SUBMISSION No. 136

A Submission to the

Joint Select Committee on Cyber Safety

Parliament of Australia

Inquiry into Cyber-Safety

Prepared by

Stewart Healley

Youth Support Worker

Melrose High School

Canberra

ACT

Australia

27th March 2011

The Author:

Stewart Healley

Current:

Youth Support Worker - 5 Years
Department of Education & Training
Youth Support Workers in High School Program
Melrose High School
Marr Street, Pearce
Canberra, ACT, 2607
Australia

Relevant Background:

BSc (Psychology & Sociology) - 2002
Certificate IV - Youth Work - 2007
Ex Victoria Police - 11 Years
Ex NSW Ambulance - 2 Years
Ex Victoria Ambulance - 5 Years

Preamble:

Fortunately, there is a growing effort by some members of the community to address Bullying and Cyberbullying in our society. There has been some excellent research done already with more currently underway, helping to advance our knowledge and understanding.
However, the practical applications of this research and "talk fests" have produced a very fragmented approach to addressing a Practical Response to the growing problem of Bullying and Cyberbullying in our schools and society in Australia and around the World.

The Price of Silence:
Unfortunately, our lack of Community action and support for our vulnerable teenagers has left many of them with the message that "our silence" means that this "ISSUE" and "THEY" are not important enough to FIGHT for.

This current "Void in Support and Action" has left far too many teenagers without any "ADULT PROTECTION" to help keep them safe from their feelings of helplessness and hopelessness. Resulting in some of our most vulnerable teenagers; disengaging from School Studies; Sporting Activities and engaging in "High Risk Activities'; such as Binge Drinking, Drug Exploring; Sexual Favours; Family and Social Withdrawal and even seeking comfort from engaging in "Physical Self Harm" Practices.

Tragically, others who may try out some or all of the wonderful Cyber-Safety tools and techniques still find the ANSWER in SUICIDE to end the pain and anxiety of being the unwanted VICTIM of Bullying and Cyber-Bullying.

Unfortunately I have forgotten the name of the author of a past Doctor - Ambulance Training Session, I attended many years ago. But I have never forgotten his insightful story when assessing a person's Mental Health Status. His story was as follows:

"When you attend to a call about a "Crazy Nutter" on a local street corner, take some time to talk to this person and assess them on the grounds that are they suffering FROM Insanity or are they suffering FOR their Sanity".

Unfortunately, we have far too many teenagers struggling with issues about Bullying and Cyber-bullying; suffering alone ***FOR*** their own ***SANITY*** and understanding that this ***SITUATION*** should ***NOT*** be allowed to ***START***, let alone ***CONTINUE UNCHALLENGED*** with no clear ***END*** in sight.

……. "WHERE ARE THE ADULTS" …….

In the recent School Bullying "YouTube" incident involving a Year 10 Student named "Casey", when asked did he have any advice for others who were bullied at school, revealed a rather damming comment as to the state of bullying in our school system with his simple reply of:

"Remember the good days and School doesn't last FOREVER!"

I have considered the parameters of this inquiry and conclude that we cannot disconnect Bullying from Cyberbullying.

In my opinion both Bullying and Cyberbullying should be considered as Acts and/or Comments of Discrimination and on this basis I have made 12 Recommendations to the Joint Parliamentary Committee on ways to best address this matter.

My **12 Recommendations** include the following:

1. **Appoint an Australian National Child and Young Persons Human Rights Commissioner**
2. **Establish a National Child and Young Persons Human Rights Council**
3. **Promote the United Nations Convention on the Rights of the Child (1989)**
4. **Establish a Australian National Cyberbullying 24/7 Helpline and Reporting System**
5. **Establish a National "Schools Best Practice" Model**
6. **Establish appropriate National "Base Line" Legal Framework Laws, starting with the existing Commonwealth Criminal Code 1995**
7. **Establish Constructive & Regular Consultation with teachers, parents, and young people**
8. **Establish Constructive &Regular Consultation with Government, Community, Industry & Interest Groups**
9. **Establish a National Accredited Bullying & Cyberbullying Training Program for Teachers**
10. **Establish a National Accredited Bullying & Cyberbullying Training for AFP & State Police**
11. **Establish a National Accredited Bullying & Cyberbullying Training for Magistrate Court Staff**
12. **Update the National Child Protection Policy to include Mandatory Reporting of Child Abuse from Bullying and Cyberbullying Incidents.**

Kind Regards

Stewart Healley

"Good Things Happen when Good Women & Good Men Do Something"

Contents:

Contents (cont):

Summary of Recommendations: (cont)

Details of Recommendations:

Contents (cont):

Details of Recommendations: (cont)

Appendix Reference

Contents (cont):

Appendix Reference *(cont)*

Contents (cont):

Appendix Reference *(cont)*

Contents (cont):

Contents (cont):

Additional Reference Information (cont)

Contents (cont):

Additional Reference Information (cont)

Contents (cont):

Additional Reference Information (cont)

Contents (cont):

Additional Reference Information (cont)

Summary of Recommendations:

Summary of:

Recommendations for Joint Parliamentary Committee on Cybersafety

Stewart Healley – 27th March 2011

Recommendation # 1

Appoint an Australian National Child and Young Persons Human Rights Commissioner

Appoint an **Australian National Child and Young Persons Human Rights Commissioner**, who reports to the Prime Minister.

1.1 Support the current Australian Human Rights Commission's submission before to the Australian Senate Committee for the appointment of an Australian National Child and Young Persons Human Rights Commissioner. *(see Appendix 01)*

1.2 The appointment of an **Australian National Child and Young Persons Human Rights Commissioner** empowered to oversee the implementation of new Anti-Bullying and Anti-Cyberbullying initiatives provides a politically neutral level of jurisdiction, focused on the Human Rights of Children and Young Persons.

1.3 The appointment of an **Australian National Child and Young Persons Human Rights Commissioner** offers a more acceptable and appropriate choice than the alternative suggestion of appointing a Government Cybersafety Ombudsman.

Recommendation # 2

Establish a National Child and Young Persons Human Rights Council

Assist the Australian National Child and Young Persons Human Rights Commissioner to establish and chair a **National Child and Young Persons Human Rights Council**.

2.1 Members of this Council to include representative from, Education, Health, Justice, Police, Research, Industry, Community Development and Community Support Agencies.

2.2 The National Child and Young Persons Human Rights Council will actively promote the **United Nations Convention on the Rights of the Child (1989)**, (Appendix 02) by educating the Community that bullying and cyberbullying are NOT just minor problems of "Mean Behaviour" but are **Acts and Comments of Discrimination** Against the Rights of ALL Australian Citizens, especially against our Children and Young People.

Recommendation # 3

Promote the United Nations Convention on the Rights of the Child (1989)

The National Child and Young Persons Human Rights Council will actively promote the **United Nations Convention on the Rights of the Child (1989)**, and help establish a "**Best Practice" Set of Laws** for **Acts and Comments of Discrimination** when dealing with bullying and cyberbullying incidents.

Members of the Council are charged with the responsibility for helping to:

3.1 **Establish a National Relevant Set of Laws**

Establish a **National Relevant Set of Laws** that protect victims of Acts and Comments of Discrimination in serious bullying and cyberbullying incidents. – The **Criminal Code 1995 Laws** provide a Base Line Set to add and modify to suit a National Jurisdiction. *(See Appendix 03)*

Recommendation # 4

Establish a Australian National Cyberbullying 24/7 Helpline and Reporting System

The National Child and Young Persons Human Rights Council will actively work with The **Australian Communications and Media Authority (ACMA)**, to establish a **National Cyberbullying 24/7 Hotline and Reporting System** to help support individuals involved in cases of serious Cyberbullying.

4.1 **The Australian Communications and Media Authority (ACMA)** will monitor:

- **Victims**
    - The **National Reporting System** operated by ACMA will provide a Youth Friendly, **24 / 7 Hotline & E-mail Complaints Centre** for victims of Cyberbullying incidents. These complaints are to be registered on a National Reporting System to help coordinate an effective and timely response by the Industry Service Providers. (E.g. Link ACMA into receiving a copy of ALL the Warning Notices, Site Material Removal and Site Closure Notices, The ACMA will be responsible to monitor Industry response times and compliance.)

- **Offenders**
    - The **National Reporting System** operated by ACMA will monitor and provide timely Notification to Australian Law Enforcement Agencies of **Multiple Offending Individuals** (e.g. multiple victim complaints) and / or **Repeat Offending Individuals** (e.g. same victim multiple complaints) for further investigation and prosecution.

Recommendation # 4 (cont)

Establish a Australian National Cyberbullying 24/7 Helpline and Reporting System

- **Industry** with:-
    - Timely responses to requests for the removing of **inappropriate material.** (e.g. Blocking Individuals or Closing Sites = 24 Hours)
    - Warning Notice Procedure and Process advising offending service users with **"1st Warning – Service Violation - this service has been used to send inappropriate material – a 2nd Violation will terminate this Service**".(Mobile Phone / Internet Message).
    - Timely response to requests for **Account Details by Australian Law Enforcement Agencies** (time to be set by AFP =? Hours)
    - The Australian Government to provide the necessary resources, support and funding to cover AFP and State Police for request of **Account Details from Service Providers**, who currently charge a substantial fee for requests by Police for Account Details in non life threatening incidents, under current Legislative conditions of "Cost Recovery"
    - Businesses operating in Australia, with or without a Representative Office on Australian Soil are still legally bound by Australian Practices and Content Conditions in accordance to **Australian Government Laws and Practices** (e.g. NOT Subject to USA Law Protection under the 1st Amendment Bill of Rights – Free Speech Claim)

Recommendation # 5

Establish a National "Schools Best Practice" Model

The National Child and Young Persons Human Rights Council working with appropriate Expert Working Groups will help develop, publish and promote a **National "Schools Best Practice" Model** to be included in the **National Safe Schools Framework** to standardize a minimum protection level that is contained in ALL School Policies and Procedures.

5.1 A **National School Best Practice Model** will help to guarantee an Australian wide Protection Standard for ALL children and young people no matter which State or what type of School.

5.2 Provide the necessary resources to support schools to minimise bullying and cyberbullying practices by adding to the **National "Schools Best Practice" Model** with **"Local Best Practice" Policies** and **Procedures** and ensure School ownership.

Recommendation # 6

Establish appropriate National "Base Line" Legal Framework Laws starting with the existing Criminal Code 1995

6.1 The National Child and Young Persons Human Rights Council working with appropriate Expert Working Groups will help develop, publish and promote a **National "Base Line" Legal Framework Laws**, starting with the existing **Commonwealth Criminal Code 1995.** (see Appendix 04)

6.2 A **National "Base Line" Legal Framework Law** will help to guarantee an Australian wide Protection Standard for ALL children and young people no matter which State or what type of School.

6.3 Providing Police & Community protection and support for victims and offenders with a Community Trial of the Practical "Respect It or Lose It" - Cyber Safety Model, promoting **a Police Charge / Caution** with a **Restorative Justice Program Pathway**

Recommendation # 7

Establish Constructive and Regular Consultation with teachers, parents, and young people

The National Child and Young Persons Human Rights Council to seek and maintain an active input from **teachers, parents,** and **young people** through linking with existing groups and organisations.

Recommendation # 8

Establish Constructive and Regular Consultation with Government, Community, Industry and Interest Groups

The National Child and Young Persons Human Rights Council to seek and maintain an active input from Government, Community, Industry and Interest Groups through linking with existing **Government, Community, Industry and Interest Groups**

Recommendation # 9

Establish a National Accredited Bullying & Cyberbullying Training Program for Teachers

Provide the necessary resources to support **Schools** to minimise bullying and cyberbullying practices by providing **Teachers** with a **National Accredited Bullying & Cyberbullying Training Program** that is independently funded by the Australian Government and validated by the National Child and Young Persons Human Rights Council

Recommendation # 10

Establish a National Accredited Bullying & Cyberbullying Training Program for AFP & State Police

Provide the necessary resources to support Federal and State Police to minimise bullying and cyberbullying practices by providing Police Members with a **National Accredited Bullying & Cyberbullying Training Program** that is independently funded by the Australian Government and validated by the National Child and Young Persons Human Rights Council.

Recommendation # 11

Establish a National Accredited Bullying & Cyberbullying Training Program for Magistrate Court, DPP & Justice Staff

Provide the necessary resources to support Magistrate Court and DPP Staff to minimise bullying and cyberbullying practices by providing Judges and Prosecutors with a **National Accredited Bullying & Cyberbullying Training Program** that is independently funded by the Australian Government and validated by the National Child and Young Persons Human Rights Council.

Recommendation # 12

Update the National Child Protection Policy to include Mandatory Reporting of Child Abuse from Bullying and Cyberbullying Incidents

Provide the necessary resources to support a Training Program for a National Child Protection Policy to include Mandatory Reporting of Child Abuse from Bullying and Cyberbullying Incidents, to minimise bullying and cyberbullying practices. This Training Program is independently funded by the Australian Government and validated by the National Child and Young Persons Human Rights Council.

Details of Recommendations:

Recommendation # 1

Appoint an Australian National Child and Young Persons Human Rights Commissioner

Details of:

Recommendations for Joint Parliamentary Committee on Cybersafety

Recommendation # 1

Appoint an Australian National Child and Young Persons Human Rights Commissioner

Appoint an **Australian National Child and Young Persons Human Rights Commissioner**, who reports to the Prime Minister.

1.2. Support the current Australian Human Rights Commission's submission before to the Australian Senate Committee for the appointment of an Australian National Child and Young Persons Human Rights Commissioner. *(see Appendix 01)*

1.3. The appointment of a **Australian National Child and Young Persons Human Rights Commissioner** empowered to oversee the implementation of new Anti-Bullying and Anti-Cyberbullying initiatives provides a politically neutral level of jurisdiction, focused on the Human Rights of children and Young Persons.

1.4. The appointment of a **Australian National Child and Young Persons Human Rights Commissioner** offers a more acceptable and appropriate choice than the alternative suggestion of appointing a Government Cybersafety Ombudsman.

Comment

I recommend the Joint Parliamentary Committee support the Australian Human Rights Commission's Application to the Senate Legal and Constitutional Affairs Committee for the Appointment of a Commonwealth Commissioner for Children and Young People.

Extract of submission (see Appendix 01)

Australian Human Rights Commission
Commonwealth Commissioner for Children and Young People Bill 2010

1 Introduction

The Australian Human Rights Commission (the Commission) makes this submission to the Senate Legal and Constitutional Affairs Committee in its inquiry into the Commonwealth Commissioner for Children and Young People Bill 2010. This submission considers the broad issues raised by the Bill. It does not make a detailed analysis of each proposed provision.

The Commission has for a number of years supported the establishment of the Office of a national Children's Commissioner as an important way of better respecting and promoting the rights of all children in Australia.

Recommendation # 1 *(cont)*

Australia ratified the United Nations Convention on the Rights of the Child (CRC) in 1990. This means that under international law the Australian Government has specific human rights obligations to children. (see Appendix 02)

The United Nations Committee on the Rights of the Child has expressed concern that there is no national commissioner with a specific mandate for monitoring children's rights in Australia. The Committee has also noted that despite the valuable work of the Australian Human Rights Commission in the area of children's rights there is no unit devoted specifically to children's rights at the Commission.[1] Establishing a Commonwealth Commissioner for Children and Young People would be an important step towards meeting Australia's international obligations to protect and promote the rights of children in Australia.

2 Summary

The Commission would welcome the establishment of the office of a Commonwealth Commissioner for Children and Young People.[2] The Australian Human Rights Commission believes that a Commonwealth Commissioner for Children and Young People could play an important role in protecting the rights of children and young people, in particular by:

- *operating as a national advocate for children's rights, ensuring that government decision making processes and outcomes are consistent with the best interests of children*
- *developing mechanisms to secure the participation of children in decisions that affect them*
- *providing a coordinated national approach to children's rights.*

The Australian Human Rights Commission believes that the key features of a national Children's Commissioner are:

- *independence from government*
- *statutory authority and power, including security of tenure*
- *adequate resourcing*
- *accessibility to children, including establishment of a child-appropriate complaints process*
- *exclusive focus on children under 18 years of age*
- *ability to act proactively and reactively and to direct its own agenda.*

[1] The Committee on the Rights of the Child, 40th Session, Concluding Observations: Australia, 20 October 2005; The Committee on the Rights of the Child, 16th Session, Concluding Observations: Australia, 21 October 1997.

[1] The Australian Human Rights Commission has called for the establishment of a 'national Children's Commissioner'. As the Bill uses the term Commonwealth Commissioner for Children and Young People, this term will be used throughout this submission.

Recommendation # 1 *(cont)*

3 Recommendations

The Commission recommends that:

- *Recommendation 1: A statutory office of Commonwealth Commissioner for Children and Young People should be established.*
- *Recommendation 2: The functions and powers of a Commonwealth Commissioner for Children and Young People should extend to 'all children in Australia' regardless of their citizenship or residency status.*
- *Recommendation 3: The Australian Government should retain responsibility for preparing reports to the United Nations Committee on the Rights of the Child. The Commonwealth Commissioner for Children and Young People should be able to prepare an independent report to the Committee should he or she wish to do so.*

4 Why does Australia need a national Children's Commissioner?

Many children in Australia are able to enjoy their rights. However, the rights of some children are vulnerable. These include children experiencing homelessness, children experiencing violence, bullying or harassment and children who live with a disability, including those living with mental illness.

There are also certain groups of at-risk children who are less likely to be able to enjoy their full range of rights. These groups include Aboriginal and Torres Strait Islander children; children in out of home care; children in detention, including those in immigration detention; and children living in rural and remote areas of Australia.

A Commonwealth Commissioner for Children and Young People would play an important role in promoting and protecting the rights of all children in Australia, particularly of those who are most at risk. This could improve their opportunities to develop to their full potential and to make a positive contribution to society. In particular, a Commonwealth Commissioner for Children and Young People could:

- *operate as a national advocate for children's rights, ensuring that government decision-making processes and outcomes are consistent with the best interests of children*
- *develop mechanisms to secure the participation of children in decisions that affect them*
- *provide a coordinated national approach to children's rights.*

Recommendation # 1 *(cont)*

Comment

I would recommend to the Joint Parliamentary Committee to support the appointment of an **Australian National Child and Young People Human Rights Commissioner**, to help educate the Community that bullying and cyberbullying are NOT just minor problems of "Mean Behaviour" but are **Acts and Comments of Discrimination** Against the Rights of ALL Australian Citizens, especially against our Children and Young People.

The **National Child and Young People Human Rights Commissioner** would help by introducing into the debate on Bullying and Cyberbullying a change in Approach and Focus.

1. A change from the **Old Approach** with a:

1.1. A **"Bottom-Up Push**" regarding the proving of an **ACT or COMMENT to be "mean" or "illegal" BEHAVIOUR** by one individual and/or group against another individual and/or group.

2. A change to a **New Approach** with a:

2.1. A "**Top-Down Push**" regarding the identification of an **ACT or COMMENT as DISCRIMINATION** by one individual and/or group against another individual and/or group. The advantage of this approach is that it can be:

2.2. A measured **Authoritative Approach** (not an "Bullying" Authoritarian Approach)

2.3. An Authoritative Approach can introduce a "**Reverse Onus of Proof**" to be placed on the accused person to prove "**Beyond Reasonable Doubt**" to a "**Reasonable Person**" that the Act or Comment" was **NOT** an **Act or Comment of Discrimination**.

3. A change from the **Old Focus** where:

3.1. Unfortunately, the use of any "Label" tends to influence the self perception of people especially young people who tend to first believe the truth of the label then begin to behave according to the positive or negative connotation of the label, for example – "Skinny" or "Fat"; "Smart' or "Stupid; "Pretty or Ugly"; "Winner" or "Loser"; "Bully" or "Victim".

3.2. The use of "Labels" of "Bully" and now "Cyberbully" also help to reinforce a "POWER" position on the "Bully" and/or "Cyberbully". By using these Labels we can unwittingly become a player in the "The Bullying Game", which has very predictable dialogue rules, which the "Bully" and "Cyberbully' are well skilled in manipulating the situations with "Under Reactions" by adults by planting the "seeds of doubt" and "Over Reactions" by adults with "Blame the Victim":

Recommendation # 1 *(cont)*

3.3. Examples of Under Reactions by adults with planting the "seeds of doubt";

3.3.1. "I was only joking"
3.3.2. "What a sissy"
3.3.3. "I never said that"
3.3.4. "It wasn't me"
3.3.5. "I didn't do anything"
3.3.6. "Prove it"

3.4. Examples of Over Reaction by adults with "Blamer the Victim"::

3.4.1. "She started it"
3.4.2. "He's a Loser"
3.4.3. "She's weird"

4. A change to a **New Focus** where:

4.1. Future research could investigate the possibility of moving away from using the reinforcing negative labels of Bully, Cyberbully and Victim to a more neutral description with a Legal and Industry Standard Terminology. This move will help neutralize the current "power dialogue" with new descriptors such as:

4.2. Definitions - Legal and Industry Standard Terminology

4.2.1. **The Main Offender ("Person A")**

4.2.1.1. **A person who has offender another person or persons with an act and / or comment of discrimination.**

4.2.2. **The Offended Person ("Person B1")**

4.2.2.1. **A person or persons who have been offended another person or persons with an act and / or comment of discrimination.**

4.2.3. **The Other Offended Persons ("Person B2"; "Person B3"; "Person B4"; etc.)**

4.2.3.1. **Persons who have also been offended another person or persons with an act and / or comment of discrimination.**

4.2.4. **The Other Offenders ("Person C1"; "Person C2" "Person C3" etc.)**

4.2.4.1. **Persons who have also offender another person or persons with an act and / or comment of discrimination**

Recommendation # 1 *(cont)*

4.3. Examples - Legal and Industry Standard Terminology

4.4. Single Bully and / or Cyberbully

4.4.1. = **Alleged Offending Person** = "**Person A**"

4.5. Victim

4.5.1. = **Alleged Offended Person = "Person B"**

4.6. Multiple Victims

4.6.1. = **Alleged Offended Persons = Person B1; Person B2; Person B3;** etc.

4.7. Multiple Bullies and /or Cyberbullies

4.7.1. = **Alleged Offending Persons** = **Person C1**; **Person C2; Person C3;** etc.

Further examples of "**The Cycle of Inaction"** by adults by planting the "seeds of doubt" outlined in "**The dynamic of misleading teachers by claiming 'provocation'"** plus the **"The Cycle of Over Reaction"** by adults with "**The dynamic of 'blaming the victim'"** are provided in the National Safe Schools Framework Reference Section. (Appendix 03)

Appendix 03

The cycle of inaction

Cross et al. (2009) have described a 'cycle of inaction' that can occur in response to covert bullying:

- *The cycle begins when a teacher receives a report about covert bullying and they do not respond to it seriously or effectively. This may occur as a result of their inexperience and lack of knowledge about covert bullying and/or a belief that what is happening to a student either is not really bullying or is not as harmful as other types of bullying.*

- *The student who is being covertly bullied reacts to the teacher's inaction by feeling disempowered and hence becomes less willing to ask for teacher support if it happens again.*

- *The students who are doing the covert bullying interpret the teacher's inaction by forming a belief that covert bullying is tolerated in the school.*

- *All students who are bullied are less likely to seek help because they perceive that there is a culture of acceptance of (covert) bullying.*

Recommendation # 1 *(cont)*

The dynamic of misleading teachers by claiming 'provocation'

Some students can become quite adept at misleading teachers about their role in bullying (and aggressive assaults) by claiming 'provocation' by things that the bullied student has (supposedly) said about them or their family, or by actions they have (supposedly) taken. This common dynamic serves a dual purpose:

1. *It shifts the blame onto the student who is being bullied and helps the bullying student feel less discomfort over behaving in a socially unacceptable way (Burns et al., 2008)*

2. *It encourages adults to see their behaviour as justified, to not take it as seriously and so not apply consequences.*

In some cases this claimed provocation from things said or done might be true, but more often it is exaggerated or fabricated. In some cases 'provocation' simply represents annoyance with, or intolerance of, the bullied student's 'different' social behaviour or physical characteristics (Phillips, 2003; Teräsahjo & Salmivalli, 2003; Akiba, 2004).

The cycle of over-reaction

Mishna & Alaggia (2005) argue that students weigh up the benefits and the risks of asking a teacher for support when they are being bullied. The benefits are that they may be effectively supported and the bullying will stop. The risks are many: they may not be believed or taken seriously; they may be blamed by the teacher for their own victimisation and feel ashamed; there may be retaliation from the student complained about or their friends; the teacher may handle the situation insensitively or ineffectively, and it will either make no difference or even make the situation worse; it may make them feel like they cannot handle their problems by themselves (Bijttebier & Vertommen, 1998; Boulton & Underwood, 1992; Clarke & Kiselica, 1997; Miller et al., 1998; Mishna et al., 2005; Naylor et al., 2001; Newman et al., 2001; Rigby & Slee, 1991; Smith, 1991; Smith & Myron-Wilson, 1998).

The cycle of over-reaction can start when a student decides to seek support from a teacher because they are being bullied.

1. *The teacher responds to this request for support by quickly punishing the students who are bullying.*

2. *The student who is being bullied receives either 'payback' or condemnation from the students who have been punished (or their friends) for bullying, and may then be socially marginalised.*

3. *The bullying goes underground for a while and sometimes other students bully on behalf of the students who were punished.*

4. *The next time the student is bullied they decide to remain silent about it and assure the teacher that the bullying has stopped.*

Recommendation # 1 *(cont)*

Other students who are bullied are less likely to ask a teacher for support when they become aware of this dynamic. Secrecy empowers students who bully. When no one talks about bullying, students who bully feel they can carry on without consequences.

A punitive response by the school may ultimately be necessary in some circumstances. However, an approach which initially engages students who are bullying and attempts to enhance their feelings of empathy and understanding for the student they are harming is more likely to bring about a change in behaviour (Cross et al., 2004; Tyler, 1998).

Fear of retaliation and social exclusion as a result of peers being punished often prevents students from letting teachers know that they are being bullied (Rigby & Barnes, 2002). Students perceive that the best way for a school to respond to a bullying situation is to find a way for students who are being bullied to rationally work through the problem with the aggressor (Gamliel et al., 2003). However, more than simple mediation is required because it inappropriate for mediation to be used in situations where one student is clearly the aggressor. The Support Group Method (Robinson & Maines, 2008), the Method of Shared Concern (Rigby & Griffiths, 2007) or Restorative Practices (Armstrong & Thorsborne, 2006) can be used as a first step in responding to many bullying situations.

The dynamic of 'blaming the victim'

The 'Belief in a Just World' theory (Montada & Lerner, 1998) refers to the tendency of most people to want to believe that the world they live in is 'just' and not unfair. Therefore, when students, teachers and parents witness (or know about) a student who is being unfairly treated, they can find this injustice difficult to explain to themselves. To make themselves feel better and safer, people may search for things that the other has done to deserve the mistreatment they are experiencing.

