; or

(ii) produces, supplies or obtains material; and

(b) the material is child pornography material; and

(c) the person has that possession or control, or engages in that production, supply or obtaining, with the intention that the material be used:

(i) by that person; or

(ii) by another person;

in committing an offence against section 474.19 (using a carriage service for child pornography material).

Penalty: Imprisonment for ten years.

If an individual possesses, controls, produces, supplies or obtains child pornography or child abuse material via a mobile telephone, computer or other device, they may be charged with an offence under the abovementioned sections of the *Criminal Code Act 1995* (Cth).

Practical Options
Where an individual receives child pornographic images or child abuse material, they have the following options:

1. Report the conduct; and/or
2. Ask the individual providing the images to stop; and/or
3. Change their personal email account and telephone numbers.

An individual can report this type of conduct to a number of agencies including their local police, the AFP, their Internet Service Provider (ISP), telecommunications provider or online via the Think U Know website (www.thinkuknow.org.au), Virtual Global Taskforce website (www.virtualglobaltaskforce.com) or the Australian Communications and Media Authority (ACMA) website (www.acma.gov.au) . These websites have a 'report abuse' help button, where assistance will be provided and the AFP may also be notified where appropriate.

2b. What recourse do adults have if photographs of themselves are compromised and distributed without their knowledge?

Unfortunately, the individual may not have any legal recourse. As mentioned above, there are no offences in relation to the conduct of creating, receiving and possessing adult pornographic images. However, distributing pornography could amount to conduct that is prohibited by s474.17 of the *Criminal Code 1995* (Cth).

> **474.17 Using a carriage service to menace, harass or cause offence**
>
> (1) A person is guilty of an offence if:
> (a) the person uses a carriage service; and
> (b) the person does so in a way (whether by the method of use or the content of a communication, or both) that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive.
>
> Penalty: Imprisonment for three years.

This section also includes behaviour where the use of a mobile telephone, computer or other device is being used in such a way to menace, harass or cause an individual offence. Behaviour such as distributing compromising pornographic images to colleagues, acquaintances, family and friends of an individual could potentially be an offence under this section.

Practical Options
An individual's recourse in this situation depends on how the photograph is being distributed. Possible responses include :

1. Report the conduct to their ISP or telecommunications provider; and/or
2. Ask the individual providing the images to stop; and/or
3. Change their personal email account and telephone numbers.

3. Five areas of concern:
(i) having identities assumed or created, involving new or manipulated images
(ii) the distortion of a person's personal interest, reputation or character
(iii) the broadcasting of personal data that is inaccurate, offensive, profoundly disturbing or intensely damaging
(iv) the use of ICT to bully or intimidate another party, to act in a manner contrary to their will, their free choice or interest
(v) and maliciously and intentionally hurtful campaigns of retribution, of character diminishment with no public interest or freedom of speech value.

There are existing Commonwealth, State and Territory Acts that deal with the categories of behaviour identified and in which ICT merely acts as an enabler in the commission of such offences.

In each instance, a formal complaint should be made to the relevant law enforcement authority by the person subject to the activity causing concern.

For example, in the Commonwealth *Criminal Code Act 1995* (Cth), offences related to use of telecommunications include:

- s474.14 Using a telecommunications network with intention to commit a serious offence;
- s474.15 Using a carriage service to make a threat; and
- s474.17 Using a carriage service to menace, harass of cause offence.

Following are two examples of equally applicable of State legislation:

s184 of the *Crimes Act 1900 (NSW)* Fraudulent personation

> Whosoever falsely personates, or pretends to be, some other person, with intent fraudulently to obtain any property, shall be liable to imprisonment for seven years.
>
> Nothing in this section shall prevent any person so personating, or pretending, from being proceeded against in respect of such act, or pretence, under any other enactment or at Common Law.

s529 of the *Crimes Act 1900 (NSW)* Criminal defamation

> (1) Common law misdemeanour of criminal libel abolished. The common law misdemeanour of criminal libel remains abolished.
>
> (2) Blasphemous, seditious or obscene libel not affected Subsection (1) does not affect the law relating to blasphemous, seditious or obscene libel.
>
> (3) Offence of criminal defamation A person who, without lawful excuse, publishes matter defamatory of another living person (the 'victim'):
>
> (a) knowing the matter to be false, and
>
> (b) with intent to cause serious harm to the victim or any other person or being reckless as to whether such harm is caused is guilty of an offence.
>
> Maximum penalty: 3 years imprisonment.

In addition to the above, please refer to responses for previous questions.

4. What are the key messages for an education campaign to motivate consumers to protect themselves from cyber crime?

The AFP recognises the importance of educating Australian consumers to raise awareness of the risks faced online, particularly toward empowering them to mitigate such risks. The Crime Prevention Team (CPT) within the AFP's High Tech Crime Operations (HTCO) portfolio is primarily responsible for developing and implementing cyber safety education initiatives to raise awareness.

Cyber crime prevention and safety education initiatives need to be multi-faceted to address varying levels of inter-generational risk . It is important, therefore, that educational messages cover the broad spectrum of Australian consumers, from youth to parents and teachers, as well as seniors. To this end, the AFP has prepared a number of educational flyers addressing the specific risks faced by young Australians, for example, cyber-bullying and protecting your online reputation, and older Australians, for example, security on the internet. As part of the ThinkUKnow cyber-safety program, the AFP in conjunction with Microsoft Australia has developed additional flyers for parents, carers and teachers on cyber security issues of concern .