This 'blame the victim' dynamic can be detected in how many students or teachers respond to bullying situations. For example: a student who talks to a teacher about being bullied might be asked, 'what did you do to deserve it?'; or a teacher, when talking to parents about their complaint that their daughter being bullied, might comment several times on their daughter's poor social skills, implying that she is the 'cause' of her own mistreatment.

Several researchers (e.g. Gini, 2008; Hara, 2002; Teräsahjo & Salmilvalli, 2003) have demonstrated that children (especially boys) tend to blame the student whom they are bullying for their own plight. They underestimate their bullying behaviour by constructing it as a harmless 'game' and claim that is justifiable behaviour because the real problem is the 'deviance' of the student. Teräsahjo & Salmilvalli (2003) also showed that many bullied students accept this construction of what is happening and in turn blame themselves for being bullied. Students who blame themselves are less likely to seek support and more likely to 'suffer in silence' (Graham et al., 2006).

To further illustrate the call for a Human Rights Focus that perceives bullying and cyberbullying as NOT just minor problems of "Mean Behaviour" but are **Acts and Comments of Discrimination** Against the Rights of ALL Australian Citizens, especially against our Children and Young People.

Recommendation # 1 *(cont)*

A good example that pulls ALL of the Bullying and CyberbBullying Components together and illustrates WHY I recommend we need to TAKE a:

1 HUMAN RIGHTS Approach with a

2 Top Down, REVERSE ONUS of PROOF with a

3 Power NEUTRAL Dialogue of an

4 ACT or COMMENT of DISCRIMINATION

Are best illustrated in understanding the different WAYS people and especially children engage in SOCIAL POSITIONING as described in;

"**The dynamic of rejecting difference and imposing conformity"** which identifies the many levels of Bullying and Cyberbullying as described in the National Safe Schools Framework Reference Section. (Appendix 03)

"The dynamic of rejecting difference and imposing conformity"

O'Brien has described bullying as a 'demonstration of the norms of young people's social groups, outlawing and punishing those who do not conform' (2007:297).

The most common explanation given by students to explain why some peers bully a classmate is that the classmate is different or 'deviant' in some way (Bosacki et al., 2006; Buchanan & Winzer, 2001; DeRoiser & Mercer, 2009; Frisén et al., 2008; Hamarus & Kaikkonen, 2008; Hazler & Hoover, 1993; Hoover et al., 1992; Teräsahjo & Salmivalli, 2003; Thornberg, 2010; Varjas et al., 2008).

Such 'differences' may relate to their appearance, their speech, their preferences, with whom they spend time, their family and their circumstances, their sexual orientation, their interests and achievements, or a disability of some kind (Thornberg, 2010). The process of rejecting and isolating those who are different is part of an attempt to affirm the 'correct' way to be and highlight supposed superiority. This conformity process creates apprehension in students that their own social inclusion might be threatened if they dress, speak or act in the 'wrong' way (Thornberg, 2010), and some steps to reduce this apprehension can including taking part in bullying the 'stigmatised' student in order to disassociate themselves from him/her.

Recommendation # 2

Establish a National Child and Young Persons Human Rights Council

Details of:
Recommendations for Joint Parliamentary Committee on Cybersafety (cont)

Recommendation # 2

Establish a National Child and Young Persons Human Rights Council

Assist the Australian National Child and Young Persons Human Rights Commissioner to establish and chair a **National Child and Young Persons Human Rights Council**.

2.1 Members of this Council to include representative from, Education, Health, Justice, Police, Research, Industry, Community Development and Community Support Agencies.

The National Child and Young Persons Human Rights Council will actively promote the **United Nations Convention on the Rights of the Child (1989)**, by educating the Community that bullying and cyberbullying are NOT just minor problems of "Mean Behaviour" but are **Acts and Comments of Discrimination** Against the Rights of ALL Australian Citizens, especially against our Children and Young People.

2.1 **United Nations Convention on the Rights of the Child (1989)**
(see Appendix 02)

Comment

While the Convention on the Rights of the Child aims at protecting children from Discrimination in some of the worst places in the World, we should not forget our own children and attempt to raise the standards or respect and protection for all children to be free from discrimination, violence, exploitation and abuse.

The Convention on the Rights of the Child (CROC) is an International Convention that protects your right as a child and youth up to the age of eighteen.

The UN Convention on the Rights of the Child states that all children are entitled to the same rights, regardless of the child's, or their parent's or legal guardian's race, colour, sex, language, religion, political or other opinion, national, ethnic or social origin, property, disability, birth or other status.

However, discrimination is a daily reality for millions of the world's children. When children are discriminated against they can be denied access to essential care and services. They can be excluded from school or unable to get essential medical treatment. Discrimination can also result in violence or exploitation. Many of the children exploited in the worst forms of child labour, for example, come from minority or excluded groups

Recommendation # 2 *(cont)*

Some of the relevant Children's Rights include the following:

- **Protection from all forms of discrimination** (Article 2)
- **You have the right to life** (Article 6)
- **You have the right to freedom of expression and information if it is done lawfully** (Article 13)
- **You are to be protected from neglect and abuse** (Article 19)
- **You have the right to education** (Article 28)
- **Indigenous children and those belonging to a minority group have the right to practice your own religion and culture, and use your own language (Article 30)**
- **You have the right to take part in leisure, recreation and cultural activities** (Article 31)
- **You should be protected from sexual exploitation and abuse** (Article 34)
- **You must not be subject to torture or any other cruel punishment** (Article 37)
- **Your freedom and liberty should not be unlawfully taken from you** (Article 37)
- **You have rights that relate to the administration of justice and criminal procedure including the right to support in preparation and presentation of a defence to any charges brought against you (Article 40)**

Appendix 02

Extract

http://www.ncylc.org.au/croc/what.html

The Convention on the Rights of the Child (CROC) - International Treaty

Australian Signatory

AUSTRALIAN TREATY SERIES

1991 No. 4

Convention on the Rights of the Child
(New York, 20 November 1989)
Entry into force generally: 2 September 1990

Entry into force for Australia: 16 January 1991

Recommendation # 2 *(cont)*

[Extract Summary]

Background Note:

The United Nations has sought to set out the rights of children, either directly or indirectly, in most of its 80 human rights treaties.
However, in 1989, ten years after work began on its drafting, the nations of the world agreed to adopt the ***Convention on the Rights of the Child.***
The Convention sets out, amongst other things, children's right to education, health care and economic opportunity; protection from abuse, neglect and sexual and economic exploitation. It also says that decisions that affect kids should be based on their 'best interests'.
Since it was adopted, the Convention has become the world's most widely ratified human rights treaty. This puts an important responsibility on the governments of the world to do all they can to promote and protect the rights of children and young people.

Child protection from discrimination, violence, exploitation and abuse

The UN Convention on the Rights of the Child states that all children are entitled to the same rights, regardless of the child's, or their parent's or legal guardian's race, colour, sex, language, religion, political or other opinion, national, ethnic or social origin, property, disability, birth or other status.
However, discrimination is a daily reality for millions of the world's children. When children are discriminated against they can be denied access to essential care and services. They can be excluded from school or unable to get essential medical treatment. Discrimination can also result in violence or exploitation. Many of the children exploited in the worst forms of child labour, for example, come from minority or excluded groups.

Convention on the Rights of the Child (CROC)

The Convention on the Rights of the Child (CROC) is an International Convention that protects your right as a child and youth up to the age of eighteen. While it is quite lengthy, the overall message is the same. You have rights and it is important that they are upheld and recognised. Here are some of the rights identified in CROC:

- ***Protection from all forms of discrimination*** *(Article 2)*
- *All decisions made about you must be in your best interest (Article 3)*
- ***You have the right to life*** *(Article 6)*
- *You have a right to a name and the right to acquire a nationality (Article 7)*
- *You have a right to know about your identity such as your nationality, name and family (Article 8)*
- *You can't be separated from your parents if it is against your will or in our best interest (Article 9)*

Recommendation # 2 *(cont)*

- *If you are capable of forming your own views you also have the right to express your views (Article 12)*
- ***You have the right to freedom of expression and information if it is done lawfully*** *(Article 13)*
- *You have the right to freedom of thought, conscience and religion (Article 14)*
- *You have the right to privacy (Article 16)*
- *You have the right to obtain information, especially information that will benefit you, and you should be able to access this information through the media (Article 17)*
- ***You are to be protected from neglect and abuse*** *(Article 19)*
- *Child refugees have the right to special assistance and protection (Article 22)*
- *Disabled children have the right to special care (Article 26)*
- *You have the right to the best possible health services (Article 24)*
- *You have the right to benefit from social security (Article 26)*
- *You have the right to an adequate standard of living (Article 27)*
- ***You have the right to education*** *(Article 28)*
- *Indigenous children and those belonging to a minority group have the right to practice your own religion and culture, and use your own language (Article 30)*
- ***You have the right to take part in leisure, recreation and cultural activities*** *(Article 31)*
- *You should be protected from economic exploitation and work which harms your development and/or education (Article 32)*
- *You should be protected from illegal drugs (Article 33)*
- ***You should be protected from sexual exploitation and abuse*** *(Article 34)*
- *You have the right to be protected or prevented from abduction, sale or trafficking and all other forms of exploitation (Article 35 and 36)*
- ***You must not be subject to torture or any other cruel punishment*** *(Article 37)*
- ***Your freedom and liberty should not be unlawfully taken from you*** *(Article 37)*
- *Under no circumstances should you be sentenced to death or life imprisonment (Article 37)*
- *If you have faced neglect, abuse or punishment, you have the right to rehabilitative care (Article 39)*
- *You have rights that relate to the administration of justice and criminal procedure including the right to support in preparation and presentation of a defence to any charges brought against you (Article 40)*

Recommendation # 3

Promote the United Nations Convention on the Rights of the Child (1989)

Details of:
Recommendations for Joint Parliamentary Committee on Cybersafety (cont)

Recommendation # 3

Promote the United Nations Convention on the Rights of the Child (1989)

(see Appendix 02)

The National Child and Young Persons Human Rights Council will actively promote the **United Nations Convention on the Rights of the Child (1989)**, and help establish a "**Best Practice" Set of Laws** for **Acts and Comments of Discrimination** when dealing with bullying and cyberbullying incidents.

Members of the Council are charged with the responsibility for helping to:

3.1 **Establish a National Relevant Set of Laws**

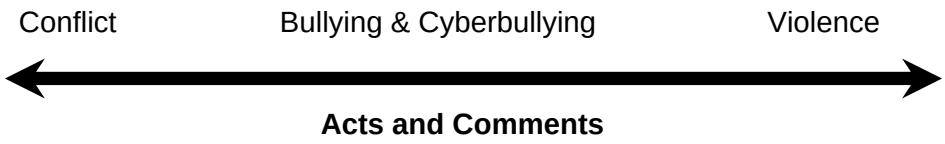
Establish a **National Relevant Set of Laws** that protect victims of Acts and Comments of Discrimination in serious bullying and cyberbullying incidents. – The **Commonwealth Criminal Code 1995 Laws** provide a Base Line Set to add and modify to suit a National Jurisdiction. *(See Appendix 04)*

3.2 **Define the Rights of Children & Young People with relation to Acts of Discrimination**

i.e. Develop the concept and definition of a Behaviour Continuum of Bullying and Cyber – Bullying Model, such as proposed by the Author, Stewart Healley.

Appendix 05

This Continuum positions Acts and Comments of Bullying and Cyberbullying between Acts & Comments of Conflict through to Acts & Comments of Violence. e.g.:



Comment

Unfortunately, the current debate and focus on Bullying and Cyberbullying has targeted the school as the main identity responsible for dealing with "Inappropriate Behaviour"; followed by the Parents and / or Caregivers; then by the Community Agencies such as Psychologists and Researchers with a plethora of new Approaches, some of which offer excellent conflict resolution models and are researched based and validated in the real world application.

Recommendation # 3 *(cont)*

However, I am seriously concerned that the current debate and focus on "**irresponsible student behaviour"** and "**misbehaviour**" has been slowly but effectively "hijacked" to a certain degree by the "Media" and some "Experts", pushing their own form of "self interest, profit and promotion". This situation has pushed the very idea of any form of Police or Legal Action as just too "Punitive" to contemplate, let alone be considered as a necessary and valuable part of a "Best Practice Model" dealing with Bullying and Cyberbullying behaviour.

In preparing this submission, an analysis of bullying and cyberbullying components have been reviewed from a traditional and contemporary approach. I have tried to offer an analysis for a practical and workable Model that requires a Holistic, International and Local focus.

The caption of **"*Think Global act Local*"** is especially relevant in this review

Recommendation # 3 *(cont)*

Appendix 06

WA Department of Education and Training - *"Managing Student Behaviour" Pamphlet*

A quotation from Pamphlet will illustrate this point.

> ***Managing extreme behaviour***
>
> *We believe that, even with those students who have been suspended and become alienated from school by their extreme behaviour, there is still scope to re-engage these students. By facing up to what effect their behaviour has had and by making an effort to put things right, students can restore damaged relationships and be re-connected with the school.*
>
> *Those students whose circumstances make it difficult for them to succeed at school often exhibit unproductive behaviours*
>
> *Reacting to these unwanted behaviours in a* ***punitive or narrow behavioural control sense*** *is not the way to go. These students first need an appropriate curriculum and understanding teachers who develop strategies to engage them in learning. They also need, like all other students, clear limits and consistent consequences so they can learn behaviours that are acceptable at school. In other words, while their behaviour certainly needs to be managed, it is best to take a broad view of the management strategies and use successful engagement in learning as the desired outcome rather than simply trying to eliminate the misbehaviour.*
>
> *For those students who persistently engage in* ***extremely disruptive behaviour****, our* ***school psychologists*** *will help school staff to enable them to put in place individual programs to manage the behaviour and learning of these students. For those who simply cannot be managed in a normal classroom we will provide alternative placements that will give them the intensive help they need with the aim of reintegrating them back into mainstream classes wherever possible.*
>
> ***We will not allow persistent disruptive, aggressive behaviour to continue to interfere with the school's work. We accept that some students can only progress in a different environment to the normal mainstream classroom and as a system we are committed to providing such alternatives for the small percentage of students who need them.***
>
> ***Matching support to need***
>
> *We accept that some schools have more difficult student behaviour to deal with than others. Community and family circumstances can significantly affect a student's ability to meet the school's behavioural expectations. It is only fair that we provide those schools with a higher level of support than schools where the great majority of students*

Recommendation # 3 *(cont)*

come to school ready to learn. In the future we will ensure these schools receive a greater share of the time of support services such as school psychologists.
We would also want to assert that our teachers deserve to be respected – and to be able to teach and be safe from threats, insults and harassment. On occasions the behaviour of students is beyond what any employee behaving as a responsible professional should be subject to. The Department will take strong action to ensure our staff have a safe workplace.

Enlisting outside support

The school system cannot manage the most difficult and complex cases alone. The behaviour of these students is a symptom of problems well beyond the school. Our teachers should be held accountable for using the most effective educational strategies to help students progress, but these strategies will only be effective if they are part of a broader intervention that is beyond the brief of education. We will therefore take the initiative to build productive, cooperative approaches by all agencies that exist to support these students and their families. Finally, we will take every opportunity to publicly promote the position that student behaviour is a shared responsibility between school and home. It is unrealistic for society to expect schools to shoulder the total burden of ***irresponsible student behaviour****. While schools can and should act to prevent* ***misbehaviour*** *in school and to manage it well when it does occur, parents also have a significant influence on their children's behaviour. We are likely to have much greater success if all parties play their part.*

In my work as a **Youth Worker in High Schools** I am the first to fight for students to "negotiate" issues and problems, which includes "conflict resolution" by whatever Model that produces a positive outcome for all parties.

However, my previous 11 years as an operational **Police Officer** have given me the knowledge and experience to know however few in number, whatever conflict resolution methods you employ there are some children and adults that do not wish to alter their behaviour choices and see that they have a right to do whatever, wherever, whenever they chose and that includes inflicting pain and suffering on others with an attitude of **"who's going to stop me, then!"**

When you analyse the research studies for the various conflict resolution models you will find that there are always some examples where the results have not always been so positive and the situations have not always improved or been resolved. This is where the next step of a Best Practice Model should include the involvement of another "Expert Agency" the **Local Police**.

However there is an enormous "**Gap**" in this next step as the **Local Police** are:

1. Generally, reluctant to engage in "Misbehaviour" incidents – "**not really a crime**"

2. Advise an easy option for Victim (and self) to attend Magistrates Court for an intervention / AVO with the "**condition to not contact**"

Recommendation # 3 *(cont)*

3. The Police have to pay a "**substantial fee**" for requesting Account Details from Service Providers in a **Non-Life threatening situation**.

4. Reluctance from experience of doing all the investigation work for a brief to have the Offenders Solicitor convince the Magistrate to treat the incident lightly with a warning and no penalty or even dismissed the Charges, reinforcing the Court Message to the Offender "go do what you like" and to the Victim – "**SORRY**".

Appendix 07

"Bullying is it a Crime?"
The SPRESS; Headspace & AFP - Bullying & Cyberbullying Pamphlet– May 2010

A Mixed Message on the Law - a quotation from:-

"Cyber bullying could be a crime?"

Knowing how to report it, how to block it and how to prevent it can help you to take action or assist your friends if it is happening to you or someone you know.

Blocking Cyber Bullies

Often ignoring cyber bullying can be a simple way of making it stop. One way to ignore it is by blocking the communications from people who cyber are bullying you. ThinkUKnow has a fantastic step-by-step guide on how to do this across Facebook, MySpace, MSN, Bebo, Twitter, YouTube, mobile phones and other websites (see www.thinkuknow.org.au/site/stop.asp)

For example, in Facebook you can:

- *Go to the "Privacy" page and enter the person's name in the "Block" search field at the bottom of the page;*
- *Remove the person from your friend list;*
- *Save a copy and then delete any comments they have made on your profile;*
- *Save a copy and then delete any emails they have sent you through your Facebook inbox without opening them;*
- *If someone has posted an image of you without your permission and named you in the photo, You can remove your name from the photo by selecting the "Remove Tag" option. Ask the person who posted the image to take it down. Facebook cannot force people to remove photos unless they violate the Terms of Use. If someone is constantly tagging you in embarrassing or inappropriate photos, remove them from your friend list so that they will no longer be able to tag you in photos;*
- *If someone has posted an offensive note, you can report this to Facebook using the "Report this Note" link under each note.*

Recommendation # 3 *(cont)*

Facebook administrators may also take action against the person who is cyber bullying. This might be temporarily banning them from the site, shutting down their account or even blocking them from starting up a new account. If it is occurring via your mobile phone, you can contact your mobile phone provider to report nuisance calls and/or text messages.

If someone sends you a link to a website which is cyber bullying someone, or an email which is spreading rumours about someone, don't forward it on. Delete the message and let the person know that you don't want to receive any more. If you are passing on these cyber bullying messages, you are contributing to the problem.

If the cyber bullying is occurring between you and someone who goes to your school, you can report it to the school. Schools often have policies and guidelines in place to deal with bullying and implement solutions. The most appropriate people to speak to include your teacher, school counsellor or pastoral care coordinator.

If the cyber bullying escalates and you are genuinely fearful for your safety and well being, you can make a report to your local police (find your local police via the White Pages).

It helps when reporting cyber bullying to have a record of what's been said/posted/texted. For example, chat logs, copies of emails or screenshots of websites. Providing this information will assist in understanding what has occurred and how to address the problem.

Is cyber bullying a crime?

Many of the laws in Australia relating to threats and harassment were created before the internet became a part of our everyday lives. But these laws could be used in dealing with offensive behaviour online, such as serious cases of cyber bullying. In particular, where there is a specific threat to someone's physical safety and well being, state and territory laws relating to threatening and harassing behaviour might be used.

Police are often reluctant to charge young people with criminal offences where other, less punitive, measures can be used. This may involve the use of restorative justice, where the person who has been cyber bullied and the people doing the cyber bullying (as well as their support network) are brought together to talk through the issues and come up with an agreed solution. Other options include cautions or disciplinary action taken by schools or parents.

Top tips for preventing cyber bullying

- *If you're not friends with someone offline, don't add them as a friend online;*
- *Set your online profiles and accounts to private so that you can control who has access to them;*
- *Be careful who you share your phone number, email address and user IDs with;*
- *If a relationship ends badly, consider removing that person from your contact/buddy list;*
- *Think before you post! If you post something mean on someone's profile, it could encourage them to cyber bully you in retaliation;*

Recommendation # 3 *(cont)*

- *Learn how to block communications on the sites and applications you use and where to report cyber bullying;*
- *Find out your school's policy on cyber bullying and who you can talk to;*
- *Don't share your password with anyone, not even your best friend!*
- *Make sure you log out of your accounts properly so that someone can't access your accounts and deface your profile;*
- *Take a stand against cyber bullying. Talk with your school about what you can do to send the message that cyber bullying is NOT acceptable!*

Cyber bullying can happen to anyone. It can be upsetting and stressful, impacting on different areas of your life, including; self-esteem, relationships, work or study.

But there is help available. Talking to someone is a good starting point, particularly if you are feeling unsafe or frightened. See www. headspace.org.au to find help and support.

Appendix 08

Cyber bullying, e-crime and the protection of children and young people
Coalition to Decrease Bullying, Harassment and Violence in South Australian Schools

Another Mixed Message on the Law - a quotation from:-

Extract:

What is cyber bullying?

E-technology *provides individuals with a powerful means of communicating instantly with others in both a positive and negative ways.*

Cyberbullying is bullying which uses e-technology as a means of victimising others. It is the use of an internet service or mobile technologies – such as e-mail, chat rooms, discussion groups, instant messaging, WebPages or SMS (text messaging) – with the intention of harming another person.

Examples *can include communications that seek to intimidate, control, manipulate, put down or humiliate the recipient.*

Recommendation # 3 *(cont)*

Activities *can include repeated negative messages, sexual and racist harassment, denigration, impersonation, trickery, exclusion and cyber stalking.*

Cyberbullying may involve varying levels of severity, ranging from occasional messages to frequently repeated and highly disturbing threats to a person's life.

The targeted person often feels powerless and may need help.

Cyber bullying can be an e-crime, a fact often not clearly understood by those involved.

Examples from the South Australian Police (SAPOL)

1. Sexting may be an e-crime

With my mobile phone I took a photo of my girlfriend naked and sent it by text to everyone. What a laugh!

Offence: *Production or dissemination of child pornography*
Maximum penalty*: Imprisonment for 10 years*

2. Impersonation may be an e-crime

I got into their e-mail account and sent abusive e-mails to everyone in the address book.

Offence: *Unlawful operation of a computer system.*
Maximum penalty*: Imprisonment for 6 Months or $2,500*

3. Intimidation may be an e-crime

He told me if I didn't do what he said he would put that photo on the internet and tell all my friends. I was so embarrassed.

Offence: *Blackmail*
Maximum penalty*: Imprisonment for 15 years*

4. Harassment may be an e-crime

I created a Website about X and we all put some stuff on there about how much they and everyone else like them are hated.

Offence: *Racial Vilification*
Maximum penalty*: Imprisonment for 3 years, or $5,000 or both.*

Recommendation # 3 *(cont)*

Other offences - Using internet or mobile phone carriers:

- ***For suicide-related material***

  Maximum penalty: *$100,000*

- ***To make a Threat***

  Maximum penalty: *Imprisonment for 7 Years*

- ***To menace, harass or cause offence***

  Maximum penalty: *Imprisonment for 3 Years*

Seek support

Use the contacts in this pamphlet if you are concerned about changes in your child's behaviour. For example you could contact ACMA to request the removal of offensive or illegal content from a website.

Recommendation # 3 *(cont)*

Appendix 07

"Bullying is it a Crime?"
The SPRESS; Headspace & AFP - Bullying & Cyberbullying Pamphlet– May 2010

Comment:

This pamphlet also presents a vague message with both **Negative** and **Positive Messages** in the fight against Cyberbullying.

The Negative Messages:

1. The opening statement - ***"Cyber bullying could be a crime?"-*** is still a negative message.

2. The next statement – *"**Police are often reluctant to charge young people with criminal offences"*** – again is a negative message.

3. The **Example** chosen while **legally accurate** are again delivering a negative message in that the likely hood that a child or young person would be **Charged** with the **Offences** and **Penalties** are **unrealistic** and **too punitive** to **worry any child or young person** and hence **lose their effectiveness as a warning completely**.

4. A summary of the **examples** is as follows:

Examples:

1. *Production or dissemination of child pornography = Penalty 10 Years Imprisonment*
2. *Unlawful operation of a computer system = Penalty 6 Months or $2,500*
3. *Blackmail = Penalty 15 Years Imprisonment*
4. *Racial Vilification = Penalty 3 Years and/or $5,000*
5. *Suicide related Material = Penalty 3 years + $100,000*
6. *To make a Threat = Penalty 7 years*
7. *To menace, harass or cause offence = Penalty 3 years*

If these Laws are the best the South Australian Police can consider apply to the various ways of Cyberbullying, then I am not surprised that the "**Police are often reluctant to charge young people with criminal offences".**

Recommendation # 3 *(cont)*

The Positive Message:

Fortunately, there is contained a **Positive Message** in the Police statement that refers to a **Restorative Justice Pathway Approach** e.g.:

"Police are often reluctant to charge young people with criminal offences ***where other, less punitive, measures can be used. This may involve the use of restorative justice, where the person who has been cyber bullied and the people doing the cyber bullying (as well as their support network) are brought together to talk through the issues and come up with an agreed solution. Other options include cautions or disciplinary action taken by schools or parents."***

This Restorative Justice alternative is regarded as a "less punitive" method of dealing with cyberbullying is worth further exploration.

To establish a "Best Practice Model" for Schools to deal with Bullying and Cyberbullying also requires the inclusion of a "Best Practice of Appropriate Laws and Legal Processes" for dealing with bullying and cyberbullying.

It is my recommendation that a "**Best Practice Model for Schools with Appropriate Laws and Legal Framework**"

Should contain the following components:

1. Initial use of alternative **"Conflict Resolution Models**" to be used in Schools.

1.1. **Shared Concerns** Model

1.2. **Group Support** Model

1.3. **Support Circles** Model

1.4. **Mediation** Model

1.5. **Restorative Practice** – Schools Model

2. Student Support and Student Behaviour Management Model

3. Pastoral Care and Wellbeing Model

I am pleased to say that the latest National Safe schools Framework released on the 18th March, 2011 (see Appendix 03) does cover the above components in a framework model only without a practical base line model to work from.

Recommendation # 3 *(cont)*

Never the less, it is still progress even though at times it is slow going.

However to have a good "Best Practice Schools Model we need to add a few more components.

These additional components should contain the following Models:

4. **Magistrate Court Model** - Application for Intervention Order / Apprehended Violence Order

5. **Mandatory Reporting Model** for serious cases of Emotional Abuse from incidents of Bullying and Cyberbullying. While intimidation is often the aim of Bullying and Cyberbullying, sometimes the Emotional Harm done is greater than that intended, needing expert psychological support and treatment for the victim.

6. Criminal Behaviour Model with Police Investigation and Charges for serious cases of Bullying and Cyberbullying with a **Magistrate Children's Court Pathway**.

7. Criminal Behaviour Model with Police Investigation and Charges for serious cases of Bullying and Cyberbullying with a Police Caution with a **Voluntary Restorative Justice Pathway.**

8. **"Respect It or Lose It" – Cyber Safety Model** (see Appendix 10)

To assist the successful implementation of Component # 7, the **Criminal Behaviour Model** with a Restorative Justice Pathway, the Author, Stewart Healley has proposed a practical

"Respect It or Lose It" – Cyber Safety Model.
This Model proposes that with some additional modifications the **Commonwealth Criminal Code 1995 Laws** should be used as a Base Line **"Best Practice Set of Laws"** for **Acts and Comments of Discrimination** when dealing with bullying and cyberbullying incidents.
E.g. need to add a Stalking Law (see Appendix 04)

9. **"*Behaviour Continuum Model of Bullying and Cyber – Bullying"*** (see Appendix 05)

One more Model needs to be included in the "**Best Practice Model for Schools"** to help in assessing the most appropriate Level and Method of Response to an incident of Bullying and Cyberbullying.

Recommendation # 3 *(cont)*

This is a ***Behaviour Continuum Model of Bullying and Cyber - Bullying*** proposed by the Author, Stewart Healley, 2011.

This final model proposes that practical unbiased decisions need to be made as to the seriousness of any **Act and/or Comment of Discrimination** when dealing with a bullying and/or cyberbullying incident/s.

The Model present a **continuum of behaviour** stretching from incidents of physical and/or mental **conflict** to incidents of physical and/or mental **violence**, with the area in between filled with incidents of **Bullying and/or Cyberbullying** with varying levels of seriousness.

To assist a "**Best Practice Model for Schools"** it would be proposed that one of the first tasks for the **National Child and Young Persons Human Rights Council**, would be to work with an Expert Working Group to match relevant scenarios of Bullying and Cyberbullying to the various levels on the Behaviour Continuum, mapping out the seriousness of acts and comments of the offender, towards the victim with appropriate responses.

Example 1, it may be that on the

Discrimination on Physical Wellbeing - Physical Conflict, Harassment, Violence & Assault Scale

- **Physical Assault** by Individual = P-Level 5 may constitute a **Police Response**.

Example 2, it may be that on the

Discrimination on Mental Wellbeing - Mental Conflict, Harassment, Violence & Attack

- **Social Attack** – Individual Comments = M-Level 5 may constitute a **Police Response**.

(See Appendix 05 - Behaviour Continuum of Bullying and Cyberbullying Definitions)

Recommendation # 3 *(cont)*

Appendix 05

Behaviour Continuum of Bullying and Cyber - Bullying Discrimination - *Definitions:*

1. ***Conflict:***
   A disagreement where the needs of one or both parties are not being met. It does not necessarily involve an abuse of power, even if parties do not have perceived equal power. If handled well, conflict is seen as an opportunity for personal growth.
2. ***Harassment:***
   Negative behaviour intended to annoy or trouble another individual, which may be based on obvious differences such as gender, race, religious or cultural beliefs, physical difference, sexual orientation, ability or disability and socio-economic status. It may be a one-off incident between individuals or groups or may continue over time.

3. ***Bullying:***
   A product of social dynamics which can be defined as the repeated negative actions by individuals or groups against a target individual or group, which involves an imbalance of power. Bullying can take different forms – physical, social, or psychological. Actions can be observable (overt) or hidden (covert).

4. ***Cyberbullying:***
   A product of social dynamics which can be defined as the repeated negative comments by individuals or groups against a target individual or group, which involves an imbalance of power. Cyberbullying can take different forms – verbal, social, cyber or psychological. Comments can be observable (overt) or hidden (covert).

5. ***Assault:***
   An intended Physical Assault on an Individual or Group, by another Individual or Group. It could be physically baiting, humiliating or provoking an individuals or group to physically retaliate providing a public opportunity to exploit a power imbalance and or to deliberately provide a opportunity to cause pain and suffering to another less powerful or outnumbered individual or group. It may be a one-off incident between individuals or groups or may continue over time.

6. ***Attack:***
   An intended Social Attack on an Individual or Group, by another Individual or Group. It could be posting comments on Mobile Phone, Web Sites & Social Web Pages
   It could be posting or distributing personal images un-altered or altered, it could be "Happy Slapping Events, considered to be child abuse or child pornographic video material. It may be a one-off incident between individuals or groups or may continue over time

7. ***Violence:***
   Incidents where a person or group is intimidated, abused, threatened, physically assaulted or where property is deliberately damaged by another person or group. It is an extreme use of force often resulting in injury or destruction. Violence does not necessarily involve an imbalance of power.

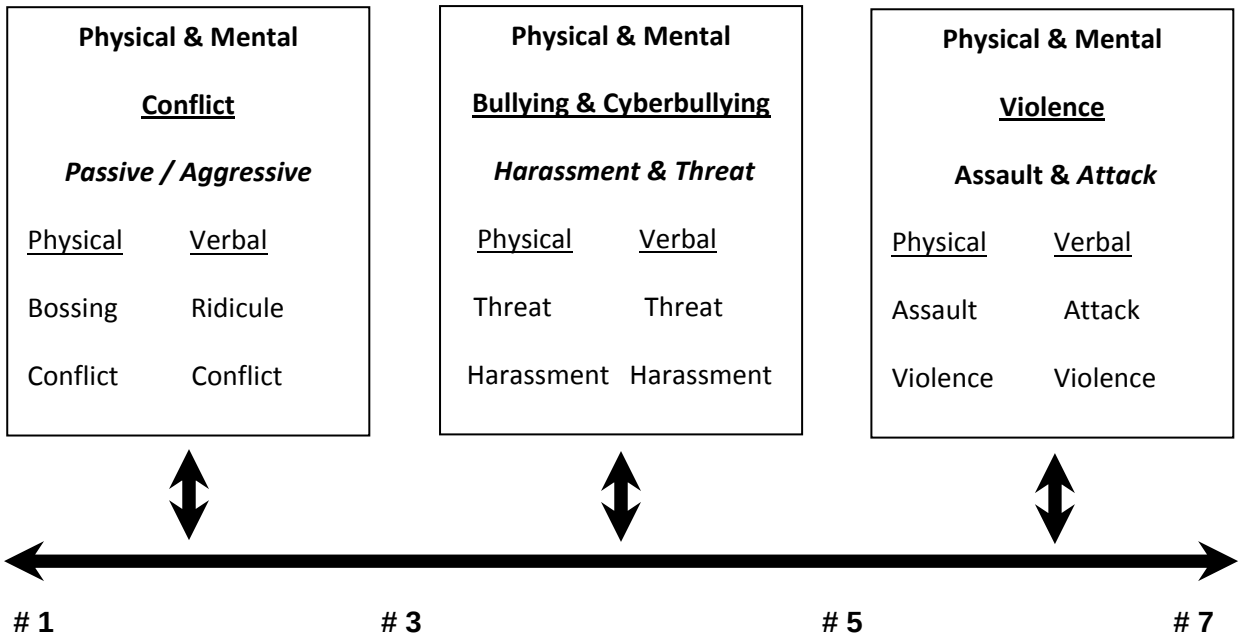
Recommendation # 3 *(cont)*

Reference 05: Best Practice Model for Schools - Stewart Healley - 2011

Behaviour Continuum of Bullying and Cyber – Bullying Discrimination

Seriousness of Acts and Comments of Offender towards the Victim

Behaviour Continuum



Discrimination Against the Physical and Mental Wellbeing of a Child / Adult

Discrimination on Physical Wellbeing - Physical Conflict, Harassment, Violence & Assault

- Physical Conflict…… P - Level 1
- Physical Harassment. …… P - Level 2
- Physical Bullying by Individual…… P - Level 3
- Physical Bullying by Group..... . P - Level 4
- Physical Assault by Individual …… P - Level 5
- Physical Assault by Group…… P - Level 6
- Physical Violence…… P - Level 7

Discrimination on Mental Wellbeing - Mental Conflict, Harassment, Violence & Attack

- Social Conflict - Comments …… M - Level 1
- Social Harassment - Comments…… M - Level 2.
- Social Cyberbullying - Individual Comments..... M - Level 3
- Social Cyberbullying - Group Comments…… M - Level 4
- Social Attack - Individual Comments..... M - Level 5
- Social Attack - Group Comments…… M - Level 6
- Social Violence - Comments…… M - Level 7

Recommendation # 3 *(cont)*

Cyberbullying Scenarios:

Examples of what the **National Child and Young Persons Human Rights Council**, working with an Expert Working Group, would involve in establishing a "**Best Practice Model for Schools"** and matching relevant scenarios of Bullying and Cyberbullying to the various levels on the Behaviour Continuum are as follows:

Cyberbullying Scenarios – Hinduja & Patchin, 2010 - USA

Dr. Sameer Hinduja, is an assistant professor in the Department of Criminology and Criminal Justice at Florida Atlantic University
Dr. Justin W. Patchin, is an assistant Professor of Criminal Justice in the Department of Political science at the University of Wisconsin-Eau Claire
Together, they lecture across the United States on the causes and consequences of cyberbullying and offer comprehensive workshops for parents, teachers, counselors, mental health professionals, law enforcement, youth and others concerned with addressing and preventing online aggression.

Their book, Bullying Beyond the Schoolyard: Preventing, and Responding to Cyberbullying, is available from Sage Publications (Corwin Press)
Website: www.cyberbullying.us.

The Cyberbullying Research Center is dedicated to providing up-to-date information about the nature, extent, causes, and consequences of cyberbullying among adolescents.

Reference 01: Extract: Cyberbullying Scenarios – Hinduja & Patchin, 2010 - USA

Scenario 1

James is frustrated and saddened by the comments his high school peers are making about his sexuality. Furthermore, it appears a group of male students are creating fake email accounts at Yahoo.com and are sending love notes to other male students as if they came from James—who is mortified at the thought of what is happening.

If you were a guidance school counselor or administrator within the school, what would you do if James approached you with the problem? What about if you were James's mom or dad? What can James do to deal with the embarrassment? What would be some incorrect and unacceptable ways that James might try to deal with this problem?

Scenario 2

Two female sixth graders, Katie and Sarah, are exchanging malicious instant messages back and forth because of a misunderstanding involving a boy named Jacob. The statements escalate in viciousness from trivial name calling to very vicious and inflammatory statements, including death threats.

Should the police be contacted?

Recommendation # 3 *(cont)*

Reference 01: Extracts: Cyberbullying Scenarios – Hinduja & Patchin, 2010 – USA (cont)

Are both girls wrong? What should the kids do in this instance? What would you do as a parent if you discovered this problem? What might a school counselor do?

Scenario 3

A mother is walking by her son Jonathan while he is on the computer and notices that he keeps hiding the screen when she walks by. Upon further observation, the mother sees that Jonathan is making fun of someone else via instant messaging.

What should the mother do first? Does the mother need to contact the parents of the other child? Should Jonathan be allowed to use the computer?

Scenario 4

Lindsay has just moved to town from Oregon and enrolls in the local middle school. Very pretty, outgoing, and funny, she quickly wins the attention of a number of the school's football players—much to the chagrin of the school's cheerleaders. Bonnie, the head cheerleader, is concerned about Lindsay stealing away her boyfriend Johnny, who plays quarterback. With the help of her cheerleader friends, Bonnie decides to create a "We Hate Lindsay" Web site, where girls can post reasons why they hate Lindsay and why they think she should move back to Oregon. Soon, the entire school becomes aware of the site's Web address, and many others begin to post hurtful sentiments about Lindsay. Desperately wanting to make friends in a new town, Lindsay is crushed and begins to suffer from depression and a lack of desire to do anything aside from crying in bed.

If you were her mom or dad, what would you do? What might the school do to help Lindsay? If you were her best friend, what might you say or do to help?

Scenario 5

Chester, a tall, skinny teenager who excels in math and science classes, feels embarrassed when he has to change into gym clothes in the boy's locker room at school because he lacks muscularity and size. Other, more athletic and well built teens notice Chester's shyness and decide to exploit it. With their camera enabled cellular phones, they covertly take pictures of Chester without his shirt on and in his boxer shorts. These pictures are then circulated among the rest of the student body via cellular phone. Soon enough, boys and girls are pointing, snickering, and laughing at Chester as he walks down the school hallways. He overhears comments such as "There goes Bird Chested Chester" and "Wussy Boy" and "Chicken Legs Chester" and "Stick Boy." These words cut him deeply, and the perception that his classmates have of him begins to affect his math and science grades.

If you were his teacher, what would you do? If you were his parent, what would you do? What can Chester do to deal with the harassment—now and in the future? How can his harassing classmates really understand how much pain they are causing with their words and actions? What would you do if you were a bystander?

Recommendation # 3 *(cont)*

Reference 01: Extracts: Cyberbullying Scenarios – Hinduja & Patchin, 2010 – USA (cont)

Scenario 6

Heather is a fourth grader who is extremely proficient at using the Internet. On Monday, she receives an email from someone named "stalker@hotmail.com." The subject and body of the email state: "I'm watching you. Be afraid." Heather immediately deletes it and thinks nothing of it. On Tuesday, she receives another email from stalker@hotmail.com, and this time, the subject and body of the email state: "I am getting closer, and I see you on the computer right now as you read this." Heather starts to get worried but doesn't want to tell her parents because she is concerned they will take away her Internet privileges. On Wednesday, she awakens to a new email from stalker@hotmail.com that states: "Be very afraid. Today may be your last." Definitely frightened and concerned now, she makes up her mind to tell her parents about the emails when she returns from school that day. She is unable to concentrate in any of her classes because of intense fear as to what the email meant when it said: "Today may be your last." She rushes home after school, bent on bringing it up to her mom and dad as soon as she sees them. To her dismay, she finds a note on the table stating that her mom went grocery shopping and that her dad will be home late. Her palms begin to sweat and her heart begins to race. She goes to her bedroom, throws her backpack on her bed, and checks her email. Twenty-five new emails pop up. Each one is from the same sender: stalker@hotmail.com. They all say the same thing: "I am in your house. I am on a wireless Internet connection. You don't know where I am, but I know where you are!" Heather grabs her house key, rushes out of the front door, locks it, runs to her friend's house, and tells her friend's mom about her situation.

What would you do if you were her friend's mom? What can Heather do to ensure her safety now and in the future? To whom else should she turn for help?

Scenario 7

Stan is an eighth grader who is physically abused by his alcoholic uncle when he visits him on weekends. Additionally, Stan is being pushed around by some of his peers in middle school because he wears black all the time and is basically a loner. Recently, Stan has realized that on the Internet—in chat rooms and via instant messaging—he can freely become a person who seems much more attractive and fun and lighthearted than he is in real life. By taking on a different persona, he is finding social interaction with others much easier and more rewarding. Nonetheless, he still harbors much anger and bitterness within due to how his uncle and some of his classmates treat him. He decides to get back at his uncle and some of his classmates by posting personal information about them—along with some true stories about his negative experiences with them—on a very popular teen oriented message board. This information includes their cell phone numbers, their home phone numbers, and their home addresses. Because Stan has made many friends on this teen oriented message board, they rally around him in support and decide to exact some vigilante justice on their own to help Stan get revenge. A large number of his online friends use the phone numbers and addresses to make repeated prank calls, to order hundreds of pizzas to the victims' doors, and to sign them up for many, many pornographic magazines and Sears catalogs. Stan is extremely pleased at the harassment that his uncle and mean classmates are now experiencing.

Recommendation # 3 *(cont)*

Reference 01: Extracts: Cyberbullying Scenarios – Hinduja & Patchin, 2010 – USA (cont)

Scenario 7 (cont)

What would you do if you were a parent or school administrator and the police alerted you, themselves contacted by Sean's Internet service provider after an online complaint was filed by Stan's uncle about these incidents? How might Stan learn that such vengeful behavior is inappropriate? How might Stan get help for the abuse he suffers and the way he feels?

Scenario 8

Karen is a very devout teenager who leads a prayer meeting every morning by the high school flag pole. Many boys and girls are simply drawn to Karen as a friend because of her sweet nature and hopeful innocence. Other girls in her school, however, feel threatened by Karen's piety and commitment to holy living, and they begin to drum up ideas to expose her as a fraud. Specifically, they begin to spread rumors via the High School's social network on MySpace.com that Karen is sleeping around with the boy's track team. Karen is alerted to the online rumors by a close friend and is heartbroken. She tells her teachers and pastor, who then contact the school administration.

What would you do if you were the principal in this situation? What would you do if you were Karen? What would you do if you were Karen's close friend and really wanted to help? How could those who spread the rumors understand how hurtful their actions were?

Scenario 9

Casey loves playing video games on his computer, especially those that allow you to link up to and compete with other players across the world through the Internet. He recently met one teenager in Russia named Boris while playing video games online, and they became fast friends because both enjoyed and excelled at one particular game. Together, they became almost unbeatable whenever they competed as a team against other teams online. At some point, though, Casey told Boris he had found a better gaming partner and didn't want to play with Boris anymore. Boris was outraged that he was being "dumped" as a gaming partner for someone else, and he began to tell other people on the gaming network that Casey "sucked" at all video games and that no one should ever be his partner unless they wanted to lose really badly. Soon after these statements started circulating, Casey's new gaming partner dumped him, and everyone else on the network treated him like a pariah. Since the video game he loved so much could only be played with a partner, Casey was no longer able to play and felt totally rejected on the Internet (which had heretofore been a safe haven for him). When coupled with recollections of other instances of rejection in his life, this experience began to make Casey feel completely hopeless. He then started to express suicidal intentions to his sister.

If you were his sister, what would you say and do? Can this example really be characterized as cyberbullying?

Recommendation # 3 *(cont)*

Reference 01: Extracts: Cyberbullying Scenarios – Hinduja & Patchin, 2010 – USA (cont)

Scenario 10

Trevor is 16 and into drag racing. He and his friends often go down to the local drag strip and race other 16 and 17year olds in their souped up cars. Because drag racing is a testosterone heavy event, egos get involved quickly. Speed is often equated to masculinity and strength, and physical fights sometimes break out when winners gloat too much over losers of drag races. Local police have had to report to the drag strip often in recent weeks and have threatened to shut down the strip completely if any more fights occur. Therefore, the aggression has been transferred from the real world to cyberspace, and winners are gloating over, and making fun of, losers online through emails and public forum posts at the local drag racing Web site. Trevor is undefeated in his racing exploits, and this has given him a very inflated self conception His success has gotten to his head, and has been getting his kicks by berating and humiliating online those who lose against him. Some guys he has defeated are sick of how he's acting and are organizing a group to go over to his house, trash and mangle his hot rod with shovels and sledgehammers, and beat him up. Trevor gets tipped off about this plan the day before it is supposed to happen.

What should he do? Whom should he tell, and what should they do?

Recommendation # 4

Establish a Australian National Cyberbullying 24/7 Helpline and Reporting System

Details of:
Recommendations for Joint Parliamentary Committee on Cybersafety (cont)

Recommendation # 4

Establish a Australian National Cyberbullying 24/7 Helpline and Reporting System

The National Child and Young Persons Human Rights Council will actively work with The **Australian Communications and Media Authority (ACMA)**, to establish a **National Cyberbullying 24/7 Hotline and Reporting System** to help support individuals involved in cases of serious Cyberbullying.

4.1 **The Australian Communications and Media Authority (ACMA)** will monitor:

- **Victims**
    - The **National Reporting System** operated by ACMA will provide a **Youth Friendly**, **24 / 7 Hotline & E-mail Complaints Centre** for victims of Cyberbullying incidents. These complaints are to be registered on a National Reporting System to help coordinate an effective and timely response by the Industry Service Providers. (E.g. Link ACMA into receiving a copy of ALL the Warning Notices, Site Material Removal and Site Closure Notices, The ACMA will be responsible to monitor Industry response times and compliance.)

- **Offenders**
    - The **National Reporting System** operated by ACMA will monitor and provide timely Notification to Australian Law Enforcement Agencies of Customer Activity for further investigation and possible prosecution, such as **Multiple** or **Repeat Offending Individuals**, **Hate Sites** and **Vandalism** of **Historical** and **Memorial Sites**.

- **Industry** with:-
    - Timely responses to requests for the removing of **inappropriate material.** (e.g. Blocking Individuals or Closing Sites = 24 Hours)
    - Warning Notice Procedure and Process advising offending service users with **"1st Warning – Service Violation - this service has been used to send inappropriate material – a 2nd Violation will terminate this Service**".(Mobile Phone / Internet Message).

Recommendation # 4 *(cont)*

- Business operating in Australia, with or without a Representative Office on Australian Soil are still legally bound by Australian Practices and Content Conditions in accordance to **Australian Government Laws and Practices** (e.g. NOT Subject to USA Law Protection under the 1st Amendment Bill of Rights – Free Speech Claim)

- **Police** with:-
  - A **"One Stop Shop"** for **Police Enforcement Agencies** regarding Cybersafety Issues and Cyber Crime Investigations
  - Timely response to requests for **Account Details by Australian Law Enforcement Agencies** (time to be set by AFP =? Hours)
  - The **National Reporting System** operated by ACMA will monitor and provide timely Notification to Australian Law Enforcement Agencies of **Multiple Offending Individuals** (e.g. many victim complaints) and / or **Repeat Offending Individuals** (e.g. same victim many complaints) for further investigation and prosecution.
  - The Australian Government to provide the necessary resources, support and funding to cover AFP and State Police for request of **Account Details from Service Providers**, who currently charge a substantial fee for requests for non life threatening details under Legislative condition of "Cost Recovery"

Comment

Current advice from ACMA Website includes the following information:

The Australian Communication and Media Authority (ACMA)
Cybersmart website - *www.cybersmart.go.au*

1. *You can contact the ACMA to request the removal of offensive or illegal content from a website.*
2. *Facebook administrators may also take action against the person who is cyber bullying. This might be temporarily banning them from the site, shutting down their account or even blocking them from starting up a new account.*
3. *If it is occurring via your mobile phone, you can contact your mobile phone provider to report nuisance calls and/or text messages*

Recommendation # 4 *(cont)*

Comment (cont)

One worrying type of Cyberbullying is “Cyber Attacks” on Public Figures and “Free Speech” and sets a dangerous precedent worthy of particular note here. (see Appendix10)

This type of Cyberbullying was well illustrated by Clive Hamilton from “The Drum” ABC Television show, with a series of five articles on “***Bullying, Lies and the Rise of Right-Wing Climate Denial”***

Hamilton claims:

> *“Journalists too have become the victims of cyber-bullying. I have spoken to several, of them off record, who have told of torrents of abusive emails when they report on climate change, including some sufficiently threatening for them to consult their supervisors and consider police action”.*

Extract of the first of five articles:

Recommendation # 5 *(cont)*

Appendix 10

"Bullying, Lies and the Rise of Right-Wing Climate Denial"

Clive Hamilton

http://www.clivehamilton.net.au/cms/media/documents/articles/abc_denialism_series_complete.pdf

This series of five articles appeared on the ABC The Drum website on 22-26 February 2010.

> ***Two years ago the Labor Party won a decisive election victory in part by riding a public mood demanding action on climate change after years of stonewalling.***
>
> ***The new Government promised to spearhead world efforts to reduce greenhouse gas emissions. Today it's on the run, retreating from a surge of militant anti-climate activism that believes climate science is a left-wing plot aimed at promoting elites, wrecking the economy and screwing the little man. What happened?***

Part 1: Climate cyber-bullying

Australia's most distinguished climate scientists have become the target of a new form of cyberbullying aimed at driving them out of the public debate.

In recent months, each time they enter the public debate through a newspaper article or radio interview these scientists are immediately subjected to a torrent of aggressive, abusive and, at times, threatening emails. Apart from the volume and viciousness of the emails, the campaign has two features—it is mostly anonymous and it appears to be orchestrated.

The messages are typically peppered with insults. One scientist was called a

> *LOUDMOUTH, ARROGANT, CONCEITED, IGNORANT WANKER*

The emails frequently accuse the scientists of being frauds who manipulate their research in order to receive funding, such as this one to Ben McNeil at the UNSW:

> *It's so obvious you are an activist going along with the climate change lie to protect your very lucrative employment contract …*

They often blame the recipients of being guilty of crimes, as in this one received by Professor David Karoly at the University of Melbourne.

> *It is probably not to extreme to suggest that your actions (deceitful) were so criminal to be compared with Hitler, Stalin and Pol Pot. It is called treason and genocide.*
>
> *Oh, as a scientist, you have destroyed peoples trust in my profession. You are a criminal Lest we forget.*

Recommendation # 4 *(cont)*
Appendix 10 (cont)

Receiving emails like these is unsettling and at times disturbing, which of course is the point. They become worrying when they cross the line to personal threats, such as these sent to Professor Andy Pitman at the UNSW.

> *There will be a day of facing the music for the Pitman type frauds..... Pitman you are a f**king fool!*

And this one:

> *If we see you continue, we will get extremely organised and precise against you.*

When Pitman politely replied to the last, the response was more aggressive:

> *F**k off mate, stop the personal attacks. Just do your science or you will end up collateral damage in the war, GET IT*

All threats have to be taken seriously, and at times warrant calling in the police. The police are able to trace anonymous emails to their sources and take action against those who send them. The police are now advising those who received abusive and threatening emails to resist the immediate urge to delete them and keep them in a separate folder for future reference.

Climate campaigners have also noticed a surge in the frequency and virulence of this new form of cyber-bullying. The following was received by a young woman (who asked that her name not be used).

> *Did you want to offer your children to be brutally gang-raped and then horribly tortured before being reminded of their parents socialist beliefs and actions? …*
>
> *Burn in hell. Or in the main street, when the Australian public finally lynchs you.*
>
> *Another campaigner opened her inbox to read this:*
>
> *F**k off!!!*
>
> *Or you will be chased down the street with burning stakes and hung from your f**king neck, until you are dead, dead, dead! …*
>
> *F**K YOU LITTLE PIECES OF S**T, SHOW YOURSELVES IN PUBLIC!!!*

Greens Senator Christine Milne told me that senators' inboxes are bombarded every day by climate deniers and extremists, so that now they are running at least 10 to one against those who call for action on climate change. She describes it as a "well-organised campaign of strident, offensive and insulting emails that go well beyond the bounds of the normal cut and thrust of politics".

Recommendation # 4 *(cont)*
Appendix 10 (cont)

It was widely reported that in the days before the Liberal Party leadership challenge last November, MPs were blitzed with emails from climate deniers.1 Some MPs were spooked into voting for Tony Abbott,2 the only one of the three contenders who had repudiated climate science. Australia's alternative government is now led by climate deniers.