From a 'whole-of-government' perspective, the AFP has participated in national awareness raising events such National E-Security Awareness Week (NEAW) in 2008 and 2009. The importance of such events is the delivery of consistent messages on cyber security from government, non-government agencies, and industry groups. In 2009, the following set of positioning messages concerning risks to identity was developed:

- "Every year, there's more information about you online".
- "People are finding more ways to use your personal and financial information to harm you, or even pretend to be you".
- "Do five simple things to better protect yourself online".

These positioning messages were then translated into five 'top tips' for internet security. The following five actions to improve the security of personal and financial information were included in all promotional and information materials, media releases and backgrounders:

1. Get a better, stronger password and change it at least twice a year;
2. Get security software, and update and patch it regularly;
3. Stop and think before you click on links or attachments from unknown sources;
4. Be careful about what you give away about yourself and others online. Information is valuable; and
5. Go to www.staysmartonline.gov.au for further information and to sign up for the email alert service.

As part of its awareness raising campaign, the CPT delivers cyber-safety presentations to primary and secondary schools in the Australian Capital Territory (ACT) and in

regional New South Wales. Included in these presentations are short films depicting 'online child grooming; and cyber-bullying'. These short films are also made available through the 'ThinkuKnow website (www.thinkuknow.org.au).

5. What are the take-home messages that the AFP would like to see the Committee consider? (in compiling a report on cyber crime)

The AFP advise the Committee consider that:

- Cyber crime will continue to be a rapidly evolving landscape, necessitating an emphatic, coordinated response;
- Legislation frameworks need to be responsive and conducive to cross-jurisdictional/transnational environments and contexts. Cyber crime is a global issue, therefore effective investigations are time-critical and not bound by traditional understandings of time and space; .
- Law enforcement efforts directed towards the mitigation, disruption and prosecution of cyber crimes can only go so far in combating cyber crime;
- Prevention of cyber crime requires Australian consumers take proactive measures to ensure their online experience is safe, and that they do not fall victim to some of the vulnerabilities which exist in the online environment;
- The volume and sophistication of threats online make it imperative that multi-layered, real time protection is made available to Australian consumers to ensure online safety; and
- The public message should be "Cyber security is everybody's responsibility". Australian consumers need to be empowered to be able to protect themselves online through the delivery of public education and awareness raising initiatives.

6a. What are the key challenges the AFP face in obtaining electronic data during an investigation into cyber crime, in particular, where that investigation crosses national borders?

Key challenges faced by the AFP and other domestic and international Law Enforcement Agencies (LEA's) are posed by the dynamic and transnational nature of cyber crime and include:

- the inability to obtain information and intelligence for forensic data analyses in a timely manner from source entities such as overseas Internet Service Providers (ISP's) or communication services to identify and prosecute offenders (data is generally not received in time to be submitted to court. In some cases this can take up to eighteen months unless the investigation is high profile);
- Mutual Assistance frameworks that currently inhibit LEA ability to obtain evidence to identify transnational cyber offenders in a timely manner for prosecution;
- inconsistent international legislation, in particular:
    - The inability to enforce obligation on overseas service providers to adhere to Australian legal processes where the service or data holdings are based outside Australian jurisdiction; and

    - The inability to prosecute individuals based overseas for cyber offences where there is no similar offence in the country of origin;
- the ability to adapt current LEA methodologies to a borderless environment where, in addition to legislative challenges, capability and capacity to support cyber investigations can vary between organisation, state and/or nation (this includes inconsistent trans-national telecommunications intercept data retention laws);
- the exponential growth in personal information maintained on ICT that will assist predicate offences such as identity theft, financial fraud or other underlying offences;
- the under-reporting of the genesis of predicate offences where data is compromised through the use of ICT;
- the convergence of technologies that will reduce the ability of service providers to correlate unique users or service subscribers to particular services;
- the development of simple-to-use, legitimate encryption and data protection techniques providing Virtual Private Networks and protections to online offenders by inhibiting the ability of LEA's to detect, deter, mitigate and prosecute offences through robust obfuscation techniques; and
- the ability of criminals to commit or facilitate offences through the use of disposable ICTs such as prepaid mobile and wireless communications and free g-mail electronic addresses thereby restricting the ability of LEA's to obtain evidentiary material.

6b. What are the key challenges the AFP face in relying on electronic data, which is evidence of a cyber crime, in Australian courts?

Key challenges for the AFP in relying on electronic data may include:

- the timeliness and/or availability of data and the capacity of telecommunication carriers in Australia to meet their legislative obligations under the *Telecommunications (Intercept and Access) Act* 1979 (Cth) to ensure subscriber details are available upon request by relevant LEA's, including emergency call location and general subscriber information. Carrier capabilities may be limited by the technical capacity to provide information or "no cost/benefit" required under the *Telecommunications (Intercept and Access) Act* 1979;
- the implications of full disclosure requiring potentially large volumes of data to be made available. The increase in data volumes that will occur through enriched access to faster and more accessible services is not expected to correlate with the growth in human resources dedicated to the forensic analysis or the improvements in automated tools required to facilitate the examination;
- the ability to store, review and analyse (including encrypted information) voluminous data. The paucity of tools/systems available to LEAs which can robustly demonstrate chain of evidence handling of digital media;

- the lack of an Australia-wide standard for the display of electronic evidence to court
- the education of LEA professionals in understanding emerging technologies and the manner in which an individual can be connected to an offence through the analysis of the available data;
- retaining appropriately skilled investigators, prosecutors and judiciary members conversant with ICT processes and methodologies required for effective to cyber crime investigations and data analyses; and
- the limited ability to educate the judiciary in the seriousness of cyber offences and potential subsequent harm caused.