Journalists hit

Journalists too have become the victims of cyber-bullying. I have spoken to several, off them Off record, who have told of torrents of abusive emails when they report on climate change, including some sufficiently threatening for them to consult their supervisors and consider police action.

One was particularly disturbed at references to his wife. Another received the following from someone who gave his name and identified himself as medical representative at major pharmaceuticals company:

> *you sad sack of s**t. It's ok to trash climate change skeptics yet, when the shoe is on the other foot, you become a vindictive, nasty piece of s**t not able to face the fact that you're wrong about climate change and you're reputation is now trash*

Anonymous emails are usually more graphic.

> *YOUR MOTHER WAS A GOAT F**KER!!!!!!YOUR FATHER WAS A TURD!!!!!!!YOU WILL BE ONE OF THE FIRST TAKEN OUT IN THE REVOLUTION!!!!!!!!YOUR HEAD WILL BE ON A STAKE!!C**T!*

Few of those on the receiving end of this hatred doubt that the emails are being orchestrated. Scores of abusive emails over a few hours are unlikely to be the product of a large number of individuals spontaneously making the effort to track down an email address and pour forth their rage.

While some individuals act alone, increasingly the attacks are arranged by one or more denialist organisations. It's fair to assume operatives in these organisations constantly monitor the media and, when a story or interview they don't like appears, send messages out to lists of supporters, linking to the comments, providing the scientist's email address and urging them to let him or her know what they think.

One or two of the cyber-bullies have hinted at the level of organisation, with one following an abusive rant with the comment: "Copies of my e-mails to you are also being passed out to a huge network for future reference."

---

1 http://www.thepunch.com.au/articles/the-holy-war-on-climate-change/
2 http://www.smh.com.au/national/candle-burnt-out-long-before-20091127-

Recommendation # 4 *(cont)*
Appendix 10 (cont)

Net rage and free speech

The purpose of this new form of cyber-bullying seems clear; it is to upset and intimidate the targets, making them reluctant to participate further in the climate change debate or to change what they say. While the internet is often held up as the instrument of free speech, it is often used for the opposite purpose, to drive people out of the public debate.3

Unlike the letters pages of newspapers, on the internet anonymity is accepted and the gatekeepers, where they exist, are more lax, so the normal constraints on social discourse do not apply. On the internet, the demons of the human psyche find a play-ground.

If a group attempts to have a considered discussion about climate science on an open forum it is very soon deluged with enraged attacks on climate science, sometimes linking for authority to well-known denialist websites. Most scientists long ago stopped attempting to correct the mishmash of absurd misrepresentations and lies in web "discussions".

Is the new campaign of cyber-bullying working? Receiving a large number of offensive emails certainly wears most people down. Some scientists and journalists probably do change what they say or withdraw from debate. Others have strategies for dealing with the abuse—never replying, deleting without reading or swapping loony emails with colleagues, and cultivating a thick skin.

The effect of the cyber-bullying campaign on some scientists—including those I have mentioned—is quite opposite to the intended one. The attempts at intimidation have only made them more resolved to keep talking to the public about their research. Their courage under fire stands in contrast to the cowardice of the anonymous e-mailers.

Tomorrow: Who is behind the cyber-bullying campaign?

Recommendation # 5

Establish a National "Schools Best Practice" Model

Details of:
Recommendations for Joint Parliamentary Committee on Cybersafety (cont)

Recommendation # 5

Establish a National "Schools Best Practice" Model

The National Child and Young Persons Human Rights Council working with appropriate Expert Working Groups will help develop, publish and promote a **National "Schools Best Practice" Model** to be included in the **National Safe Schools Framework** *(see Appendix 03)* to standardize a minimum protection level that is contained in ALL School Policies and Procedures.

1.1 A **National School Best Practice Model** will help to guarantee an Australian wide Protection Standard for ALL children and young people no matter which State or what type of School.

1.2 Provide the necessary resources to support schools to minimise bullying and cyberbullying practices by adding to the **National "Schools Best Practice" Model** with **"Local Best Practice" Policies** and **Procedures** and ensure School ownership.

Comment

Unfortunately, the debate and focus on Bullying and Cyberbullying has targeted the school as the main identity responsible for dealing with "Inappropriate Behaviour"; followed by the Parents and / or Caregivers; then by the Community Agencies such as Psychologists and Researchers with a plethora of new Approaches, some being researched based and validated, others providing a short term "interest" with no real practical or long term application.

That is, we often get the "Great Motivational Talk" but without the "Practical Tools" to follow!

Even the "National Safe Schools Framework" is just that a "Framework Discussion" providing over 18 Pages of References to Documents and/or Web sites with the implied message "**to consult and comply with**"; without any Practical Tools for a "Best Practice" Model, Proforma or Example.

Unfortunately, this format reinforces a growing frustration with yet another example of the old practice of Real - "**Management and Support**", being replaced with a new practice of "Make Believe" – "**Supervision and Referral**".

"Yes we can all be sued for taking responsibility and making a choice BUT we can also be sued for NOT taking responsibility and NOT making a choice either!"

Recommendation # 5 *(cont)*

Surely, with over **3,000 Schools in Australia** one could consider setting up a Working Group to provide a basic "Best Practice Model" as a worthwhile "Base Line Model" to help **each School**, and their **over worked staff**, to then **add specific local information** to produce a **Local "Best Practice Model".**

This "Best Practice Model would also ensure that the **minimum standards of child protection** methods and procedures would be **guaranteed** and available to **ALL children and families** no matter which **State** or which type of **School** they attend.

A **National "Schools Best Practice" Model**, should include a number of Proforma Documents to ensure the essential elements of policy and procedure are standardized.

A **National "Schools Best Practice" Model**, should also include a number of Proforma Documents to assist the Schools compile a standardized Framework to assist the promotion of an Anti – Bullying and Cyber Safe School environment.

Some excellent examples of the type of standardized and useful **School Proforma Documents** that should be included in the **National "Schools Best Practice" Model**, are provided by Sameer Hinduja, Ph.D. and Justin W. Patchin, Ph.D. - Cyberbullying Research Center, USA, as follows:

Sameer Hinduja, Ph.D. and Justin W. Patchin, Ph.D. - Cyberbullying Research Center

Proforma School Documents:

1. **Appendix 12 - Cyberbullying Report Card**
2. **Appendix 13 - Cyberbullying Incident Tracking Report Form – Pages 1- 3**
3. **Appendix 14 - Internet Use Contract**
4. **Appendix 15 - Family Cell Phone Contract**

Recommendation # 5 *(cont)*

Appendix 12 - Cyberbullying Report Card

Sameer Hinduja, Ph.D. and Justin W. Patchin, Ph.D. - Cyberbullying Research Center

Is your school adequately addressing or prepared for cyberbullying concerns? Fill out this Report Card to find out. If you answer yes to all of these statements, you are prepared. If you answer no or don't know the answer, you have work to do!

1. ***General Assessment -*** *? no yes*
   - 1.1. We know how many students at our school have been victims of cyberbullying.
   - 1.2. We know how many students at our school have cyberbullied others.
   - 1.3. Cyberbullying is a not a significant problem in our school.

2. ***School Climate/Culture -*** *? no yes*
   - 2.1. Students who witness cyberbullying are empowered to step up and inform a trusted adult rather than remain silent bystanders.
   - 2.2. Teachers regularly remind students to approach them for help if they are dealing with an issue related to cyberbullying or online safety.
   - 2.3. It is clear to students that the inappropriate use of technology will not be tolerated by school administration.
   - 2.4. We work to create a school climate in which cyberbullying is not considered "cool" among the student population.

3. ***Curriculum and Education -*** *? no yes*
   - 3.1. Students are taught about acceptable computer and Internet use during the school year through presentations and assemblies.
   - 3.2. Students are taught about safe password practices and the protection of personal information.
   - 3.3. Students are taught about how to recognize cyberbullying and threats to their online safety.
   - 3.4. Students are taught about how to respond to cyberbullying in an appropriate manner.
   - 3.5. Teachers know how to recognize cyberbullying issues and how to intervene in an appropriate manner.
   - 3.6. We distribute materials to students and parents to educate them about cyberbullying.
   - 3.7. We hold afterschool meetings and events during the school year for parents and community members about online safety among youth.
   - 3.8. We use older students to educate younger students about identification and prevention of cyberbullying and how to respond to it.
   - 3.9. We are (and stay) familiar with the relevant major court decisions related to student speech using computers and the Internet.
   - 3.10. We are familiar with the ways in which the school district might be civilly liable for negligently preventing or improperly responding to cyberbullying incidents, and we work to avoid them.

Recommendation # 5 *(cont):*

Appendix 12 - Cyberbullying Report Card (cont)

4. ***Cyberbullying Response -*** *? no yes*

   4.1. We take suspected and actual incidents of cyberbullying seriously at our school.
   4.2. We have developed and made known a continuum of disciplinary consequences for cyberbullying incidents.
   4.3. We know when we can intervene in cyberbullying incidents that originated off-campus.
   4.4. We have developed a formal procedure for investigating incidents of cyberbullying.
   4.5. We have an anonymous reporting system to allow students and teachers to report instances of cyberbullying without fear of reprisal.
   4.6. We have a formal relationship with a local law enforcement department capable of conducting computer and network forensic examinations should the need arise.

5. ***Policies -*** *? no yes*
   5.1. Our school has a clear cyberbullying policy.
   5.2. Our cyberbullying policy includes language about off-campus behaviors being subject to discipline.
   5.3. Our school has a clear policy regarding cell phones and other portable electronic devices.
   5.4. Students know our policy regarding technology.
   5.5. Parents know our policy regarding technology.
   5.6. Signage about acceptable computer and Internet use is posted in school computer labs.

6. ***Technology -*** *? no yes*
   6.1. We have Web site-blocking and content-monitoring software/hardware installed on our network to ensure age appropriate
   6.2. Web browsing and communications.
   6.3. We avoid putting student information on the district Web site.

7. ***Other Areas -*** *? no yes*

   7.1. (Note: Physical Bullying – should be included in school policies and procedures - Added by Author of this Submission – Stewart Healley)

Rec 5: Appendix 13 - Cyberbullying Incident Tracking Report Form – Page 1/3

Sameer Hinduja, Ph.D. and Justin W. Patchin, Ph.D. - Cyberbullying Research Center

Report taken by: …… Date of report: ……

Complainant Information

Name: …….. Student Staff (circle one)

Age: ……. Sex:……. School: …….. Grade: …….

Target Information

Name: …….. Student Staff (circle one)

Age: ……. Sex:……. School: …….. Grade: …….

Offender 1 Information

Name: …….. Student Staff (circle one)

Age: ……. Sex:……. School: …….. Grade: …….

Offender 2 Information

Name: …….. Student Staff (circle one)

Age: ……. Sex:……. School: …….. Grade: …….

Offender 3 Information

Name: …….. Student Staff (circle one)

Age: ……. Sex:……. School: …….. Grade: …….

Other Party Information (witness, bystander)

Name: …….. Student Staff (circle one)

Age: ……. Sex:……. School: …….. Grade: …….

Rec 5: Appendix 13 - Cyberbullying Incident Tracking Report Form – Page 2/3

Sameer Hinduja, Ph.D. and Justin W. Patchin, Ph.D. - Cyberbullying Research Center

Location of Incident: ……..

Description of Incident (use additional sheets if necessary)**:**

Did the incident involve any of the following features?

Threat to someone's physical safety	Yes / No
Sexual harassment	Yes / No
Discrimination based on race, class, gender, sexual orientation, or other protected status	Yes / No
Repeated cyberbullying after previous intervention	Yes / No
Image or video- or audio-recording of harassment	Yes / No
Other notable feature (please list)	Yes / No

Did the incident result in a substantial disruption of the school environment or infringe on the rights of other students or staff? Yes/ No

(if yes, please describe in as much detail as possible)

Attach printouts of all evidence and additional sheets with statements by individuals listed on page 1.

Rec 5: Appendix 13 - Cyberbullying Incident Tracking Report Form – Page 3/3

Sameer Hinduja, Ph.D. and Justin W. Patchin, Ph.D. - Cyberbullying Research Center

Description of Action Plan:

What sanctions are being applied and what steps are being taken to ensure behavior does not continue?

What additional consequences will be applied if offender fails to comply with action plan?

Comments by principal or other administrator:

Other comments:

I have been made aware of this incident and will discuss this issue further with my child.

Parent's signature: …… Date: ……

Case closed date: …… Reason for closure: ……..

Rec 5: Appendix 14 - Internet Use Contract

Sameer Hinduja, Ph.D. and Justin W. Patchin, Ph.D. - Cyberbullying Research Center

Child Expectations	**Parent Expectations**
I understand that using the family computer is a privilege that is subject to the following rules: 1. I will respect the privacy of others who use this computer. I will not open, move, or delete files that are not in my personal directory. 2. I understand that mom and dad may access and look at my files at any time. 3. I will not download anything or install programs without first asking mom or dad. 4. I will never give out private information while online. At no time will I ever give out my last name, phone number, address, or school name—even if I know the person with whom I am communicating. My screen name will be: …… 5. I understand that I can use the computer for approved purposes only. 6. I will never write or post anything online that I would not want mom or dad to see. I will not use profanity or otherwise offensive language. If I receive messages or view content with offensive language, I will report it to mom and dad immediately. 7. I will never agree to meet an online friend in person without first asking mom or dad. Dangerous people may try to trick me into meeting up with them. 8. If I ever feel uncomfortable about an experience online, I will immediately tell mom or dad. I understand that mom and dad are willing to help me and will not punish me as long as these rules are followed.	I understand that it is my responsibility to protect my family and to help them receive the best of what the Internet has to offer. In that spirit, I agree to the following: 1. I will listen calmly. If my child comes to me with a problem related to online experiences, I promise not to get angry but to do my best to help my child resolve the situation. 2. I will be reasonable. I will set reasonable rules and expectations for Internet usage. I will establish reasonable consequences for lapses in judgment on the part of my child. 3. I will treat my child with dignity. I will respect the friendships that my child may make online as I would offline friends. 4. I will not unnecessarily invade my child's privacy. I promise not to go further than necessary to ensure my child's safety. I will not read diaries or journals, nor will I inspect e-mails or computer files unless there is a serious concern. 5. I will not take drastic measures. No matter what happens, I understand that the Internet is an important tool that is essential to my child's success in school or business, and I promise not to ban it entirely. 6. I will be involved. I will spend time with my child and be a positive part of my child's online activities and relationships—just as I am offline. List of Prohibited Web sites and software applications: …… …… …… ……

Child's Signature: …… Parent's Signature: ……

Rec 5: Appendix 15 - Family Cell Phone Contract

Sameer Hinduja, Ph.D. and Justin W. Patchin, Ph.D. - Cyberbullying Research Center

Child Expectations	**Parent Expectations**
1. I acknowledge that using a cell phone is a privilege and, therefore, will not take it for granted. 2. I will not give out my cell phone number to anyone unless I first clear it with my parents. 3. I will always answer calls from my parents. If I miss a call from them, I will call them back immediately. 4. I will not bring my cell phone to school if it is prohibited. If allowed to bring it to school, I will keep it in my backpack or locker and turned off between the first and last bell. 5. I will not use my cell phone for any purpose after _____am / pm on a school night or after _____am / pm on a nonschool night, unless approved by my parents. 6. I will not send hurtful, harassing, or threatening text messages. 7. I will not say anything to anyone using the cell phone that I wouldn't say to them in person with my parents listening. 8. I will pay for any charges above and beyond the usual monthly fee. 9. I will not download anything from the Internet or call toll numbers without first asking my parents. 10. I will not enable or disable any setting on my phone without my parent's permission. 11. I will not take a picture or video of anyone without that person's permission. 12. I will not send or post pictures or videos of anyone online without that person's permission. 13. I will not send or post any pictures or videos to anyone without first showing them to my parents. 14. I will not be disruptive in my cell phone use. If my parents ask me to end a call or stop text messaging, I will.	1. I will respect the privacy of my child when my child is talking on a cell phone. 2. I will not unnecessarily invade my child's privacy by reading text messages or looking through call logs without telling my child first. If I have a concern, I will express it to my child, and we will look through this material together. 3. I will pay the standard monthly fee for the cell phone contract. 4. I will be reasonable with consequences for violations of this contract. Consequences will start at loss of cell phone privileges for 24 hours and progress according to the seriousness of the violation.

Child's Signature: …… Parent's Signature: ……

Recommendation # 6

Establish appropriate National "Base Line" Legal Framework Laws starting with the existing Commonwealth Criminal Code ACT 1995

Details of:
Recommendations for Joint Parliamentary Committee on Cybersafety (cont)

Recommendation # 6

Establish appropriate National "Base Line" Legal Framework Laws starting with the existing Commonwealth Criminal Code ACT 1995.

The National Child and Young Persons Human Rights Council working with appropriate Expert Working Groups will help develop, publish and promote a **National "Base Line" Legal Framework Laws**, starting with the existing **Criminal Code 1995.**

5.1 A **National "Base Line" Legal Framework Law** will help to guarantee an Australian wide Protection Standard for ALL children and young people no matter which State or what type of School.

5.2 Providing Police & Community protection and support for victims and offenders with a Community Trial of the Practical "Respect It or Lose It" - Cyber Safety Model, promoting a **Police Charge / Caution** with a **Restorative Justice Program Pathway**

Comment

Reference to some appropriate material will high light some important areas for consideration in the recommendation to establishing a National "Base Line" Legal Framework Laws starting with the existing **Commonwealth Criminal Code ACT 1995.** *(see Appendix 04)*

Reference material includes the following:

Reference 02

New Laws to Counter Bullying
Writer Helen Splarn. Editor Dr Rimes Manocha.
Source: National Centre Against Bullying.

Reference 03

Victoria Police serve intervention on Facebook
By Liz Tay on Oct 20, 2010 10:50 AM Filed under Oddware

Reference 04

Magistrate slams cyber bullies- *April 8, 2010*
The Sydney Morning Herald - APP
snh.com.au

Recommendation # 6 *(cont)*

Reference 05

Shooting suspect made harrowing warning
Nine News web site 14:30 AEST Sat Mar 26 2011

Appendix 15

Cyber Bullying In Schools and the Law
Is There an Effective Means of Addressing the Power Imbalance?
By Liz Tay on Oct 20, 2010 10:50 AM Filed under Oddware

Appendix 16

Future directions in technology-enabled crime: 2007-09
Kim-Kwang Raymond Choo, Russell G Smith, Rob McCusker
Australian Institute of Criminology - Research and Public Policy Series No. 78

Appendix 10

"Respect It or Lose It – Cybersafety Community Model
Stewart Healley - 2010

Note*: Pertinent Reference material includes*:

Cyber Bullying In Schools and the Law
Is There an Effective Means of Addressing the Power Imbalance?
Des Butler, Sally Kift & Marilyn Campbell - 2009

(c) Misuse of Telecommunications Services (Appendix 16 - page 94)

The Commonwealth Criminal Code Act 1995 contains a number of offences which may be ***effective means of redress against a cyber bully*** *who misuses telecommunication services to menace, threaten or hoax other persons. Section 474.17 makes it an offence to use telecommunication services to menace, harass or cause offence (punishable by 3 years). It does not matter whether the menace or threat is caused by the type of use (such as multiple postings on a website) or by the content of the communication or both, provided reasonable persons would regard the use as being menacing, harassing or offensive in all the circumstances.*

Recommendation # 6 *(cont)*

Media Reports - Extracts:

Reference 02

New Laws to Counter Bullying

Writer Helen Splarn. Editor Dr Ramesh Manocha.
Source: National Centre Against Bullying.

June 11th, 2010 | Cybersafety, cyberbullying, internet safety, technology, violence

- Victorian Government to introduce new anti-bullying laws
- 600 intervention court orders this year against children
- New laws to focus on mediation
- 10% of Australian teenagers are victims of cyber-bullying

The changes come at a time when more children are taking out intervention orders against other children in an attempt to deal with the growing number of cases of school bullying, especially cyber-bullying.

Former cyber-safety project officer with the Victoria Police and Generation Next speaker, **Susan McLean** said the increase in cyber-bullying at schools meant that the student's concerns needed to be resolved immediately in order to avoid long term trauma for the victims.

If these new laws are to be effective they must be supported by extensive training in cyber-bullying for all mediators, school councillors and teachers.

"They can't wait six weeks for mediation – that would defeat the purpose," Ms McLean said. "As an adult, if someone sends you something nasty you delete it. Children read and re-read."

There are also concerns that teachers are not equipped to deal with both the increased cases of bullying and the nature it is now taking, which includes cyber-bullying, stalking and acts of violence including the use of weapons.

Research carried out by online bullying expert Dr Spears, a senior lecturer at the University of South Australia surveyed 700 student teachers "we know pretty well all universities are giving pre-service teachers behaviour management courses, but we need to focus on the specifics of how you help somebody. If a child comes to me then what do we do?" Dr Spears said.

"If we're looking for a whole school community response (to cyber-bullying) then we can't ignore the people training to be teachers."

"There's an understanding that these young people are digital natives, online and offline their worlds are one and the same," she said.

Recommendation # 6 *(cont)*

Media Reports - Extracts☹cont)

Reference 02 (cont)

> "The fact is nothing is private online," Dr Spears said. "If the information is there it can be accessed. Young people need to realise once it is there it is there forever."
>
> For this reason, it was important for Internet users to adopt the rule of thumb: **What goes online stays online**, she said.
>
> The National Centre Against Bullying is also calling for all student teachers to receive compulsory and comprehensive training in both bullying prevention and bullying management during their training.
>
> http://www.generationnext.com.au/blog/?p=1451

Recommendation # 6 *(cont)*

Media Reports - Extracts☹cont)

Reference 03

Victoria Police serve intervention on Facebook

By Liz Tay on Oct 20, 2010 10:50 AM Filed under Oddware

Court order served to online bully.

Victoria Police has served a cyberbullying intervention order via Facebook, after unsuccessful attempts to reach the accused by phone and in person.

The man was a "prolific Facebook user" who had allegedly threatened, bullied and harassed a former partner online.

Police were approached by the victim in August, but were unable to locate the accused by traditional means.

In what police believe to be an Australian first, the accused was served with an interim intervention order, extract, explanation, contacts and a video of Leading Senior Constable Stuart Walton via a Facebook private message.

The accused was ordered not to publish any material about the victim online, and not to contact the victim "by any means", including phone and e-mail, except through the police or a lawyer.

"If you do not obey this order, you may be arrested and charged with a criminal offense," Walton said in the video.
The accused did not attend Court as ordered, and police were unable to confirm that the message had been read. However, a Victorian Court Magistrate upheld the order indefinitely and a final order was served via Facebook.

Police finally succeeded in contacting the accused after the final order was served, and ascertained that he had read both interim and final documents via Facebook and agreed to

"Internet bullying, stalking and intimidation are taken very seriously by Police. In this instance we were able to deliver justice through the same medium as the crime committed," Walton stated.

"Police will always pursue traditional means to enforce the law and to protect the community - but we won't shy away from innovative methods to achieve positive outcomes, either."
Facebook claims to take users' privacy "very seriously", and works with law enforcement "to the extent required by law".

In May, the Australian Federal Police called for Facebook to establish a local law enforcement contact who would be immediately accessible to Federal, state and territory agencies.

Recommendation # 6 *(cont)*

Media Reports - Extracts☹cont)

Reference 04

Magistrate slams cyber bullies- *April 8, 2010*

The Sydney Morning Herald - APP
snh.com.au

http://news.smh.com.au/breaking-news-national/magistrate-slams-cyber-bullies-20100408-ru23.html

A Melbourne magistrate has pleaded with young people to think before sending hateful text messages, as he sentenced a cyber bully whose victim committed suicide.

Allem Halkic was 17 when he jumped to his death from Melbourne's West Gate Bridge on February 5, 2009.

His former friend, Shane Gerada, 21, of Bacchus Marsh, had sent him five threatening text messages in the hours leading up to his death.

In one of the first cyber bullying cases to come before a Victorian court, Gerada was convicted of one count of stalking but avoided a jail term. He was sentenced to an 18-month community-based order, which involves 200 hours unpaid community work.

Allem's parents Ali and Gina Halkic want new laws to make it easier to prosecute cyber bullies.

"His community-based service ... if you can weigh that up against Allem's life, I mean, it breaks our heart," a tearful Mr Halkic told reporters.

Police prosecutor Glenn Collins said some studies had found that up to 30 per cent of children were victims of cyber bullying.

"Cyber bullying has reached almost plague proportions," he told the Melbourne Magistrates' Court.

"It's a cowardly form of bullying.

"It essentially brings bullying into the home."

Magistrate Peter Reardon said he accepted Gerada did not intend for Allem to take his own life.

"(But) a message needs to be sent to the community that this sort of act should be punished," Mr Reardon said.

He urged young people to think about the consequences of sending threatening messages on mobile phones or via social networking sites.

Recommendation # 6 *(cont)*

Media Reports – Extracts (cont)

Reference 04 (cont)

"People really should think about what they are doing instead of just hammering some message of hate or aggression," he said.

"Because you don't know necessarily what the reaction will be."

Gerada's lawyer Sam Norton described his client's behaviour as "schoolyardish" and a result of stupidity rather than malice.

Gerada sent Allem threatening messages after a falling out.

"Hahaha, dude ... ill put u in hospital," one of the messages read.

"Dont be surprised if u get hit sum time soon. You f***** with the wrong person Allem," another threatened.

Four hours before Allem suicided, he telephoned Gerada. He also sent him a message pleading for help.

"Shane man just listen to me I need your help ... you might not give a f*** about me or whatever but just be a man and help me out."

Gerada told the media he sent the messages out of revenge. He later told police he did it to appear tough.

He wrote a letter expressing remorse, which was tendered to the court.

"I wish I had never said what I did to Allem. He was one of my best friends and I now have to live with the loss of him everyday," Gerada said.

Mr Halkic said he had sold the family home to fund civil action against the state government and VicRoads for not acting quickly enough to erect barriers on the 53-metre-high West Gate Bridge.

*For emotional crisis telephone support contact Lifeline 24 hours a day, seven days a week, on 13 11 14 or visit their website for information and self help resources at www.lifeline.org.au.

Recommendation # 6 *(cont)*

Media Reports – Extracts (cont)

Reference 05

Shooting suspect made harrowing warning

Nine News web site 14:30 AEST Sat Mar 26 2011

A US teenager wrote "today is the day" on his Facebook Page before allegedly shooting a fellow high school student in Indiana.

The 16-year-old allegedly shot Chance Jackson, 15, twice in the stomach at 7am, 20 minutes before class was due to begin at Martinsville West Middle School on Friday (US time), ABC
News reports.

The alleged shooter, from Martinsville, southwest of Indianapolis, only enrolled at the school on Monday and had been either suspended or expelled that week, Indiana State Police sergeant Curt Durnil said.

The victim was flown to hospital and his family said he was in a stable condition after surgery.
"We appreciate all of the thoughts, prayers and support and ask that you also pray for the families of all involved," they said in a statement.

Police found the alleged shooter two blocks from the school in a wooded area near a neighbouring school and took him into custody at 8am.

They found a handgun in a field near the school.

Sergeant Durnil said social media would be a key part of the investigation.

The suspect wrote "today is the day" and "you will hear about it" on his Facebook page on Friday.

The assistant superintendant for the Martinsville School District, Randy Taylor, said the suspect was a former student.

"This student was no longer a student and should not have been on school property," he added.
There are reports the incident may have been sparked by a fight at a school dance last weekend.

http://news.ninemsn.com.au/world/8229022/shooting-suspect-posts-facebook-message-before-attack

Recommendation # 6 *(cont)*

Appendix 15 - Extract

Cyber Bullying In Schools and the Law

Is There an Effective Means of Addressing the Power Imbalance?

Des Butler, Sally Kift & Marilyn Campbell - Cyber Bullying In Schools and the Law

eLaw Journal: Murdoch University Electronic Journal of Law (2009) 16(1) 84

Cyber bullying – or bullying through the use of technology – is a growing phenomenon which is currently most commonly experienced by young people and the consequences manifested in schools. Cyber bullying shares many of the same attributes as face-to-face bullying such as a power imbalance and a sense of helplessness on the part of the target. Not surprisingly, targets of face-to-face bullying are increasingly turning to the law, and it is likely that targets of cyber bullying may also do so in an appropriate case. This article examines the various criminal, civil and vilification laws that may apply to cases of cyber bullying and assesses the likely effectiveness of these laws as a means of redressing that power imbalance between perpetrator and target.

1. Introduction

The ubiquity of modern telecommunications in the modern world has brought with it great benefits to society. However, it also has its darker side. This has included the phenomenon of „cyber bullying" – a term coined by Canadian Bill Belsey to describe „the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group, that is intended to harm others".[1] Cyber bullying is being experienced across different walks of life, although it is perhaps currently most prevalent amongst school students. Indeed, for so-called „Net-Gen" – those who have been born since 1982 – electronic socialising and interactive communications are an integral part of their daily lives.[2] Indeed, one 2005 Canadian study found that 94% of children accessed the Internet from home, with some aged as young as Grade 4 being reliant on the Internet to network with their friends. So is perhaps not surprising that what little research that has been done on cyber bullying to date has been focused primarily on these „digital natives".[3] However, as technology continues to permeate all society and as the digital natives pass from adolescence to adulthood, there is reason to expect that cyber bullying may become more common in older age groups.

* Des Butler LLB (Hons), PhD (QUT) is Professor of Law, Faculty of Law, Queensland University of Technology.
** Sally Kift LLB(Hons) (Qld), LLM (QUT) is Professor of Law, Faculty of Law, Queensland University of Technology.
*** Marilyn Campbell BA (Syd), DipEd (UNE), BEd (QUT), MEdSt, GradDipPsych, PhD (Qld) is Associate Professor, Faculty of Education, Queensland University of Technology.

Recommendation # 6 *(cont)*

Appendix 15 – Extract (cont)

The potential is clear for technologies such as on-line social network sites like MySpace and Facebook, discussion boards, on-line forums, blogs, wikis and e-mail as well as the now ubiquitous mobile phone to be used as a means of mala fides against other users. The potential for the misuse of the Internet by deviant adult predators has been widely publicised and well understood. However, there is only growing realisation that hostile behaviour utilising technology can also have serious and long lasting effects on its targets. Victims of bullying of any kind typically feel powerless to repel or fight back against their aggressors. Cyber bullying adds a new dimension to this powerlessness with its ability to reach the target 24 hours a day, 7 days a week. Now a target cannot even rely on his or her home as a safe haven from bullying behaviour.

Increasingly victims of bullying are turning to law, both civil and criminal, as a means of addressing the power imbalance between them and their bullies, or at least of obtaining some form of vindication. While this might seem an extreme response to conduct that might be considered by some to be trivial or „just a joke ", the potential harm that victims may suffer makes the effectiveness of the various laws that may be called into play worthy of scrutiny.

2. Cyber Bullying and its Effects

2.1 Concepts of Cyber Bullying

Cyber bullying may be defined by examples of how technology is used in bullying. An associated question is whether concepts applicable to traditional face-to-face bullying apply equally to cyber bullying, or whether the use of technology to bully requires fresh thinking. This question is not helped by the fact that sociological researchers do not even agree on the definition of face-to-face bullying. Nevertheless, most researchers agree that bullying per se is a form of aggression which has at least four underlying features. On examination, these concepts at least would seem to be capable of extending to cyber bullying.

First, the perpetrator intends to hurt the target, whether emotionally or physically. Bullying cannot be accidental. An intention to hurt would seem to be the present also in cyber bullying. Secondly, traditional concepts of bullying include the notion of an imbalance of power. Usually in face-to-face bullying, the bully has a power differential because of size, age or position. By contrast, in the case of cyber bullying the bully often chooses to remain anonymous. This might be thought to negate any sense of power imbalance, since the target cannot perceive that he or she is less powerful if he or she does not know the identity and attributes of the other person. However, it can be argued that the very act of bullying, creates an imbalance of power. Moreover, the bully's anonymity in itself places the target at a disadvantage and invests the bully with a measure of power over the target.

Recommendation # 6 *(cont)*

Appendix 15 – Extract (cont)

The third underlying concept of face-to-face bullying is the repetition or continued threat of further aggression. Both perpetrator and target believe the aggression will be sustained, thereby causing the target continuing agitation or fear. This notion would seem to be readily transferable to cyber bullying. Technology provides easy means to rain a seemingly ceaseless barrage of hostility upon the target. Finally, targets of face-to-face bullying are typically unable to defend themselves, or unable to fight back as they feel helplessness, hurt and shame. Due to the global reach of technology and supported by the usual anonymity of the aggressor, targets of cyber bullying are no less powerless to respond to intimidation than, for example, a physically weaker target is at a disadvantage and powerless to respond to the physical blows of a face-to-face bully.

2.2 Incidence of Cyber Bullying

There is as yet scant published research on the incidence of cyber bullying. Much of the research that has been done concerns the cyber bullying of adolescents. This is perhaps understandable since this is the first generation born which only knows of a world linked by digital technology. One Canadian study in 2006 found that 24.9% of adolescents reported they have been cyber bullied.[4] This compares to a 2005 study in Australia that placed the incidence at only 14%[5] and a 2004 North American study[6] that found only 7% reported to have been victimised. Other research shows an apparent increase from 25% of young people reporting being targets of cyber bullying in 2002[7] to a figure of 35% in 2005.[8] A factor hampering any meaningful comparison between these studies is the tendency of researchers to use varying definitions of cyber bullying which often include all forms of aggression and which do not conform to commonly understood concepts of bullying. Perhaps the best that can be said is that the current incidence of cyber bullying seems to be about 10% of adolescents.[9]

An open question is whether boys or girls are cyber bullied more, although one study found no differences.[10] It also is not known whether someone who cyber bullies also engages in face-to-face bullying. The same study found that 64% of cyber bullies admitted to also bullying face-to-face.

2.3 Consequences of Cyber Bullying

Little is yet known for sure about the consequences of cyber bullying. There have been several media reports that have linked suicides with the decedents being identified as targets of cyber bullying.[11] However, research into the effect of face-to-face bullying on adolescents has shown that it can lead to increased levels of depression, anxiety and psychosomatic symptoms in victims.[12] Research has also shown victims may suffer even more serious consequences including severe physical harm, self-harm attempts[13] as well as the reported suicides.[14] Students who are the targets of bullying may have greater interpersonal difficulties and feel socially ineffective,[15] and have higher levels of absenteeism from school and lower academic competence, with ramifications for future careers.[16]

Recommendation # 6 *(cont)*

Appendix 15 – Extract (cont)

While there is little research on the consequences of cyber bullying specifically, it may be that it could have even more serious consequences than face-to-face bullying due to the variety of attributes that may accentuate the impact of the behaviour. Depending on the particular circumstances, this may include a wider audience, anonymity of the bully, the more enduring nature of the written word and the ability to reach the target at any time and in any place, including the target's home. Further, cyber bullies may feel emboldened because they cannot see their targets or their immediate responses, and believe that, because of their anonymity, they will not be detected. It has been suggested that this anonymity may increase the intensity of the attacks and encourage them to continue for longer than they would otherwise do face-to-face.[17] While it is true that cyber bullying can only threaten physical violence rather than inflict it, research has shown that verbal and psychological bullying may have more negative long term effects.[18]

3. The Law's Response

In many respects the law has struggled to keep apace with advances in technology. The problem of cyber bullying is no different. While there is yet to be a case of cyber bullying reach an Australian court, such an eventuality is readily conceivable. It is not difficult to reconceptualise cyber bullying in terms of criminal, tortious or vilifying behaviour.

3.1 Cyber Bullying as a Criminal Offence

It may seem to some that a criminal prosecution would be an extreme response to bullying behaviour. In the first place, the Director of Public Prosecutions may be dubious in a given instance that a case can be established beyond reasonable doubt, particularly with respect to the necessary intention to commit the relevant crime. Nevertheless, even where there is such reticence on the part of the prosecuting authority, targets of cyber bullying may find that the very involvement of a police investigation helps them to regain a sense of control and power otherwise lost to the bully. Examination of the range of criminal offences that may be relevant is therefore warranted.

3.1.1 Criminal Responsibility

A threshold question when considering the criminality of behaviour is whether the offender is deemed by law to be responsible for his or her actions. In the case of young perpetrators it might be thought that they lack the same ability to appreciate the consequences of their behaviour, empathy for others and ability to control their impulses that might be reasonably expected of adults. Irrespective of such considerations, criminal responsibility is determined solely on the basis of age.

Recommendation # 6 *(cont)*

Appendix 15 – Extract (cont)

At common law, the age of criminal responsibility is 7 years. This age has been raised by statute in all Australian jurisdictions to 10 years, meaning a cyber bully under 10 will never be criminally liable, while those aged between 10 and 14 years may be criminally responsible if the prosecution can prove beyond reasonable doubt that the child knew he or she ought not to have committed the offence. In other words, it must be shown that the child knew that it was a wrong act of some seriousness, as distinct from an act of mere „naughtiness or childish mischief".[19] By contrast, anyone aged 14 and over is deemed to have the requisite capacity and is thus criminally liable for his or her conduct.

3.1.2 Offences

New South Wales is the only Australian jurisdiction to enact legislation specifically directed at bullying in schools (which would in its terms include cyber bullying),[20] unlike, for example, the United States where sixteen states including New York, California and Illinois have statutory responses.[21] Nevertheless, cyber bullying may
easily be conceived in terms of well know criminal offences such as assault, threats, extortion, stalking, harassment, and indecent conduct. In addition, an increasing array of new offences, such as torture, voyeurism, cyber stalking, and telecommunications offences may be relevant. The New South Wales provisions and some of these other offences as they apply to cyber bullying are worth closer examination.

(a) Assaults, Intimidation and Harassment at School (New South Wales)

The Crimes Act 1900 (NSW) was amended by the Crimes Amendment (School Protection) Act 2002 (NSW) (commenced February 2003) to make it an offence in s 60E where a person „assaults, stalks, harasses or intimidates" any school staff or student while attending the school. None of the terms „assault", „stalk", „harass" or „intimidate" are specifically defined, but on their natural meaning would include cyber bullying.
This section is unique in the Australian criminal law, but is limited in its reach to staff and students while „attending the school", which is defined in s 60D(2) as follows:

> *(a) while the student or member of staff is on school premises for the purposes of school work or duty (even if not engaged in school work or duty at the time), or*
>
> *(b) while the student or member of staff is on school premises for the purposes of before school or after school child care, or*
>
> *(c) while entering or leaving school premises in connection with school work or duty or before school or after school care.*

Recommendation # 6 *(cont)*

Appendix 15 – Extract (cont)

This limitation is significant. Even in the case of face-to-face bullying, it does not cover hostile behaviour directed against student or staff members while they are on the way to, or home from, school (as opposed to actually entering or leaving school premises). Much less does it cover cyber bullying occurring while the target is away from school premises. It does not even cover cyber bullying performed by a bully who is on school premises, perhaps even using school computer equipment, against a target who is not on school premises. Such a position is made even more absurd in a case in which the target is not on school premises because, for example, he or she is at home trying to recuperate from bullying behaviour directed at him or her while on school premises.

(b) Assault

A common assault may be committed by the threat of force which puts the target in fear of imminent violence.[22] Actual direct or indirect application of force is not necessary.[23] This offence exists in all States and Territories.[24] There are minor differences in the elements of the offence between jurisdictions but, generally it is required that:

- *the offender attempt or threaten to apply force,*
- *the threat must be evidenced in some way and*
- *the threat creates an apprehension in the victim of present or immediate harm by reason of the offender apparent ability to carrying out the threat.*

These elements might easily be satisfied in a cyber bullying case such as where, for example, a child receives an SMS message threatening that a gang is coming to kill him or her. However, under the Queensland, Tasmania and Western Australia statutes words or images online are insufficient evidence of a threat.[25]

All jurisdictions also provide criminal sanctions where an assault causes some form of criminal harm, although this is variously described in the various statutes as „grievous", „bodily", „actual bodily" or „serious". A relevant question in this connection is whether „harm" includes psychological harm, as cyber bullying is apt to produce. In England the House of Lords has held that „bodily harm" for the purposes of common law criminal law included mental harm or psychiatric injury provided the latter amounted to a „recognisable psychiatric illness" such as clinical anxiety or prolonged depression.[26] Taking a lead from the law concerning civil liability for psychiatric injury caused by negligence, it was held that the term „bodily harm", as used in the Offences Against the Person Act 1861 (UK), „must be interpreted in the light of the best current scientific appreciation of the link between the body and psychiatric injury".[27] Australian courts have similarly been prepared to recognise psychiatric injury as a form of damage warranting compensation, and it would not be surprising to see a similar interpretation applied to criminal statutes in this country.

This would mean that a criminal offence may be committed where cyber bullying causes its target to suffer a recognisable psychiatric illness.

Recommendation # 6 *(cont)*

Appendix 15 – Extract (cont)

(c) Misuse of Telecommunications Services

The Commonwealth Criminal Code Act 1995 contains a number of offences which may be effective means of redress against a cyber bully who misuses telecommunication services to menace, threaten or hoax other persons. Section 474.17 makes it an offence to use telecommunication services to menace, harass or cause offence (punishable by 3 years). It does not matter whether the menace or threat is caused by the type of use (such as multiple postings on a website) or by the content of the communication or both, provided reasonable persons would regard the use as being menacing, harassing or offensive in all the circumstances.

Where the threat goes further and contains a threat to kill or cause harm, an offence under s 474.15 may be committed. This section provides that it is an offence for a person to use telecommunication services, including the Internet, to threaten to kill (punishable by 10 years imprisonment) or to cause serious harm (punishable by 7 years) to another person (such as the target) or to a third person, if the bully intends the target to fear that the threat will be carried out. „Fear" is defined broadly in the Act to include apprehension, while „threat" is defined as including „a threat made by any conduct, whether express or implied and whether conditional or unconditional." It is not necessary for the target to actually fear that the threat will be carried out, just that it be intended to be so.[28] This is a significant point since most bullies intend that their targets are fearful, and there have been numerous reported cases of death threats and threats of serious harm being made in the cyber bullying context (most commonly by email or text message).[29]

Additional offences in the Criminal Code Act 1995 (Cth) that may be relevant to cyber bullying include s 474.16, which makes it an offence for a person to send a hoax communication intending to induce a false belief that an explosive has been left somewhere (punishable by 10 years imprisonment) and s 474.22, which prohibits using a carriage service for child abuse material. The latter section may catch posting video of sexual assault and other abuse like the incongruously-named „happy slapping", in which an unsuspecting victim is assaulted while an accomplice films the attack, often with a mobile phone, and distributes the video via a website.[30]

(d) Other Threat Offences

All Australian States and Territories have their own threat offences which mirror the Commonwealth threat provisions. These may apply where the cyber bullying does not result in physical injury but puts the target in fear of personal violence against him or her. For example, Crimes Act 1900 (NSW) s 31 makes it an offence to maliciously send or deliver, or cause to be received, any document threatening to kill or inflict bodily harm.[31] Less serious threat offences are also provided for in all Australian jurisdictions,

Recommendation # 6 *(cont)*

Appendix 15 – Extract (cont)

variously prohibiting a cyber bully from threatening to harm, injure or endanger a target to varying levels of gravity.[32]
British Columbia provides an example of the successful prosecution of bullies uttering threats to cause death or serious bodily harm. In the associated cases R v DW and KPD[33] *and R v DH*[34] *the bullying, which including telephone calls, involved threats like „I am going to beat you up" and „You're dead" directed at a girl called Dawn Wesley by her Grade 9 classmates. She later committed suicide, leaving a note attributing her actions to the relentless bullying. In R v DW and KPD, Rounthwaite CJ held that „bodily harm" included „psychological hurt or injury, as well as physical" and found that conditional or future threats were included in the ambit of the relevant offence.*[35]

(e) Stalking and Harassment

The last decade has seen a proliferation of anti-stalking, intimidation and harassment legislation both in Australia and overseas. All Australian jurisdictions now have stalking legislation proscribing behaviour calculated to harass, threaten or intimidate.[36] *Stalking has been described as the „pursuit by one person of what appears to be a campaign of harassment or molestation of another."*[37] *Common examples include following the target, sending articles to the target, waiting outside or driving past the target's home or place of work, and repeated contact by phone, email or text. These offences have proven extremely valuable as part of a larger strategy to contain domestic violence and like behaviours where an imbalance of power is exploited in quite unimaginable and bizarre, but extremely frightening, ways. They are therefore of particular relevance to cyber bullying where, like all cases of bullying, there is a similar exploitation of power imbalance.*

Each of the State and Territory sections contains lengthy, inclusive lists of the types of conduct caught, although there are minor differences in these lists. The anti-

stalking law in Crimes Act 1958 (Vic), s 21A is the one of the most detailed, covering a person who engages in a course of conduct (i.e. at least two occasions) which includes, amongst several other forms of conduct, telephoning, sending electronic messages or otherwise contacting the victim; giving offensive material to the victim or leaving it where it will be found by, given to or brought to the attention of the victim or acting in any other way that could reasonably arouse apprehension or fear in the victim for his or her safety. The conduct must be done with the intention of causing physical or mental harm or arousing apprehension or fear and actually have that result. The Queensland law is also very wide. Under the Queensland Criminal Code s 359B „unlawful stalking" means contacting a person in any way, including, for example, by telephone, mail, fax, e-mail or through the use of any technology, loitering near, leaving offensive material and other types of behaviour that would cause the stalked person fear of violence or property damage or cause detriment to the stalked person or another person (emphasis added).

Recommendation # 6 *(cont)*

Appendix 15 – Extract (cont)

"Detriment" is defined to include apprehension or fear of violence and serious mental, psychological and emotional harm,[38] as is often the case with cyber bullying. It is significant that the section applies to conduct engaged in on „any 1 occasion" if the conduct is protracted.

Legislation in other jurisdictions refers to a person who on at least two occasions stalks another, intending to cause physical or mental harm to that other person or to a third person, or intending to cause apprehension or fear, with „stalking" including conduct involving following, loitering outside where the other person is, interfering with property of the other person, keeping the other person under surveillance or acting in any other way that could reasonably be expected to arouse the other person's apprehension or fear (emphasis added).[39] Cyberbullying would constitute „acting in any other way". Tasmania, like Queensland, specifically includes „contacting" the target as an identified form of stalking,[40] which would embrace cyber bullying. In Western Australia the offence is simply expressed in terms of a person who „pursues another person with intent to intimidate that person or a third person".[41]

By contrast, the New South Wales legislation now proscribes „stalking or intimidation with intent to cause fear of physical or mental harm" very broadly in the newly enacted Crimes (Domestic and Personal Violence) Act 2007[42] while also retaining an offence of „intimidation of annoyance" in the Crimes Act 1900 (NSW) s 545B. The latter provision makes it an offence to use violence or intimidation to or toward another person, or that person"s spouse, child, or dependant. „Intimidation" is further defined as causing a reasonable apprehension of injury, which may be in respect of that person"s property, business, occupation, employment, or other source of income. „Injury" is also said to include „any actionable wrong of any nature". Arguably, therefore, it might also cover damage to reputation (which might otherwise found an action for defamation) or disclosure of personal information (which might otherwise
found an action for breach of confidentiality, or perhaps invasion of privacy)[43] which are potential consequences of some forms of cyber bullying.
The anti-stalking legislation has a number of advantages as a means of addressing cyber bullying. First, a wide range of hostile behaviour falls within its ambit which in itself need not be criminal.[44] For example, a threat which is merely implicit rather than explicit would still be caught. Secondly, while there are differences between jurisdictions in relation to the offender"s requisite intent and the required state of mind (if any) of the victim, it is usually sufficient that the offender, by means of repeated conduct (other than in Queensland, which refers to „at least one occasion"), intends to induce in the target an apprehension or fear of violence or harm (which in most Australian jurisdictions includes the intention to cause the target either physical or mental harm). Accordingly this offence is well suited to cases of cyber bullying, where the purpose is normally to cause emotional, rather than physical, harm and distress.

Recommendation # 6 *(cont)*

Appendix 15 – Extract (cont)

(f) Torture

Queensland and the ACT have both enacted law prohibiting torture.[45] These offences are primarily designed to outlaw the infliction of pain for coercion, punishment, obtaining information or perhaps deviant pleasure.[46] However, the wording of the Queensland section may be wide enough to catch bullying, including cyber bullying. It defines „torture" as the „intentional infliction of severe pain or suffering on a person by an act or series of acts done on 1 or more than 1 occasion", and „pain or suffering" as including physical, mental, psychological or emotional pain or suffering, whether temporary or permanent. As bullying (and by extension cyber bullying), on any sociological conception includes the intent to cause the target emotional or psychological harm and a repetition of the behaviour,[47] it therefore meets the definition of torture. Naturally, whether the prosecuting authorities would be prepared to view a case of cyber bullying in such a light is another question. However, the possibility cannot be discounted if appropriate circumstances presented themselves.

(g) Visual Recording, 'Upskirting' and Breach of Privacy

Some jurisdictions have responded to voyeuristic behaviour involving the surreptitious use of mobile phone camera and other miniature cameras to photograph unsuspecting people involved in private activities or of their private parts (for example, the practice known as „upskirting" where an image is taken covertly looking under a woman's skirt). These jurisdictions have prohibited non-consensual visual recordings of a target when the latter is engaged in a private act or in a private place
(such as showering or toileting at work or school) and the distribution of those recordings (for example, by posting on a web site).[48] When it is considered that such behaviour may result in severe emotional and psychological harm to the target, the application of these provisions in the context of cyber bullying is readily apparent.

(h) Criminal Defamation

Derogatory or denigrating material that is published to others, perhaps by way of a web site, may constitute civil defamation of the target.[49] It might also constitute a criminal defamation. In Australia the common law offence of criminal libel subsists in Victoria, but has been abolished elsewhere and replaced by a statutory offence, generally called „criminal defamation".[50] Even in Victoria there is a statutory offence of publishing false „defamatory libel" that complements the common law.[51]

The statutory offences in New South Wales, Queensland, South Australia, Tasmania, Western Australia and the ACT introduced a requirement of mens rea as an element of the offence. In other words, the prosecution must show both knowledge of falsity and an

Recommendation # 6 *(cont)*

Appendix 15 – Extract (cont)

intention to cause serious harm or reckless indifference.[52] In the absence of admissions by the accused, each fact must be proved by inference.[53] In the Northern Territory the element of mens rea was introduced by setting out a requisite intention for which the defamatory matter was published, namely:

(a) with intent to cause or that causes or is likely to cause a breach of the peace;
(b) with intent to cause loss;
(c) with intent to interfere with the free and informed exercise of a political right;
(d) with intent to prevent or deter a person from performing any duty imposed on him by law;
(e) with intent to prevent or deter any person from doing any act that he is lawfully entitled to do or to compel him to do any act that he is lawfully entitled to abstain from doing;
(f) with intent to prevent any lawful investigation or inquiry; or
(g) with intent to interfere with or to influence any judicial proceeding.[54]

Moreover, intent need not be shown in the Northern Territory where a publication actually causes or is likely to cause a breach of the peace. In Victoria there are two offences following the enactment of an offence of publication of defamatory matter knowing it to be false, which stands alongside the continued operation of the common law criminal libel which does not require an intention to defame or knowledge of falsity.55

Otherwise, most jurisdictions import the meaning of elements like „publish" and „defamatory matter" from law of tort for the purposes of the criminal offence.[56]
Prosecutions for criminal defamation are rare, prosecuting authorities usually taking the attitude that vindication of reputation is best left a matter to be determined civilly between the parties. Nevertheless, they are possible.[57] It is conceivable, then, that cyber bullying may involve a degree of denigration that reaches such a level of criminality that it warrants prosecution by the State.

(i) Accessorial Liability

All jurisdictions prohibit a person from being a party to an offence, for example, by aiding, counselling or procuring a criminal offence.[58] There are numerous ways that such provisions may be involved in a case of cyber bullying. One situation in particular where the provisions may prove useful would be a case of „happy slapping", where the assault on the unsuspecting victim is filmed by an accomplice before being uploaded to the Internet. Thus, while the initial assault may be thought of in terms of face-to-face bullying, the accomplice, in recording and then distributing the footage with the intent of causing greater emotional harm to the target, also engages in cyber bullying.

……

Recommendation # 6 *(cont)*

Appendix 15 – Extract (cont)

5. Conclusion

Cyber bullying is a growing phenomenon, particularly among „Generation Y" – the natives of the digital age. Cyber bullying shares many attributes with face-to-face bullying, including the power imbalance and the ***target's feelings*** *of* ***helplessness*** *and* ***inability*** *to* ***defend himself*** *or* ***herself****, but introduces further dimensions such as the ability to reach the target at anytime and anywhere and the perceived anonymity of the perpetrator.*

*Despite a variety of strategies, face-to-face bullying remains prevalent in our schools. Cyber bullying has now emerged as a further challenge confronting today's young people****. The invocation of the law may seem an extreme response to behaviour which the perpetrator may view as merely having fun. However, the serious harm that may result from cyber bullying may mean that the intervention of criminal, civil and/or vilification laws is appropriate****. However, the extra dimensions that technology offers for a bully, combined with the psychological nature of the harm that it produces, can have an adverse impact upon the effectiveness of the law as a means of redress for the targets of cyber bullying.*

Recommendation # 6 *(cont)*

Appendix 16 - Extract

Future directions in technology-enabled crime: 2007-09

Kim-Kwang Raymond Choo, Russell G Smith, Rob McCusker
Australian Institute of Criminology
Research and Public Policy Series No. 78

Executive summary *(page xx)*

This report examines the future environment in which Australians will use information and communications technologies (ICT) and how this environment will provide opportunities for illegality and infringement of current regulatory controls. In identifying future risk areas, particular focus is placed on the impact these will have for law enforcement, the need for additional resources, law reform, development of cooperative arrangements between Australian and overseas public and private sector organisations, and development of public information and educational resources to minimise the risk of widespread harm to the community.

This report principally adopts the term 'technology-enabled crime' to refer to crimes which require the use of ICT for their commission. Where more specific forms of technology-enabled crime are discussed, terms including 'cybercrime', 'cyberstalking' and so on are used in conformity with Australian legislation such as the *Cybercrime Act 2001* (Cth) and international instruments such as the Council of Europe Convention on Cybercrime. These types of crime are likely to continue to develop over the next two years, the period that constitutes the focus of this assessment. In this report, the term 'organised criminal' refers to criminals or cybercriminals who are involved in the use of an organisational structure to pursue illegitimate goals.

Offensive content (page xx)

Affordable technology has greatly facilitated the production and distribution of child pornography – a multi-billion dollar industry globally. Although the level of knowledge of, and measures to combat, dissemination of child pornography and the sexual abuse of children has increased; individuals and groups of criminals will continue to use ICT to carry out such crimes. The use of ICT to carry out other related sexual abuses involving child victims are also likely to continue in the near future.

Offenders will continue to use cryptographic technologies to prevent detection and to enable images to be shared securely. This will increase the need for law enforcement to enhance its cryptanalysis, steganalysis, and data analysis and storage capabilities. It can also be expected that child exploitation will continue to involve the highly disturbing practice of live child sexual abuse videos being streamed to internet chat rooms, with the actual perpetrator responding in real time to commands from other participants who can see the images. Using the doctrine of constructive presence, it may be possible for such co-offenders to be prosecuted, not only in relation to child pornography distribution, but also as accomplices in sexual assault.

Recommendation # 6 *(cont)*

Appendix 16 – Extract (cont)

With the enactment of new federal offences dealing with child pornography and grooming, it is to be expected that a proportion of future prosecutions will rely on these offences rather than state and territory laws. Law enforcement authorities have, to date, been particularly focused on websites and internet service providers (ISPs) based in Australia that carry child pornography and child abuse material, although arrests for public order offences have also targeted the use of mobile phones and SMS to incite confrontations in public places. These types of acts can fall within the broad category of offences of using a carriage service to menace, harass or cause offence, where the offensiveness of material is to be assessed by 'the standards of morality, decency and propriety generally accepted by reasonable adults'. This provision may also extend to offensive website content such as racial vilification material. It is to be expected that the future will see an increased number of prosecutions for these various forms of content-related offences

Exploitation of younger people (page xx)

As increasingly younger people (the 'digital generation') make use of personal computers and mobile devices, risks may arise where inadequate security measures are in place to secure the technologies they use. Theft of laptops, USB drives, MP3 players and mobile phones from schools and entertainment venues will continue to create problems, not only in terms of replacement costs but also in relation to stolen personal information. Stolen personal and sensitive information will be used to facilitate other crimes such as identity theft and extortion. Online scams are also likely to target young users who may be less vigilant in detecting fraud than are adult users.

A new form of bullying, including harassment targeting young users, has emerged which makes use of communication technologies such as email, text messaging, chat rooms, mobile phones, mobile phone cameras and social networking sites. Cyberbullying will continue to be a problem. Victims may feel socially ineffective and, consequently, may experience greater interpersonal difficulties including a lowering of academic performance.

Legal and evidentiary implications

Legislation *(page xxii)*

In Australia, the growing body of Commonwealth law relating to computer technology, particularly telecommunications systems is likely to increase. These laws operate alongside general criminal laws which are traditionally administered by the states and territories. Specific offences under other federal legislation dealing with such matters as IP rights, classification of publications, terrorism and national security are also likely to be subject to amendment over the next two years to deal with new technological developments and threats.

Although the process of harmonisation of cybercrime legislation throughout Australia has been proceeding, the need for uniformity will become more pronounced as the number of technology-enabled crimes continues to increase. In addition, existing offences, although

Recommendation # 6 *(cont)*

Appendix 16 – Extract (cont)

technically adequate, may be practically impossible to use, such as occurs in the case of botnet-related crimes where evidence would need to be obtained concerning the thousands of computers that have been compromised. New offences of creating a network for illegal purposes and selling established botnets might need to be developed to deal with such emerging threats.

With the addition of Part 10.6 to the *Criminal Code Act 1995* (Cth), which contains offences prohibiting misuse of telecommunications networks for a range of illicit purposes, it can be expected that section 474.14 will largely displace the need to use previously enacted unauthorised access offences such as those in section 477.1. With these new telecommunications offences, it is also likely that Australian government agencies will assume a more dominant role in investigating and prosecuting technology-enabled crimes than was previously the case. Other offences in Part 10.6 are also capable of application to a range of conduct not previously covered by Commonwealth criminal law, such as child pornography, grooming, and racial vilification.

Installing programs that collect and send back information about internet usage ('spyware') is not currently criminalised in Australia. The enactment of legislation to proscribe the usage of spyware has been proposed and its application will need to be monitored to ensure it achieves its objective. In view of these changes, the need for additional resources by federal policing and prosecution agencies will become necessary in the next two years.

Evidentiary and procedural issues *(page xxv)*

It can be expected that those charged with technology-enabled crimes will continue to challenge the legality of electronic searches conducted by law enforcement officers who seek to obtain evidence of technology-enabled crime. Difficulties will continue to arise in determining 'reasonable suspicion' of the existence of evidentiary material relevant to the crime before private premises can be searched. Difficulties will also arise owing to search warrants being insufficiently precise or insufficiently related to the purposes for which the warrant was issued.

The need for law enforcement to be able to obtain evidence legally through remote access to computers located in other jurisdictions will become increasingly important, as will the need to obtain access codes to facilitate access to encrypted or otherwise protected data through using Trojan programs. The ability to obtain evidence in this way needs legislative clarification, as does the use of digital evidence obtained covertly in court proceedings.

Section 3LA *Crimes Act 1914* (Cth) provides a power to compel, by order of a Magistrate, any person suspected of having committed offences to which the warrant relates, or the owner or lessee of the computer or an employee of such a person, to provide assistance that is reasonable and necessary to allow the officer to access data held in, or accessible from, a computer that is on warrant premises; copy the data to a data storage device; and/or convert the data into documentary form. Failure to comply with such an order is punishable by six months. Similar powers are also provided under section 201A *Customs Act 1901* (Cth). It is likely that this provision will be used more often in the future to facilitate access to encrypted or

Recommendation # 6 *(cont)*

Appendix 16 – Extract (cont)

password-protected data. Arguably, the maximum penalty may need increasing in view of the importance of the provision.

Although some memoranda of understanding have been negotiated with private sector organisations, it will become increasingly important to have the cooperation of ISPs and other organisations to facilitate access to data. It will also be likely that ISPs may, themselves, be subject to prosecution for failing to cooperate with law enforcement. There are now provisions that impose obligations on ISPs and internet content hosts to alert police to suspected online child pornography and child abuse material (*Criminal Code Act 1995* (Cth), Section 474.25), and enforcement powers to compel people with knowledge of passwords or computer security protections to assist investigators (*Crimes Act 1914* (Cth), Section 3LA). As organised crime groups move to greater use of the internet and other computer-related technologies, particularly in committing fraud and financial crimes, it can be expected that computer experts who assist by providing their tools of trade will face accessorial liability in relation to these activities.

Delays in the use of conventional mutual legal assistance applications will continue to make their use problematic in technology-enabled crime investigations where cooperation needs to be provided within hours rather than months. On the other hand, however, technology clearly facilitates surveillance and detection enabling law enforcement to follow electronic data trails. The use of data mining and database analysis tools, currently used by financial institutions to detect payment card transaction anomalies, will increase in importance and may lead to reductions in some types of technology-enabled crime.

Tighter regulatory controls may also need to be applied to private sector investigators. For example, at present the use of data surveillance devices by public police is regulated in most jurisdictions. Legislation does not, however, regulate data surveillance by private investigators that can use technologies for keyword searching and blocking of email, surveillance of internet usage and keylogging.

With increased digitisation of information, the future will see an increased likelihood of digital content being a source of disputes or forming part of underlying evidence to support or refute a dispute in judicial proceedings. Better-educated criminals are likely to explore alternatives to hiding data over the internet. These include storing data on password-protected file-sharing websites, email accounts and less reputable content providers hosted in countries with lax cybercrime legislation. Criminals are also likely to leverage the use of anti-forensic tools and information-hiding tools, including steganography, to further impede collection of evidence.

Developments in data storage and dissemination technologies such as proprietary storage media and proprietary cryptographic algorithms can also impede forensic investigators and prevent police from acquiring digital evidence and analysing digital content forensically. For example, the integrity of data can be compromised during extraction or conversion from incompatible proprietary formats. Therefore, an in-depth understanding of how different technologies and applications operate is crucial in collecting digital evidence. Moreover, in response to changing contexts, various computer forensic tools and techniques have to be re-designed and re-engineered.

Recommendation # 6 *(cont)*

Appendix 16 – Extract (cont)

Conversely, forensic investigators and incident handlers can also make use of searching utilities to reduce the time and resources needed to interrogate file systems for keywords.

Criminal trial and sentencing issues *(page xxvi)*

Criminal courts hearing cases involving technology-enabled crime, or other cases involving electronic evidence, face particular issues that will continue to arise. Difficulties concern the presentation of complex and technical evidence, the heavy reliance on expert opinion in technology-enabled crime cases, the use of complex and novel arguments relating to admissibility of evidence or the exercise of discretions, difficulties of juror comprehension of offence elements and evidence, the use of novel defences and defence arguments, and devising appropriate sentences for convicted offenders.

Much of the legislation governing technology-enabled crime has only recently been introduced in Australia and is awaiting judicial interpretation. It can be anticipated that difficulties will arise as untested provisions are relied on in prosecutions.

The need to enhance the skill base of lawyers, judges, juries, and court officials when dealing with cases involving high tech forensic issues, through initiatives such as training materials exploring both legal and technical aspects of technology-enabled crime, will continue. In addition, use of networked and electronically enabled courtrooms that can display electronic evidence in a clear and accessible way to court officials and participants in proceedings will need to be extended. Information protection standards, including best practice guidelines for managing electronic records, will also need to be developed to ensure effective use of technology and to maintain the confidence demanded of courtroom systems.

The future will also see the need to harmonise legislation concerning sentencing and punishments for technology-enabled crimes throughout Australia, and, ideally, across the globe. Achieving some measure of uniformity will help minimise the risk of offenders jurisdiction shopping to seek out countries from which to base their activities that have the least severe punishments.

In sentencing hearings, it is likely that offenders will raise a range of new mitigating considerations. In view of the ever-expanding use of personal computers, it is likely that ‘computer addiction’ (or ‘internet addiction disorder’) will be raised more often as a mitigating factor, or even as a defence vitiating intent.

The courts will continue to experiment with new punishments such as forfeiture of computers and restriction-of-use orders. Restricting access to computers or the internet can have potentially profound consequences, making punishments of this kind arguably more severe than traditional conditional orders. Rather than seeking to impose restrictions on use of computers as a means of punishment, courts could perhaps adopt the alternative approach of requiring offenders to use their computer skills or knowledge for constructive purposes. This could include orders that require offenders to deliver lectures to the public or schools about the dangers of computer crime, and discouraging others from engaging in similar conduct, and performing supervised community service in the high-tech field.

Recommendation # 6 *(cont)*

Appendix 16 – Extract (cont)

Policing and preventive strategies

The role of industry *(page xxvii)*

> Poorly designed, executed and maintained security protocols, processes and devices leave computer networks open to attack. Many of these risks could be minimised though industry developing more secure hardware and software. Security should also be integrated into the software and system development life cycle.
>
> Manufacturers need to be made aware that they could achieve marketing and competitive advantages if they produced new products with higher levels and more innovative types of security that would help combat technology-enabled crime. Law enforcement and security researchers could contribute to a stronger technology security environment by notifying manufactures and vendors of weaknesses that have been discovered in technologies to enable fixes to be formulated, by publicising weaknesses discovered during investigations, and by working with industry to identify potentially new and emerging risk areas.

Public–private sector partnerships *(page xxviii)*

Government has driven much of the response to technology-enabled crime but the private sector plays a crucial role in the fight against technology-enabled crime. Partnerships between public sector police and private sector agencies will continue to be a guiding principle of technology-enabled crime policing in the future. The perceived benefits include increased reporting to police, more timely sharing of information, sharing equipment for processing digital evidence, better preservation of evidence, avoidance of duplicated effort, reducing costs and bi-directional training of investigators. For the private sector, partnerships will also result in commercial opportunities and perhaps more effective policing avenues for their clients. Such partnerships would also prepare businesses in times of pandemics and natural disasters.

Investigations by law enforcement agencies and private investigators will, however, continue to be hindered by the global distribution and increasingly corporate ownership of internet and cyberspace infrastructure and services. Trails of evidence may pass through innumerable hosts, each requiring legal authority to access evidence, while gambling at each step on evidence retention versus business demands for data storage. Both sectors face difficulties establishing identity from online identifiers. The potential sources of digital evidence have also multiplied and are increasingly wireless, miniature and encrypted. By virtue of global organisations spanning international and interstate jurisdictions, corporate investigators will continue to face difficulties of having to deal with many police forces and inconsistent local laws. Civil search and seizure powers available to private investigators are more restrictive than police warrants. Other impediments in relation to transnational policing of technology-enabled crime include deciding jurisdiction, negotiating mutual assistance and extradition, and logistical issues such as navigating time zones and languages.

Recommendation # 6 *(cont)*

Appendix 16 – Extract (cont)

Other likely risks associated with public–private investigative partnerships include inadvertent creation of opportunities for corruption, mishandling of investigations, misinterpretation or planting of digital evidence, and copying of seized, illicit materials. The potential to constrain public police in commercial-in-confidence situations may reduce transparency and possibilities may also arise for the referral of cases to 'for-fee' private investigators that may result in incidents not being investigated if victims cannot or choose not to pay.

The emergence of international networks of Computer Emergency Response Teams, 24/7 law enforcement contact points and other public/user interest groups underscores the intrinsic importance of information sharing in fighting crime. Law enforcement will need resources for ongoing research and development in technology-enabled crime and for sharing of information and intelligence between investigative, intelligence and forensic units. A more responsive distribution mechanism for information will be needed to enable effective responses to technology-enabled crime to be implemented.

Harnessing open source private sector resources, such as development of 'Intellipedia' currently used by the United States intelligence community to disseminate and share intelligence amongst 16 United States intelligence agencies, may assist. Such (confidential) information sharing channels will also be the target of malicious attacks by criminals and terrorists. Information leaked from these channels could potentially result in the compromise of national security.

The use of task forces and training *(page xxix)*

The organisational capacity of law enforcement and other agencies within and across national borders to deal with increasingly complex technology-enabled crime will continue to be constrained. The use of task forces to respond to particularly complex technology-enabled crimes will continue to be beneficial, although this may have the effect of reducing resources for investigation of more mundane, low-value computer crimes. The need for task forces to be established quickly also creates difficulties for investigation of new types of technology-enabled crime, where immediate response is invariably needed. Standing investigatory units may, therefore, offer greater benefits.

The need for training in technology-enabled crime laws targeting IT professionals and legal professionals, particularly concerning evidence and procedure, will increase as countries enact new legislation to deal with emerging threats. Developments in network vulnerabilities will require ongoing training in computer forensics. Although establishment of computer forensics accreditation programs will ensure standards of training are maintained, problems will arise in ensuring adequate staffing levels of accredited investigators. The use of private sector contractors will continue to be necessary, although risk management will be needed to ensure trained personnel do not misuse their skills for non-policing work.

Creation of resources, such as the *Handbook of legal procedures of computer and network misuse in European Union countries*, for police and legal practitioners will continue to be necessary. Australia is well placed to guide training in high-tech law and procedures across the

Recommendation # 6 *(cont)*

Appendix 16 – Extract (cont)

Asia–Pacific region, although any initiatives should be harmonised with activities in Europe and North America.

Increasingly, well-organised groups of forensic examiners working in government facilities or private sector workplaces, such as leading accounting firms, are undertaking forensic analysis of computers for law enforcement purposes. An emerging issue is the desirability of accreditation both for individual examiners and for forensic laboratories, along with validation of forensic analysis tools. Over the next two years, developments will be needed to ensure standards of forensic computing are being maintained nationally and internationally.

Technical assistance to less capable (or less ICT-advanced) jurisdictions will also be essential as the widespread provision of training will allow the leading ICT advanced countries to manage if not prevent many of the cross-border problems now so evident in the delivery of phishing, denial-of-service attacks and other technology-enabled crime.

The absence of suitable training and inappropriate safety cultures appears to be a major challenge and includes household and end-users. For example, vulnerability in Microsoft Word allows remote code execution that requires users to open an infected Microsoft Office document. There is, therefore, a need for coordinated government agency action to promote a culture of security for information systems and networks among end-users, and to ensure the most effective crime prevention advice is provided to the community. User education, through dissemination of media releases by authoritative institutions such as the Internet Crime Complaint Center, enables users to keep abreast of the latest scams and the best fraud prevention measures available.

The complexity of the task of providing training and educational programs in the context of the transnational nature of technology-enabled crime will continue to be challenging and costly.

Prevention and deterrence *(page xxx)*

Law enforcement operates at three broad levels: crime prevention, investigation and prosecution. Public agencies have a limited role in the prevention of technology-enabled crimes, in part because the design of the personal computer and the global adoption of the internet have largely been in the hands of private sector forces with less focus on security than on functionality, and thus the burden of protection against misuse of the technology has fallen largely on individual users. There is a flourishing industry of computer security products and services, such as antivirus software, intrusion detection devices and encryption tools, servicing the increasing desire of individuals and businesses to protect themselves against computer related threats.

Clearly, there is limited capacity in law enforcement to investigate a high volume of technology-enabled crimes, and the future of security will remain largely with system administrators and software developers. Nonetheless, the threat of prosecution and punishment will continue to be a powerful deterrent in this environment, particularly where substantial penalties can be imposed. There will be an ongoing need for effective publicity to be given to the results of successful prosecutions, particularly in new areas of risk. The use of international

Recommendation # 6 *(cont)*

Appendix 16 – Extract (cont)

task force operations should also be widely publicised as indicative of the ability of law enforcement to carry out investigations against individuals located in multiple countries.

Ongoing needs exist for centralised sharing of information and intelligence across jurisdictional borders, both within Australia and internationally. New technology-enabled crime methodologies will continue to emerge and disseminate rapidly requiring the immediate sharing of intelligence and newly developed response strategies. Resources are also needed to map trends in technology-enabled crime to anticipate new areas of risk and to determine when previous types of crimes have dissipated. One of the keys to staying abreast of the latest technologies is to understand both the hardware and software characteristics of the technologies in question.

Knowledge about offender and victim behaviour, as it applies in the online environment, needs to be enhanced. Some of the information gaps are being addressed but further development, based on a clear and functional classification of computer crimes, is essential. To guide training and research, a number of cross-disciplinary applied and theoretical approaches will need to be tested. Along with these essential processes must be a greater willingness to test and re-test software and hardware defences as well as the best forms of general and specific forms of public–private partnerships in preventing technology-enabled crime.

Developments in information and communications technologies that may facilitate technology-enabled crime

New ways of accessing and sharing information electronically *(page 31)*

Ease in accessing and sharing content electronically offers governments and businesses the opportunity to engage the public online and to bridge the gap between sectors. The emerging trend of individuals using the internet to access public-domain services in preference to more traditional offline modes will increase the popularity of digital content in e-commerce, e-government and social-related activities. Examples include:

- **e-tendering:** In the New South Wales Government e-tendering system (https://tenders.nsw.gov.au/nsw/index.cfm), expressions of interest or other such public calls are released by a principal entity inviting other interested entities to tender their submissions before the specified tender closing date. Within a specified period of the tender closing date (e.g. seven working days), the names and addresses of all responding entities will be disclosed unless this would reduce competition in the e-tender process.

- **e-voting:** The Victorian Electoral Commission allows Victorian voters to use designated voting kiosks to cast electronic votes from 13 November 2006.

- **e-reporting:** The United States-based Internet Fraud Complaint Center allows anyone to report information pertaining to online fraud activities. This information is subsequently evaluated and referred to the appropriate agency or jurisdiction.

Recommendation # 6 *(cont)*

Appendix 16 – Extract (cont)

The increasing popularity of second generation of internet-based services – emphasizing online collaboration and sharing among users (i.e. Web 2.0) and supporting virtual communities – will result in new ways of assessing and sharing information electronically, such as:

- **Online chat rooms and social networking sites:** Popular online chat rooms and social networking sites such as Friendster and Myspace allow users to post their personal details and photographs and also interact with other users in real-time.

Information on such sites could be used to identify or profile a particular user and it has been known that such sites can be exploited by malware authors to, for example, increase the yield of phishing attacks as described in the next chapter. Online sexual predators have also been known to make use of chat rooms. In the first investigation leading to prosecution and sentence under s218A of the *Criminal Code Act 1899* (Qld) after it came into effect on 1 May 2003, Queensland investigators posed as a 13 year-old girl (becky_boo 13) in a chat room and received emails from a man wanting to engage the girl in sexual activity. They arrested a 25 year-old man when he appeared at an agreed meeting point to meet the girl. After a guilty plea, the defendant was sentenced to imprisonment for two and a half years, suspended after nine months. This was reduced on appeal to an 18-month term, suspended from the time of the appeal, the defendant having already served 90 days in custody (*R v Kennings* [2004] QCA 162). In another more recent case, Richard Gerard Meehan was charged with one count of using a carriage service – internet chat rooms and mobile phone text messages – to transmit communications to a person under 16 years of age with the intention of procuring that person to engage in sexual activity, contrary to ss474.26(1) of the *Criminal Code Act 1995* (Cth). On 21 July 2006, Meehan was sentenced by the Victorian County Court to 24 months' imprisonment, to be released after having served three months of that term (Hoare 2006).

The House of Representatives in the United States approved the *Deleting Online Predators Act 2006*, which requires schools and libraries in the United States to block access to such sites. Pieces of personal information obtained from social networking sites could also facilitate identity theft (Parker 2007).

Terrorists could, potentially, use online chat rooms and social networking sites as vehicles to reach an international audience, solicit funding, recruit new members, and to distribute propaganda. In March 2007, Singapore's Deputy Prime Minister and Minister of Home Affairs told Parliament that the Internal Security Department of Singapore has investigated internet-driven radicalisation cases involving 'Singaporeans who had become attracted to terrorist and radical ideas purveyed in the mass media, particularly the [i]internet' (Ahmad 2007).

- **Online gaming:** Online games typically played via the local area network and internet form part of a growing industry. Games, particularly massively multiplayer online games (MMOG) and massively multiplayer online role-playing games (MMORPG), that allow players to compete with and against each other on a grand scale in real-time, such as Half-Life, Second Life and Warcraft, are likely to remain popular with the digital generation.

- **Online video sharing websites:** An example of a popular online video sharing website is YouTube (http://www.youtube.com/) that allows users to watch, upload and share

Recommendation # 6 *(cont)*

Appendix 16 – Extract (cont)

- videos online. Law enforcement agencies can also use YouTube as an investigative tool to disseminate information to the public, particular the digital generation. For example, in December 2006, Canadian police posted surveillance video of a murder case that took place in a bar located in Hamilton, Ontario (YouTube turned crime-fighter in Canada 2006). YouTube can also be used as a channel to bring matters of public interest to the attention of law enforcement agencies.

- Examples include:

    - The Los Angeles Police Department and the FBI commenced an internal investigation after video footage was uploaded to YouTube showing two police officers allegedly beating a man during an arrest (Winton & Hong 2006).

    - In February 2007, three men were arrested and charged with possessing a thing (spray paint) with the intention to damage, enter and remain on running rail lines, and two counts of malicious damage, after one of the offenders uploaded the video, filming the act of spraying a CityRail train, to YouTube (Baker 2007).

Online video sharing can, however, be exploited to host offensive content. A recent example is a three-minute video 'lebothugs', uploaded to YouTube in November 2006 that was reportedly watched more than 8000 times.

> [t]he video is backed by a rap song and includes an image of Skaf with a rifle on his lap, footage of a Cronulla riot revenge attack, a photo montage of a group referred to as the 'Soldiers of Granville Boys', and a map of Australia in the colours of the Lebanese flag with the words 'under new management'. Another scene shows a school shirt with a knife on it. (Gibson & Creagh 2007)

Online video sharing can also be exploited as a means to distribute malicious code (e.g. embedded malicious code in MPEG files).

- **Online photo and image sharing websites:** Websites such as http://www.polarrose.com allow users to upload and share photos and images online. Instead of embedding image spam in email, spammers could abuse online photo sharing sites by posting image spam on such sites and embedding the links to the posted image in the email. Using facial-recognition technology, some sites (e.g. Polar Rose website) allow users to search uploaded photos and images based on facial attributes. This could, however, be abused by criminals and individuals to track and stalk their victims online and across websites.

- **Weblogs (Blogs):** Blogs are an emerging form of modern day communication (Rosenbloom 2004, Vogelstein et al. 2005) that allow internet users to disseminate and share information and ideas. Various communities have emerged in the blogosphere (the world of blogs) ranging from technical support communities, such as Google™ blogs (http://googleblog.blogspot.com/), through groups of bloggers who are known to each other, to hate blog groups formed by bloggers who are racists or extremists (Chau

Recommendation # 6 *(cont)*

Appendix 16 – Extract (cont)

- & Xu 2007). In fact, it has been predicted that blogs and Wikipedia will dominate the Web 2.0 landscape in 2007 (Hinchcliffe 2006); the number of bloggers in China is estimated to be 20.8 million (China tops 20m bloggers 2007).

  Blogs such as Google's Blogger.com have recently been used as vehicles to direct unsuspecting users to phishing sites (Fortinet 2007). Blogs can also be compromised by criminals and malware authors exploiting vulnerabilities of web servers or operating systems to host malware (e.g. ransomware and self-mutating Trojan malware). Unsuspecting users' computers can be infected by malware when they visit these compromised blogs (by exploiting vulnerabilities of web servers or operating systems) that host malware (e.g. ransomware and self-mutating Trojan malware).

  Blogs can be used to host offensive content including racial vilification material and insensitive statements about a particular segment in the population. For example, in October 2005, two Singaporeans were convicted under s4(1)(a) of the Sedition Act for posting invective and pejorative remarks on their blogs and a general discussion forum on the internet – see *Public Prosecutor v Koh* (2005) DAC 39442 and *Public Prosecutor v Lim* (2005) DAC 39444.

  - **Wikis (such as Wikipedia):** Implementation of wikis includes Intellipedia, used to disseminate and share intelligence among the 16 United States intelligence agencies (Shrader 2006). Wikis could potentially be exploited by posting malicious content or sensitive information. Examples include a link to the Blaster worm, disguised as a fix to the malware, posted on the German edition of Wikipedia (Leyden 2006b) and a link to the internal documents of global pharmaceutical company, Eli Lilly, alleging that the company was deliberately downplaying the side effects of the drug Zyprexa was posted on the Wiki site http://zyprexa.pbwiki.com/.

  - **Digital television (or internet television):** Research by the Australian Communications and Media Authority (ACMA 2006) indicated that, as at mid 2005, approximately 41 percent of Australian households had some form of digital television. Gartner research (Dulaney & Hafner 2006) and Microsoft chairman Bill Gates (Reuters 2007) also suggested a similar trend; increasing popularity of internet television. This will potentially be another target for distributed denial-of-service attacks and online extortion.

Networked technology will continue to evolve through the use of increasingly faster fibre optical systems that will improve transmission of data within and across networks. Future developments in computing such as web services, such as service-oriented architecture, that provides a framework for building, running, and managing services, and the combination of optical and silicon technologies to facilitate data transfer within chips via laser will also increase the popularity of electronically stored information. Developments beyond the next two years in nanoscience and nanoengineering will increase the use of micro-electromechanical systems that combine electrical and mechanical components to enhance information storage, processing and communication.

Recommendation # 6 *(cont)*

Appendix 16 – Extract (cont)

Summary *(page 43)*

In many ways anticipating the future technological environment in which technology-enabled crimes will be perpetrated is a relatively simple task. Technology will continue to advance rapidly and while those advances may permit faster access to, greater storage capacity within, and greater speed and ease of information dissemination from, computer systems, the potential for witting or unwitting negative impacts upon that information will occur. Poorly designed, executed and maintained security protocols, processes and devices leave computer networks open to attack both by critical infrastructure incidents and deliberate criminal malfeasance. The typology of recent and anticipated security breaches has been typified by the quest for and abstraction of information needed by criminals for committing large-scale and profitable financial crimes. The ability for law enforcement to maintain a watching brief on the potential impact of new technologies and to convey that knowledge to organisations through their own endeavours and/or through legislation and regulation remain ingredients to the effective understanding and mitigation of the future technology-enabled crime environment.

Risk areas and opportunities

Child exploitation and offensive content *(page 62)*

Affordable technology (e.g. websites, web cameras and powerful editing multimedia software) has greatly reduced the barrier to entry for the production and distribution of child pornography. TopTenREVIEWS™ has estimated that child pornography generates approximately US$3 billion annually worldwide (Ropelato 2007). Although the level of knowledge of and measures to combat dissemination of child pornography and involvement of children in sexual offending has increased, individual and groups of criminals will continue to use ICT to carry out such crimes. In January 2007 the FBI arrested several individuals on charges involving possession and distribution of child pornography in connection with the North American Man Girl Love Association (www.namgla.net) website investigation (FBI 2007b). The use of ICT to carry out other related sexual abuses involving child victims (e.g. promoting child sexual tourism and trafficking children) are also likely to continue in the near future.

Offenders will continue to use cryptographic technologies to prevent detection and to enable images to be shared securely. Such cryptographic technologies include steganography, encrypted peer-to-peer networking and encrypted storage media (e.g. PGP Corporation Whole Disk Encryption 9.5 that uses the enhanced-strength advanced encryption scheme 256 encryption algorithm). Instant messaging programs and social networking sites will also continue to be used for child grooming and procuring children for sexual gratification. The enhanced capacity of systems and data transmission capabilities will result in a move from pornographic still images to motion pictures involving children. This will increase the need for law enforcement to enhance its cryptanalysis, steganalysis, and data analysis and storage capabilities.

Recommendation # 6 *(cont)*

Appendix 16 – Extract (cont)

It can also be expected that child exploitation will continue to involve the highly disturbing practice of live child sexual abuse videos being streamed to internet chat rooms, with the actual perpetrator responding in real time to commands from other participants who can see the images. Using the doctrine of constructive presence, it may be possible for such co-offenders to be prosecuted not only in relation to child pornography distribution, but also as accomplices in sexual assault.

With the enactment of new federal offences dealing with child pornography and grooming, it is to be expected that a proportion of future prosecutions will rely on these offences rather than state and territory laws. For example, Richard Gerard Meehan was charged with one count of using a carriage service to transmit communications to a person under 16 years of age with the intention of procuring that person to engage in sexual activity, contrary to ss474.26(1) of the *Criminal Code Act 1995* (Cth). On 21 July 2006, Meehan was sentenced in the Victorian County Court to 24 months' imprisonment, to be released after serving three months of that term (AAP 2006, Australia Commonwealth Director of Public Prosecutions 2006).

Law enforcement authorities have, to date, been particularly focused on websites and ISPs based in Australia that carry child pornography and child abuse material, although arrests for public order offences have also targeted the use of mobile phones and SMS to incite confrontations in public places. This type of act can fall within the broad offence of using a carriage service to menace, harass or cause offence, where offensiveness of material is to be assessed by 'the standards of morality, decency and propriety generally accepted by reasonable adults' (s474.17 of the *Criminal Code Act 1995* (Cth)). This provision may extend to offensive website content such as racial vilification material. It is to be expected that the future will see an increased number of prosecutions for these various forms of content-related offences.

Exploitation of younger people *(page 63)*

As increasingly younger people (the 'digital generation') make use of personal computers and mobile devices, risks may arise where inadequate security measures are in place. Theft of laptops, USB drives, MP3 players and mobile phones from schools and entertainment venues will continue to create problems, not only in terms of replacement costs but also in relation to stolen personal information. Stolen personal and sensitive information will be used to facilitate other crimes, such as identity theft and extortion. Online scams are likely to target young users who may be less vigilant in detecting fraud than are adult users.

In recent years, a new form of bullying, including harassment targeting young users, has emerged which makes use of communication technologies such as email, text messaging, chat rooms, mobile phones, mobile phone cameras and social networking sites. Cyberbullying can also include online fights, denigration, impersonation, trickery, and cyberstalking.

> The anonymity provided by the internet introduces a new element: The victim may have no way to identify the bully. Neither parents nor school officials may know how

Recommendation # 6 *(cont)*

Appendix 16 – Extract (cont)

> to intervene to stop the harassment. Children may be reluctant to report incidents, for fear their computer privileges will be curtailed (Thomas 2006: 1015).

Findings from the second youth internet safety survey (a national telephone survey of a random sample of 1500 internet users between the ages of 10 and 17 years conducted between March and June 2005) indicated that there had been a significant increase in the prevalence of internet harassment since 2000 (Ybarra et al. 2006). Another study commissioned by the National Crime Prevention Council (2007) reported similar concerns. In the study conducted between 2 to 15 February 2006, approximately 46 percent of a nationally representative sample of 824 middle and high school students aged 13 through 17 in the United States reported that they had experienced some form of cyberbullying in the last year

Cyberbullying will continue to be a problem. Victims may feel socially ineffective and consequently, experience greater interpersonal difficulties and exhibit lower academic performance. The consequences of cyberbullying can also shift from cyberspace to a physical location. For example, in June 2004, an 11-year-old girl fatally stabbed a classmate at an elementary school in Sasebo, Japan after an intense online argument (Nakamura 2004).

Legal and evidentiary implications

Legislative reforms *(page 75)*

In Australia, the growing body of federal law relating to computer technology, particularly telecommunications systems, is likely to increase. These laws operate alongside general criminal laws, and other legislation dealing with such matters as IP rights, classification of publications, terrorism and national security which are also likely to be subject to amendment over the next two years to deal with new technological developments and threats. For example, to ensure that crimes involving the criminal misuse of identity can be prosecuted in each jurisdiction, the Australian Government is considering the introduction of legislation that will criminalise activities associated with identity crime (e.g. identity theft and fraud), on-selling of identity data, and possessing equipment to create identification information (Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General 2007). Currently, only Queensland and South Australia have provisions that specifically criminalise such crime.

Section 408D of the *Criminal Code Act 1899* (Qld) makes it an offence to obtain or deal with another entity's identification information for the purpose of committing, or facilitating the commission of, an indictable offence; punishable by a maximum of three years imprisonment.

Recommendation # 6 *(cont)*

Appendix 16 – Extract (cont)

The following provisions in Part 5A of the *Criminal Law Consolidation Act 1935* (SA) criminalise the following conduct:

- Section 144B makes it an offence to assume a false identity (including falsely pretending to have a particular qualification or have, or be entitled to act in, a particular capacity) with the intent to commit, or facilitate the commission of, a serious criminal offence; punishable by a penalty appropriate to an attempt to commit the serious criminal offence.

- Section 144C makes it an offence to misuse personal identification information with the intent to commit, or facilitate the commission of, a serious criminal offence; punishable by a penalty appropriate to an attempt to commit the serious criminal offence.

- Subsection 144D(1) makes it an offence to produce or has possession of prohibited material, with the intent to use the material, or to enable another person to use the material, for a criminal purpose; punishable by a maximum of three years imprisonment.

- Subsection 144D(2) makes it an offence to sell (or offer for sale) or give (or offer to give) prohibited material to another person, knowing that the other person is likely to use the material for a criminal purpose; punishable by a maximum of three years imprisonment.

- Subsection 144D(3) makes it an offence to has possession of equipment for making prohibited material intending to use it to commit an offence; punishable by a maximum of three years imprisonment.

The following provisions in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) could also be applied to identity crime:

- s137 makes it an offence for a person to provide false or misleading documents; punishable by a maximum of ten years imprisonment or 10,000 penalty units, or both.
- ss138(1) makes it an offence for a person to make a false document with the intention that the person or another will produce the false document in the course of an applicable customer identification procedure and the applicable customer identification procedure is under this Act; punishable by a maximum of ten years imprisonment or 10,000 penalty units, or both.

- ss138(3) makes it an offence for a person to knowingly possess a false document with the intention that the person or another will produce it in the course of an applicable customer identification procedure; and the applicable customer identification procedure is under this Act; punishable by a maximum of ten years imprisonment or 10,000 penalty units, or both.

- ss138(5) makes it an offence for a person to possess equipment for making a false document knowing that a device, material or other thing is designed or adapted for the making of a false document (whether or not the device, material or thing is designed or

Recommendation # 6 *(cont)*

Appendix 16 – Extract (cont)

- adapted for another purpose); and has the device, material or thing in his or her possession with the intention that the person or another person will use it to commit an offence against

- ss138(1); punishable by a maximum of ten years imprisonment or 10,000 penalty units, or both.

- ss138(6) makes it an offence for a person to make or adapt a device, material or other thing; and knows that the device, material or other thing is designed or adapted for the making of a false document (whether or not the device, material or thing is designed or adapted for another purpose); and makes or adapts the device, material or thing with the intention that the person or another person will use it to commit an offence against ss138(1); punishable by a maximum of ten years imprisonment or 10,000 penalty units, or both.

Examples of recent amendments of criminal law in other countries include:

- In the United Kingdom, new computer misuse provisions were introduced in the *Police and Justice Act 2006* by way of amendment to the *Computer Misuse Act 1990* on December 2006 to deal with emerging cyberthreats.

- The *Spam Control Act 2007* passed in the Parliament of Singapore on 12 February 2007 (Singapore Infocomm Development Authority 2007; Singapore Parliament 2007) to deal with emerging risks associated with spam (e.g. the use of address harvesting software designed to collect, compile and acquire electronic addresses by searching the internet will be illegal under the proposed Act).

Although the process of harmonisation of cybercrime legislation throughout Australia has been consistent, the need for uniformity will become more pronounced as the number of technology-enabled crimes continues to increase. Existing legislation may not be suitable or adequate within the context of developments in using new and emerging technologies to commit technology-enabled crimes. In addition, existing offences, although technically adequate, may be practically impossible to use, such as occurs in the case of botnet prosecutions where evidence would need to be obtained concerning the thousands of computers that have been compromised. New offences of creating a network for illegal purposes and selling established botnets might need to be developed to deal with such emerging threats.

With the addition of Part 10.6 to the *Criminal Code Act 1995* (Cth) that contains offences prohibiting the misuse of telecommunications networks for a range of illicit purposes, it can be expected that section 474.14 will largely displace the need to use previously enacted unauthorised access offences, such as those in section 477.1. With these new telecommunications offences, it is likely that Australian government agencies will assume a more dominant role in the investigation and prosecution of technology-enabled crime offences, than was previously the case. Other offences in Part 10.6 are also capable of application to a

Recommendation # 6 *(cont)*

Appendix 16 – Extract (cont)

range of conduct not previously covered by federal criminal law, such as child pornography, grooming, and racial vilification.

Although existing Australian laws cover spyware-related malicious activities, installing programs that collect and send back information about usage ('spyware') is not currently criminalised. The enactment of legislation to proscribe the usage of spyware has been proposed (DCITA 2005) and its application will need to be monitored to ensure it achieves its objective. In view of these changes, the need for additional resources for federal policing and prosecution agencies will become more pressing over the next two years.

Jurisdictional issues *(page 78)*

Traditionally, courts have accepted jurisdiction if a person against whom legal proceedings are brought is physically present in the geographical territory (i.e. country or state) in which the court operates, or is a citizen of the territory, or if there is some other sufficient 'territorial nexus'. Such a connection might arise if the alleged victim of a crime is in the territory, or some other effect of the crime, sufficient to exercise jurisdiction, is present. For crimes involving physical acts, rules of jurisdiction have largely been relatively easy to apply, but the situation is more complicated for online activity.

> One of the most important characteristics that tend to distinguish computer-related crime from 'terrestrial crime' is the matter of jurisdiction. The global nature of cyberspace makes it much easier than ever before for a person sitting on one side of the world to commit a crime on the other side (Smith et al. 2004).

It can reasonably be anticipated that technology-enabled crime prosecutions involving multiple jurisdictions will continue to arise in the years ahead. Tracking the fragile and ephemeral digital trails often requires swift action. Because online offending transcends borders so easily, numerous territories can simultaneously assert jurisdiction, particularly when an attack transits multiple jurisdictions with different regimes for preserving evidence. Timely access to evidence located in one or more foreign countries may be difficult or impossible, as it would normally require the assistance of authorities in the foreign country (or countries) that for various reasons may be unwilling or unable to assist. When the suspect is located abroad, these difficulties are compounded. This leads to the need to chose the most appropriate forum for proceedings, with the choice having important consequences due to the different legal systems and penalties that apply in different countries. Conflict in the laws and jurisdictional issues are likely to compromise the effectiveness of legislation and hamper investigation and prosecution of cross-border crimes. It will be necessary for the international community to urgently address problems of multiple jurisdictions.

Identifying and determining the physical location of the perpetrator will continue to be a challenge in an environment where a skilled offender can exploit technologies of anonymity and methods of stealing electronic identities to great advantage. The networked environment of cyberspace compounds this difficulty, as offences that appear to originate in far-flung countries

may in fact have been launched from across town. Conversely, apparently 'local' offences may have originated on the other side of the planet.

Issues relating to extradition are also likely to arise. Although to date, there are no examples of Australians having been extradited overseas, or foreign nationals being extradited to Australia, in relation to offences that could be characterised as technology-enabled crimes, a British national living in Australia, Hew Raymond Griffiths, has been extradited from Australia to the United States to face criminal charges in connection with operating the internet software piracy group, "DrinkOrDie" (US DoJ 2007h). He was extradited from Australia to the United States in February 2007 and pleaded guilty in April 2007 before United States District Judge Claude M. Hilton to one count of conspiracy to commit criminal copyright infringement and one count of criminal copyright infringement (US DoJ 2007d). If convicted on both counts, Griffiths could receive a maximum sentence of ten years in prison and a US$500,000 fine.

Decisions on whether to seek extradition of the offender to deal with them under one's own law will be heavily dependent on the financial cost involved and the existing formal arrangements between countries. There will continue to be demands placed on Australian law enforcement to work collaboratively with overseas law enforcement agencies in identifying and investigating cases suitable for extradition.

Procedural and evidentiary powers *(page 81)*

Authorities expect that those charged with technology-enabled crimes will continue to challenge the legality of electronic searches conducted by law enforcement officers who seek to obtain evidence of technology-enabled crime. Difficulties will continue to arise in determining 'reasonable suspicion' of the existence of evidentiary material relevant to the crime before private premises can be searched. Difficulties will also arise owing to search warrants being insufficiently precise or insufficiently related to the purposes for which the warrant was issued.
The need for law enforcement to be able to obtain evidence legally through remote access to computers located in other jurisdictions will become increasingly important, as will the need to obtain access codes to facilitate access to encrypted or otherwise protected data through use of Trojan programs. The ability to obtain evidence in this way needs legislative clarification, as does the use of digital evidence obtained covertly in court proceedings.

Section 3LA of the *Crimes Act 1914* (Cth) provides a power to compel, by order of a Magistrate, any person suspected of having committed offences to which the warrant relates, or the owner or lessee of the computer or an employee of such a person, to provide assistance that is reasonable and necessary to allow the officer to do one or more of the following:

- Access data held in, or accessible from, a computer that is on warrant premises.
- Copy the data to a data storage device.
- Convert the data into documentary form.

Recommendation # 6 *(cont)*

Appendix 16 – Extract (cont)

Failure to comply with such an order is punishable by 6 months imprisonment. This provision, though seldom if ever used thus far, created a degree of apprehension among legal and computer professionals after its introduction (James 2004). It is likely that this provision will be used more often in the future in order to facilitate access to encrypted or password-protected data. Arguably, the maximum penalty may need increasing in view of the importance of the provision.

Although some memoranda of understanding have been negotiated with private sector organisations, it will become increasingly important to have the cooperation of ISPs and other organisations to facilitate access to data. It will also be likely that ISPs may, themselves, be subject to prosecution for failing to cooperate with law enforcement. There are now provisions that impose obligations on ISPs and internet content hosts to alert police to suspected online child pornography and child abuse material (*Criminal Code Act 1995* (Cth), Section 474.25), and enforcement powers to compel people with knowledge of passwords or computer security protections to assist investigators (*Crimes Act 1914* (Cth), Section 3LA and *Customs Act 1901* (Cth), Section 201A). As organised crime groups move to greater use of the internet and other computer-related technologies, particularly in committing fraud and financial crimes, it can be expected that computer experts who assist by providing their tools of trade will face accessorial liability in relation to these activities.

Delays in the use of conventional mutual legal assistance applications will continue to make their use problematic in technology-enabled crime investigations where cooperation needs to be provided within hours rather than years. On the other hand, however, technology clearly facilitates surveillance and detection enabling law enforcement to follow electronic data trails. The use of data mining and database analysis tools, currently used by financial institutions to detect payment card transaction anomalies, will increase in importance in the future and may lead to reduction of some types of technology-enabled crime.

Tighter regulatory controls may also need to be introduced to control private sector investigators. For example, at present the use of data surveillance devices by public police is regulated in most jurisdictions. Legislation does not, however, regulate data surveillance by private investigators that use technologies for keyword searching and blocking of email, surveillance of internet usage and keylogging.

Computer forensic evidence*(page 83)*

With increased digitisation of information, the future will see the increased likelihood of digital content being a source of dispute or form part of underlying evidence to support or refute a dispute in judicial proceedings.
Digital evidence, typically the first step in any computer forensic process, can be broadly defined as any relevant information or data in electronic storage used to support or prove a fact at issue in judicial proceedings.

Recommendation # 6 *(cont)*

Appendix 16– Extract (cont)

The three broad ways in which digital evidence can be categorised are:

- **records that are computer-stored:** examples include email messages, word processing files, digital images and digital videos

- **records that are computer-generated:** examples include log files generated by web servers

- **records that are partially computer-stored and partially computer-generated:** examples include Excel spreadsheets that contain both human statements and computer processing (Standards Australia International 2003).

Digital evidence differs from traditional evidence. The former is intangible and often transient in nature, and can easily be duplicated, copied, shared, disseminated, modified and damaged. In order to ensure all elements of a proper (digital) evidentiary foundation are correctly established, an understanding of fundamental characteristics underlying digital evidence is crucial in addition to traditional evidential procedures (e.g. thorough documentation to ensure chain of custody). For example, volatile storage media such as hard drives should be stored in static-free bags and recorded. They should be marked as evidence and should not be stored near anything, particularly magnets that could damage evidence on the device.

To address the specific and articulated needs of law enforcement and to ensure (digital) evidentiary admissibility, forensic researchers and practitioners have developed various models for the computer forensic process. Computer forensics can be defined as the science of identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data (NIST 2006a).

Although models for the computer forensic process differ primarily in how granular each phase of the process is and in the terms used for specific phases, they reflect the same basic principles and the same overall methodology (NIST 2006c) particularly proper documentations for the chain of custody.

Example The basic model the National Institute of Standards and Technology - Source: NIST (2006c): 3–1

The process consists of:

- **Collection:** Identification of digital evidence is typically the first step in the forensic processes for computer forensic models. Knowing what evidence is present, where it is stored and how it is stored is vital to determining which processes are to be employed to facilitate its recovery. Computer forensic examiners must be able to identify the type of information stored in a device and the format in which it is stored so that the appropriate technology can be used to extract it.

-

Recommendation # 6 *(cont)*

Appendix 16 – Extract (cont)

- **Examination:** Given the likelihood of judicial scrutiny in a court of law, it is imperative that any examination of the electronically stored data be carried out in the least intrusive manner. There are circumstances where changes to data are unavoidable, but it is important that the least amount of change occurs. In situations where change is inevitable it is essential that the nature of, and reason for, the change can be explained.

- **Analysis:** Analysis of digital evidence includes extraction, processing and interpretation of digital data. This is generally regarded as the main element of forensic computing. Analyses should be performed on the evidence copy and care taken not to alter the original copy of the evidence. Once extracted, digital evidence usually requires processing before people can read it.

- **Reporting:** Presentation of digital evidence: involves the actual presentation in a court of law. This includes the manner of presentation, the expertise and qualifications of the presenter and the credibility of the processes employed to produce the evidence being tendered.

Technology-enabled crime in the courts *(page 87)*

Criminal courts hearing cases involving technology-enabled crime, or other cases involving electronic evidence, face particular issues which will continue to arise in the future. Difficulties concern the presentation of complex and technical evidence, the heavy reliance on expert opinion in technology-enabled crime cases, the use of complex and novel arguments relating to admissibility of evidence or the exercise of discretions, difficulties of juror comprehension of offence elements and evidence, the use of novel defences and defence arguments, and devising appropriate sentences for convicted offenders. For example Sprague (2006) suggested that

> [c]omputer crime prosecutions very often are, or can be forced into being, a form of "complex litigation," chock full of confusing technological terms and concepts. The average juror is generally ignorant of both the theory and practice of computer science. Even "computer savvy" jurors are unlikely to have the training or experience to comprehend complex issues involving networking, security theory and practice, computer architecture, operating systems, system administration, or programming. A conscientious juror may well (and should) have a problem concluding that all reasonable doubt has been eliminated by evidence that he or she does not fully understand (Sprague 2006: 145).

The judge in the Federal Court of Australia case of *Kabushiki Kaisha Sony Computer Entertainment v Stevens* [2002] FCA 906 (26 July 2002) also indicated that '[t]he Court should not be left in a position where it has to guess as to the operation of technological processes and how those processes might satisfy the statutory language'.

Recommendation # 6 *(cont)*

Appendix 16 – Extract (cont)

Such (technical) information that needs to be communicated to the judiciary by the security experts includes:

- the possibility of a wide variety of evidence being extracted from an increasing diversity in sources of computer or electronic exhibits (e.g. GPS devices, engine management systems, CCTV systems, digital cameras and mobile phones).

- the use of mathematical hash algorithms in computer forensics as a means of evidence authentication to be able to trust the hash values that uniquely identify electronic evidence.

- the use of filtering to reduce data volumes including the use of hash sets or targeted searching as their use or non-use may have significant impact on processing time, and accuracy of the results.

- the ability to visualise the 'actual size' of digital data. It has been noted that in a number of court cases, judges, prosecutors and unassisted defence lawyers have asked for all data on a computer exhibit to be printed out. In many technology-enabled cases, a printout of all data produced as a result of an examination would be practically impossible. For example, the amount of information gathered during the investigation in Operation Firewall by the United States Secret Service is estimated to be approximately two terabytes – the equivalent of an average university's academic library (US SS 2004). Moreover, hardcopy printout of an electronic document does not necessarily include all the information stored in the computer or electronic exhibit (e.g. data held in memory) (see *Armstrong v Executive Office of the President* 1 F 3d 1274 (DC Cir 1993)).

Much of the legislation governing technology-enabled crime has only recently been introduced in Australia and is awaiting judicial interpretation. It can be anticipated that difficulties will arise as untested provisions are relied on in prosecutions.

There will continue to be a need to enhance the skill base of lawyers, judges, juries, and court officials when dealing with cases involving computer forensic issues through initiatives such as training materials exploring both legal and technical aspects of technology-enabled crime. This will ensure that judges with appropriate experience and financial and IT skills are available to hear these trials. Continuing training in the presentation of complex technological information to courts and juries for witnesses, particularly computer forensic expert witnesses, will also need to be provided. In addition, the use of networked and electronically enabled courtrooms that can display electronic evidence in a clear and accessible way to court officials and participants in proceedings will need to be extended. Information protection standards including best practice guidelines for managing electronic records will also need to be developed to ensure effective use of technology and to maintain the confidence demanded of our courtroom systems.

Recommendation # 6 *(cont)*

Appendix 16 – Extract (cont)

Sentencing and punishment *(page 89)*

Sentencing practices in cases of technology-enabled crime are continuing to develop and arguably some sentences may seem overly lenient in view of the fact that technology-enabled crime is seen as a novel phenomenon with some types of conduct only recently having been proscribed. The future will see the need to harmonise legislation concerning punishments for technology-enabled crimes throughout Australia, and, ideally, across the globe. Achieving some measure of uniformity will help minimise the risk of jurisdiction shopping by offenders who seek countries from which to base their activities that have the least severe punishments.

In sentencing hearings, it is likely that offenders will raise a range of new mitigating considerations. In view of the ever-expanding use of personal computers, it is likely that 'computer addiction' (or 'internet addiction disorder') will be raised more often as a mitigating factor, or even as a defence vitiating intent.

The future will also see courts continuing to experiment with new punishments such as forfeiture of computers and restriction-of-use orders. Restricting access to computers or the internet can have potentially profound consequences, making punishments of this kind arguably more severe than traditional conditional orders. The simple prohibition on the use of a computer could deprive a person of the ability to find employment in today's inter-connected world. Consequently, this could reduce, not enhance, the possibility of rehabilitation.

Rather than seeking to impose restrictions on the use of computers as a means of punishment, courts could perhaps adopt the alternative approach of requiring offenders to use their computer skills or knowledge for constructive purposes. This could include orders that require offenders to deliver lectures to the public or to schools about the dangers of computer crime, and discouraging others from engaging in similar conduct, and performing supervised community service in the technology-enabled field. Care, however, has to be taken to ensure that offenders do not profit from their crimes (e.g. profiting from the sales of autobiography or rights to a movie).

Summary *(page 90)*

The prosecution and judicial disposition of cases involving technology-enabled crime (particularly arising from the global nature of much technology-enabled crime) will continue to raise certain considerations that make these cases different from cases involving conventional crime. These key issues faced by law enforcement and prosecution include the need for legislative reforms due to new offences, criminal complicity, jurisdictional issues (whether jurisdiction exists and the problem of concurrent jurisdiction); complex and novel arguments relating to admissibility of evidence or the exercise of discretions, novel defences and defence arguments (including in sentencing proceedings); and imposing appropriate sentences on convicted offenders.

Recommendation # 6 *(cont)*

Appendix 16 – Extract (cont)

Policing and preventive strategies *(page 92)*

The threat of technology-enabled crime has given rise to a growing demand for devising new strategies of response. These include the need to reduce the opportunities for technology-enabled crime to occur, to make technology-enabled crime more difficult to commit, to increase the risks of detection and punishment associated with committing technology-enabled crime, and showing that there are fewer benefits to be gained from committing such crimes.

There is no single all-encompassing answer to responding to technology-enabled crime. In fact, countering these risks is a multi-dimensional challenge. It requires effective coordination and collaborative efforts on the part of a wide range of government and private sector entities that can occur at various levels, as described in this chapter.

The role of task forces *(page 97)*

Law enforcement agencies, particularly in ICT advanced countries, have recognised the increased interdependence of global markets and have responded to the general risks of technology-enabled crimes by establishing task forces dedicated to investigating technology-enabled crime cases. The task forces need to have adequately trained personnel capable of undertaking the operational demands of the comprehensive role envisaged by public policing agencies. The organisational capacity of law enforcement and other agencies within and across national borders to deal with increasingly complex technology-enabled crime will continue to be constrained. The use of task forces to respond to particularly complex technology-enabled crimes will continue to be beneficial, although this may have the effect of reducing resources for investigating more mundane, low-value computer crimes. The need for task forces to be established quickly also creates difficulties for investigation of new types of technology-enabled crime, where immediate response is invariably needed. Standing investigatory units may, therefore, offer greater benefits than those units convened in response to a specific identified crime.

Training and educational needs *(page 97)*

Technological expertise, computer forensic capabilities, and sufficient investigative powers within government agencies are important. A focus on training a few experts no longer suffices: both generic and specialist training with common standards are now demanded. The need for training in technology-enabled crime legislation, particularly concerning evidence and procedure, will increase as countries enact new legislation to deal with emerging threats.

Recommendation # 6 *(cont)*

Appendix 16 – Extract (cont)

In fact, it was identified that:

> [i]ncreased funding for law enforcement, including training in cyber forensics, improved vehicles for international cooperation (like the efforts in the G-8 to create national points of contact for cybercrime), and effective national laws (modeled on the Council of Europe Cybercrime Treaty) will also help narrow the opportunities for cybercriminals (McAfee 2005: 17).

Such training should be targeted towards IT professionals, legal professionals and juries, computer forensics professionals and law enforcement officers, as well as end-users and the computer-using public.

Training for information technology professionals *(page 98)*

IT professionals are becoming more actively involved in the investigation and prosecution of technology-enabled crimes. For example, IT professionals may be called upon to help facilitate compliance with legal obligations, developing and operating secure computer systems to ensure the privacy of protected information is not compromised. Training would equip IT professionals with a working knowledge of key legal challenges and issues they are likely to encounter in the course of professional activities.

Training for legal professionals and juries *(page 98)*

Training targeted towards lawyers, prosecutors, judges and juries involved in technology-enabled crime cases, will help them understand technical terminologies crucial to the case. Such terminology would include spyware, adware, encryption, slack space, file allocation table and date/time stamps.

> Crime involving technology is now part of everyday policing and has an effect on all types of crime. A comprehensive training program that reaches the widest audience is therefore essential … Any crime scene could be an electronic crime scene and the correct handling of this type of evidence can positively affect an investigation. However, detections, disruptions, prosecutions and crime reduction/prevention can only be achieved with properly trained personnel who are appropriately equipped to investigate the various aspects of computer-enabled criminality that they encounter in their daily duties (Jones 2005).

Training for legal professionals and juries *(page 98)*

Training targeted towards lawyers, prosecutors, judges and juries involved in technology-enabled crime cases, will help them understand technical terminologies crucial to the case. Such terminology would include spyware, adware, encryption, slack space, file allocation table and date/time stamps.

Recommendation # 6 *(cont)*

Appendix 16 – Extract (cont)

Crime involving technology is now part of everyday policing and has an effect on all types of crime. A comprehensive training program that reaches the widest audience is therefore essential … Any crime scene could be an electronic crime scene and the correct handling of this type of evidence can positively affect an investigation. However, detections, disruptions, prosecutions and crime reduction/prevention can only be achieved with properly trained personnel who are appropriately equipped to investigate the various aspects of computer-enabled criminality that they encounter in their daily duties (Jones 2005).

Training for computer forensics professionals and law enforcement officers *(page 98)*

Developments in network vulnerabilities will require ongoing training in computer forensics. Although establishment of computer forensics accreditation programs (e.g. Certified Forensic Computer Examiner offered by the International Association of Computer Investigative Specialists) will ensure that standards of training are maintained, problems will arise in ensuring adequate staffing levels of accredited investigators. Use of private sector contractors will continue to be necessary, although risk management will be needed to ensure trained personnel do not misuse their skills for non-policing work. A recent example concerns a 'so-called' computer forensics expert hired to testify at two child pornography court cases in the United States who 'pleaded guilty to federal perjury charges for falsifying his resume and lying in open court, presumably about his credentials' (Goodin 2007b, US DoJ 2007a). The indictment alleged that '[a]t the time he worked on the child porn cases, he had already been qualified as an expert witness in computers and submitted court testimony in several jurisdictions, including federal court in California, and in courts in at least two California counties'.

Creation of resources, such as the 'Handbook of Legal Procedures of Computer and Network Misuse in European Union Countries', for police and legal practitioners will continue to be necessary. Australia is well placed to guide training in technology-enabled laws and procedures across the Asia–Pacific region, although any initiatives should be harmonised with activities in Europe and North America.

Increasingly, forensic analysis of computers for law enforcement purposes is being undertaken by well-organised groups of forensic examiners working in government facilities or private sector workplaces. Such groups include leading accounting firms such as KPMG, Deloitte, Ernst & Young and PricewaterhouseCoopers. An emerging issue is the desirability of accreditation both for individual examiners and for forensic laboratories, along with validation of forensic analysis tools. Over the next two years, developments will be needed to ensure that standards of forensic computing are being maintained nationally and internationally.

Technical assistance to less capable (or less ICT advanced) jurisdictions will also be essential as the widespread provision of training will allow the leading ICT advanced countries to manage if not prevent many of the cross-border problems (e.g. rendition of fugitives) now so evident in the delivery of phishing, denial-of-service attacks and other technology-enabled crime.

Recommendation # 6 *(cont)*

Appendix 16 – Extract (cont)

Training for end-users and the computer-using public *(page 99)*

Although Kerr (2007) has suggested that 'user education was no longer applicable because nothing could be done to prevent infection', information security awareness training courses do help reinforce organisations' information security policies. As Rothke (2007) suggested:

> [b]y all means, we need to run the safest operating system we can, fortify our networks and police the whole thing. But once we've done all that, we're left with one unalterable fact: Users will still make errors galore. Training can help.

Information security awareness training courses inform end-users about their accountability for ensuring the integrity, confidentiality, privacy and availability of IT assets within the organisations. For example, in 2007 Microsoft investigated targeted attacks against Microsoft Word using a vulnerability in Microsoft Office 2000 and Office XP that allowed remote code execution when users opened an infected document (Microsoft TechNet 2007).

> It is generally understood by the IT security professional community that people are one of the weakest links in attempts to secure systems and networks. The 'people factor' – not technology – is key to providing an adequate and appropriate level of security. If people are the key, but are also a weak link, more and better attention must be paid to this 'asset'.

> A robust and enterprise wide awareness and training program is paramount to ensuring that people understand their IT security responsibilities, organizational policies, and how to properly use and protect the IT resources entrusted to them (NIST 2003).

Information security awareness training courses will also equip employees with the capacity to recognise basic security breaches or threats and respond to a perceived breach or threat (e.g. to whom and how suspicious occurrences should be reported). Although there is growing awareness among end-users of the need for basic security online, constant and ongoing promotion of a culture of security for information systems and networks among end-users is essential to ensure employees (and also the public) are kept abreast of technology-enabled crime developments and how new security measures can be used to their advantage.

The 2006 AusCERT survey (AusCERT 2006) indicated that 53 percent of respondents ranked inadequate staff training and education in security practices and procedures as one of the most common weaknesses within organisations and one they believed contributed to electronic attacks. The escalating complexities of the end-user environments underline the need for continuing training requirements. The Australian Bureau of Statistics estimated that, as at 30 June 2006, approximately 43.8 percent of the population in Australia was aged 40 and above (ABS 2006b). This particular group might not be as IT literate as the younger generation and hence, might be an easier target for criminals. Constant and ongoing training programs are essential in educating this ageing population about the transnational nature of technology-enabled crime.

Recommendation # 6 *(cont)*

Appendix 16 – Extract (cont)

There is, therefore, a need for coordinated action by government agencies to ensure the most effective crime prevention advice is provided to the community. User education through dissemination of media releases by authoritative institutions, such as the Internet Crime Complaint Center, would enable users to maintain current knowledge of the latest scams and the best fraud prevention measures available.

Costs of training *(page 100)*

The complexity of the task of providing training and educational programs in the context of the transnational nature of technology-enabled crime will continue to be challenging and costly. A survey the Computer Security Institute conducted in 2006 indicated that the reported average security awareness training expenditures per employee ranged from US$18 per employee to US$318 per employee (CSI 2006: 7). This amount is, however, insufficient particularly in light of AusCERT's survey in which 65 percent of the respondents indicated that their organisations needed to improve on the level of qualifications and training for their IT security staff (AusCERT 2006). Moreover, Gartner Research (Fiering & Kirwin 2006) pointed out that an untrained or under-trained desktop user would cost five times more to support than a well-trained worker.

Costs of training depend on various factors, such as:

- whether the training is conducted in-house or outsourced
- the media used in conducting training courses – for example:
    - web-based training that can be undertaken at the organisation's premises
    - classroom-based training courses that take the employees out of the office to outsourced trainers
    - onsite instructor-led training courses that involve no additional travelling for employees
- the type of training courses – training for key security personnel, system administrators and network administrators will be more costly than general security training for those in the organisation performing non-security specific functions (NIST 2003); for example, the cost of the 'SEC 508: System Forensics, Investigation & Response' course conducted in Brisbane on 19–23 February 2007 was approximately $3735 per trainee (SANS Institute 2007)
- opportunity costs such as lost wages and productivity when employees attend training costs
- costs for hosting onsite courses (e.g. training rooms, teleconferencing facility and computer equipment).

Recommendation # 6 *(cont)*

Appendix 16 – Extract (cont)

Policing and technology-enabled crime prevention through deterrence *(page 101)*

Law enforcement operates at three broad levels: crime prevention, investigation and prosecution. Public agencies have a limited role in preventing technology-enabled crime. This is in part due to the design of the personal computer and the global adoption of the internet being largely in the hands of private sector forces that are less focused on security than on functionality. Thus the burden of protection against misuse of the technology has fallen to individual users. There is a flourishing industry of computer security products and services, such as antivirus software, intrusion detection devices and encryption tools, servicing the increasing desire of individuals and businesses to protect themselves against computer-related threats.

Clearly, there is limited capacity in law enforcement to investigate a high volume of technology-enabled crimes, and the future of security will remain largely with system administrators and software developers. Nonetheless, the threat of prosecution and punishment will continue to be a powerful deterrent in this environment, particularly where substantial penalties can be imposed. There will be an ongoing need for effective publicity to be given to the results of successful prosecutions, particularly in new areas of risk. The use of international task force operations should also be widely publicised as indicative of the ability of law enforcement to carry out investigations against individuals located in multiple countries.

Intelligence and the anticipation of future technology-enabled crime *(page 102)*

Centralised sharing of information and intelligence across jurisdictional borders, both within Australia and internationally needs to be an ongoing priority. New technology-enabled crime methodologies will continue to emerge and disseminate rapidly thus requiring the immediate sharing of intelligence and newly developed response strategies. Resources also need to be allocated to mapping trends in technology-enabled crime to help anticipate new areas of risk and to determine when previous types of crimes have dissipated. One of the keys to staying abreast of the latest technologies lies in understanding both the hardware and software characteristics of the technologies in question.
Knowledge about offender and victim behaviour, as it applies in the online environment, needs to be enhanced. Some of the information gaps are being addressed but further development, based on a clear and functional classification of computer crimes, is essential. To guide training and research, a number of cross-disciplinary applied and theoretical approaches will need to be tested. Along with these essential processes must be a greater willingness to test and re-test software and hardware defences as well as the best forms of general and specific forms of public–private partnerships in preventing technology-enabled crime.

Summary *(page 102)*

The rapid uptake of information communications technologies and its convergence with the internet poses new challenges in the formulation of policing and preventative strategies. It is also likely that the incidence of technology-enabled crime will continue to increase over the next two years, with the number of large-scale, organised attacks taking prominence.

Recommendation # 6 *(cont)*

Appendix 16 – Extract (cont)

Over the past decade, considerable progress has been made within and between countries to develop the capacity of law enforcement agencies to respond to technology-enabled crime and there is now growing awareness amongst computer users of the need for basic security online. The saying 'think globally act locally' is especially pertinent in the control of technology-enabled crime given that the pace of technological change will continue unabated, and cybercriminals will continue to adapt (Broadhurst 2006). As reporting of incidents increases among businesses and consumers, the capacity of law enforcement to respond in a timely manner will diminish unless additional resources are made available. The issue of retaining specialist forensic computing staff in the law enforcement sector will also continue to present a significant challenge, particularly due to the high demand for computer forensic experts in the highly paid private sector. Therefore, harnessing expertise of computer forensics in the private sector may be an important way in which the future investigatory caseload could be managed.

The key to future success in controlling technology-enabled crime is the continued development of partnerships between the various stakeholders including industry, academia, government and law enforcement.

Conclusion *(page 105)*

As the internet and other ICT continue to advance, the risks and opportunities for criminals to commit unlawful activities will increase. It is possible to gauge the nature of such threats by examining the kind of technological developments likely to occur and associated community and social changes. With an appreciation of these developments it is possible to predict how criminals in the next two years might act.

Technology-enabled crime ranges across a wide spectrum of activities and behaviours. At one end of the spectrum are crimes that involve fundamental breaches of personal or corporate privacy, such as assaults on the integrity of information held in digital repositories and use of illegally obtained digital information to blackmail individuals or to extort funds from organisations. A related threat is the growing crime of identity theft. Midway along the spectrum are transaction-based crimes such as fraud, trafficking in child pornography, money laundering, and counterfeiting. Another aspect of this type of crime involves individuals within corporations or government agencies who deliberately alter data for profit, personal or political objectives. At the other end of the spectrum are crimes that involve attempts to disrupt the actual workings of the internet. These range from spamming, hacking, and denial-of-service attacks against specific sites to acts of cyber-terrorism.

Technical assistance to less capable or less ICT-advanced jurisdictions will also be essential as the widespread provision of training will allow leading ICT-advanced countries to manage if not to prevent many cross-border problems from emerging.

Only three years ago Smith et al. (2004: 156) observed when discussing crime in the digital environment that 'those who fail to anticipate the future are in for a rude shock when it arrives'. Hopefully, the present report will be of assistance in preventing such a situation from arising over the next two years.

Recommendation # 6 *(cont)*

Appendix 10 – Extract (cont)

"Respect It or Lose It"- Cyber Safety Model - Summary

Stewart Healley - 2010

Appendix 00 - Extract

Introduction:

The Community Cyber Safety Model 2010 - **"Respect It or Lose It"** proposed by Stewart Healley, calls upon the "Proactive Use" of the current Australian Federal Legislation to help set some Basic and Respectful Ground Rules allowing for a Positive Response to the growing problem of Cyber Bullying among our young teenagers aged between 10 and under 18 years old.

A review of current literature reveals a growing concern for how to stop the increase in Cyber-Bullying, especially when it is identified as a major factor in Youth Suicide, now with its own Death Label of "Cyber-Bullycide".

Most Research Papers and many Experts from across the various spectrums are calling for a more active and direct approach focussing on Cyber-Safety.

In my opinion, based on 18 Years of Community Service Experience, is that until we begin to promote the Criminal consequences of Cyber-Bullying, along with actual enforcement, all of our efforts on Cyber-Safety will continue to be seen as "Toothless" with "No" appropriate or adequate protection being offered to our vulnerable victims, families, peers, nor to our community in general. The modern Cyber World has not outstripped the Law.

The Law has been available since 1995, but we have lacked the political will and conviction as a Community to use it. This lack of "Will" and Inertia have allowed a perfect breeding ground for "Bullies" to prosper, with individuals "Free" to "Practice" their methods with the help of some "Irresponsible" Cyber Industry Companies trading our young teenagers for some "Dirty Profit" – "Enough is Enough, it is Time to Act".

To put it more succinctly, of ALL of our pitfalls as a Society the worst occurs when we as a Community "DO NOTHING" to protect our most vulnerable, who are being left to stand alone.

In fact, I would propose that we as a community are helping to reinforce our victims trauma when they finally do "Tell an Adult" the "Adults" do nothing but tell the Victim to "just ignore the Bully"- not very easy for a vulnerable young teenager, especially when the offenders see them

Recommendation # 6 *(cont)*

Appendix 10 – Extract (cont)

as “easy prey” at school and in the neighbourhood, usually on their own with no protection – the “ideal target” for any bully, male and female.

It is now time we as a community stood together to say “NO to Bullying” in any form and to lead the Community and bring on a Test Case or Two?

The **“Respect It or Lose It”** - Cyber Safety Model proposes to encourage ALL Victims of Cyber Bullying incidents, that leave them feeling worried for their Physical and Mental Wellbeing, to attend their nearest Police Station and to formally report the Cyber-Bullying incident with the help of a supportive Parent / Guardian or Adult.

Developing a User Friendly Model:

The **“Respect It or Lose It”** - Cyber Safety Model proposes to assist the attending General Duties Police Officer with:

1. “Easy to Use” Proformas for Victim & 1st Complaint Statements with

2. “Free & Easy Access” to ALL “Carriage Service” Providers for Details & Evidence

3. Referral of case to the Specially Trained Crime Prevention Police Officers for
   3.1 Interview and Assessment of Victim for appropriate Legal Pathway and
   3.2 Interview and Assessment of Offender for appropriate Legal Pathway,

4. Issue Summons for Magistrate Court Pathway as “Ineligible Offender” or

5. Issue Referral for Restorative Justice Pathway as “Eligible Offender”

The **“Respect It or Lose It”** - Cyber Safety Models – “Core Offence” is linked to the use of telecommunications with the help of a “Carriage Service”; specifically under the:

Commonwealth Criminal Code Act 1995:
Chapter 10, Part 10.6, Division 47, Subdivision C

474.17 - Using a carriage service to menace, harass or cause offence

(see Appendix 04)

Recommendation # 6 *(cont)*

Appendix 10 – Extract (cont)

The Community Cyber Safety Model 2010 - **"Respect It or Lose It"** proposal requires a number of Public Departments and Private Enterprises to coordinate a successful Partnership to ensure the success of this new Cyber-Safety Model.

Some of these new Partnerships will need to include:

1. **Police Departments (AFP – ACT)**

    1.1 General Duties Training in Model Statements, Requests & Referrals

    1.2 Detective Training in Model Statements, Requests & Referrals

    1.3 Hi Tech Crime Technician –
    - 1.3.1 Apply & Execute Search Warrant for Evidence
    - 1.3.2 Check Equipment & Present as "Expert" Court Evidence

    1.4 Crime Prevention – Cyber-Safety Education Unit
    - 1.4.1 Teach a 1 x Day or 2 x Evenings Training Program for "Eligible Offender" on Caution & Restorative Justice Pathway
    - 1.4.2 Apply & Execute Warrant for Equipment Search & Evidence

2. **Department of Public Prosecutions (ACT) [or Police Prosecutions Office]**

    2.1 Obtain Warrant Equipment Search & Evidence

    2.2 Magistrate Court – Offender Prosecution

3. **Restorative Justice Program, ACT - [Dept. Justice & Community Safety]**

    3.1 General Duties Training in Cyber-Safety Model

    3.2 Crime Prevention – Cyber-Safety Education Unit

4. **ACMA & All Service Providers – Mobile Phones / Internet – "Carriage Services"**

    5.1 Telstra - Cyber Safety Unit – providing Free & Easy Account details

    5.2 Optus - Cyber Safety Unit – providing Free & Easy Account details

    5.3 Vodafone - Cyber Safety Unit – providing Free & Easy Account details

    5.4 Dodo - Cyber Safety Unit – providing Free & Easy Account details

    5.5 New Carrier Service/s – providing Free & Easy Account details

Recommendation # 6 *(cont)*

Appendix 10 – Extract (cont)

Developing a new Socially Responsible and Sustainable Business Model:

Current Carriage Service Provider practice is:

1 The Police are provided with “Free” Carriage Service assistance when dealing with a “Life Threatening” situation.

2 The Police are “Charged” a “Variable” but “Substantial Fee” for Carriage Service assistance when dealing with a “Non - Life Threatening” situation, as required under current Legislation for Service Cost Recover.

3 The initial and continued use of ANY Carriage Service is based on the User Agreeing to accept the Provider’s Terms and Conditions that may vary at any stage and payment of the Service Use Account.

Note: ALL Account holders must be a minimum of 18 Years to legally open an Account with ANY Carriage Service Provider. This means, ALL teenagers aged between 10 and under 18 years old, are using an Account set up by their Parent / Guardian or Support Adult.

A Socially Responsible and Sustainable Business Practice” response to these conditions includes;

1 Continuing the “Free” Carriage Service assistance for “Life Threatening” situation is a “High Value” - Socially Responsible and Sustainable Business Practice”.

2. The current Practice of charging any “Fee” to the Police is a “Low Value” - Socially Responsible and Sustainable Business Practice” and will inhibit the implementation, use and effectiveness of this new Cyber Safety Model by Police.

All of the Carriage Service Providers will need to be granted an alternative Service Costs Recovery method to also include Non Life-Threatening Cases. This is a crucial step to help Off-Set ANY costs to the Police Budget and to remove one financial barrier that has reportedly “Restrained” Police Action on Cyber-Bullying complaints.

3. Part of the scope of the new Cyber Safety Model is to make the Offender and Account Holder e.g. Parent / Guardian / Support Adult more accountable and visible.

The “Maturing” Teenager – A Reality Check:

Fortunately, most Parents / Guardians do see their children in real terms, capable of “great deeds” and “amazing stupidity”. Most “normal teenagers” learn and are guided by testing behaviour patterns and decision making against “KNOWN” boundaries and “IMMEDIATE” consequences”, set by ADULTS e.g. “I didn’t know & “that’s not fair”.

Recommendation # 6 *(cont)*

Appendix 10 – Extract (cont)

This situation is fortunately or unfortunately being proven as "normal" or "to be an expected" scenario when viewed with the latest Teenage Brain Development studies.
So, if you are looking for teenagers to have a "Consistent, Mature and Rational" response to MOST situations we may have to come back in 5 to 10 Years Time! Or, we can ASK our TEENAGERS to HELP set these BOUNDARIES – TOGETHER.
Adults and especially teenagers need to "KNOW" their thoughts and feelings really do matter and when ASKED to TALK about their PROBLEMS, like Cyber Bullying they learn to respond with TRUST instead of – "You don't understand – whatever".

Thankfully, for around 90% of teenagers, when given support, encouragement and opportunity, do learn to accept Social Responsibility and prefer to make "Friends" and be part of "The Group" than to make "Enemies" and be outside "The Group".

For this group of teenagers the new Cyber Safety Model will allow them to participate in a Restorative Justice Pathway and learn as most participants do , along with Parents / Guardians; that "ALL Things are Negotiable" and Negotiating your Problems in a Positive Way, builds confidence, resilience and a healthy feeling of wellbeing.

Parent / Guardian Support:

Parents / Guardians can also show their support for the new Cyber Safety Model by agreeing to voluntarily request their Carriage Service Provider to withhold Outgoing Calls for a "Just and Fair Penalty Period of 7 Days". This is also a form of insurance so, that the teenager is not tempted to make a silly mistake of making a "Revenge Call in the Heat of the Moment". Thereby, causing the teenager to be reassessed and excluded from the Restorative Justice Pathway, as an "Ineligible Offender".

An important safety feature is maintained while the Carriage Service Provider can bar or block all outgoing calls on a Mobile Phone. All incoming calls are still allowed, ensuring Parents / Guardians can still keep in contact with their teenager and if need be all Emergency Service calls are still available to help keep the teenager safe.

Unfortunately, for the remaining 10% of teenagers that do not "choose to be" or "accept" any form of Social Responsibility; and are usually supported "blindly" and sometimes "aggressively" by their Parents / Guardians no matter what evidence is produced, will not be suitable for the Restorative Justice Pathway and will be assessed as an "Ineligible Offender".

This group of teenagers, prefer to push the "Power" or "Bullying" Tactics for social status and acceptance with an attitude of "well, who's going to stop me then!". Unfortunately, this group will continue to present themselves in various conflicts, sometimes as the "Victor" when they have the Power Advantage and sometimes as the "Victim" when they do not have a Power Advantage..

Recommendation # 6 *(cont)*

Appendix 10 – Extract (cont)

For this group of teenagers the new Cyber Safety Model – Restorative Justice Pathway will not be their first choice as they travel along the usual and predictable, Summons, Warrant, Magistrate Court Pathway, usually kicking and screaming out “your all a pack of X#%!” and that’s just the girls.

However, as these teenagers progress along the Magistrate Court Pathway, they are still able to choose a Restorative Justice Pathway, if and only if they choose to do so voluntarily and are re-assessed as an “Eligible Offender”.

Hence, real progress can still be fostered in these teenagers, who face an enormous personal challenge in changing their core beliefs and behaviour by accepting new ways to trust, grow and learn “Social Responsibility”.

Recommendation # 6 *(cont)*

Appendix 10 (cont) **- "Respect It or Lose It"- Cyber Safety Model - Legislation**

Commonwealth Criminal Code Act 1995

Schedule Criminal Code

Chapter 10 National infrastructure

Part 10.6 Telecommunications Services

Division 474 Telecommunications offences

Subdivision C - Offences related to use of telecommunications

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 3 years.

(2) Without limiting subsection (1), that subsection applies to menacing, harassing or causing offence to:

(a) an employee of the NRS provider; or

(b) an emergency call person; or

(c) an employee of an emergency service organisation; or

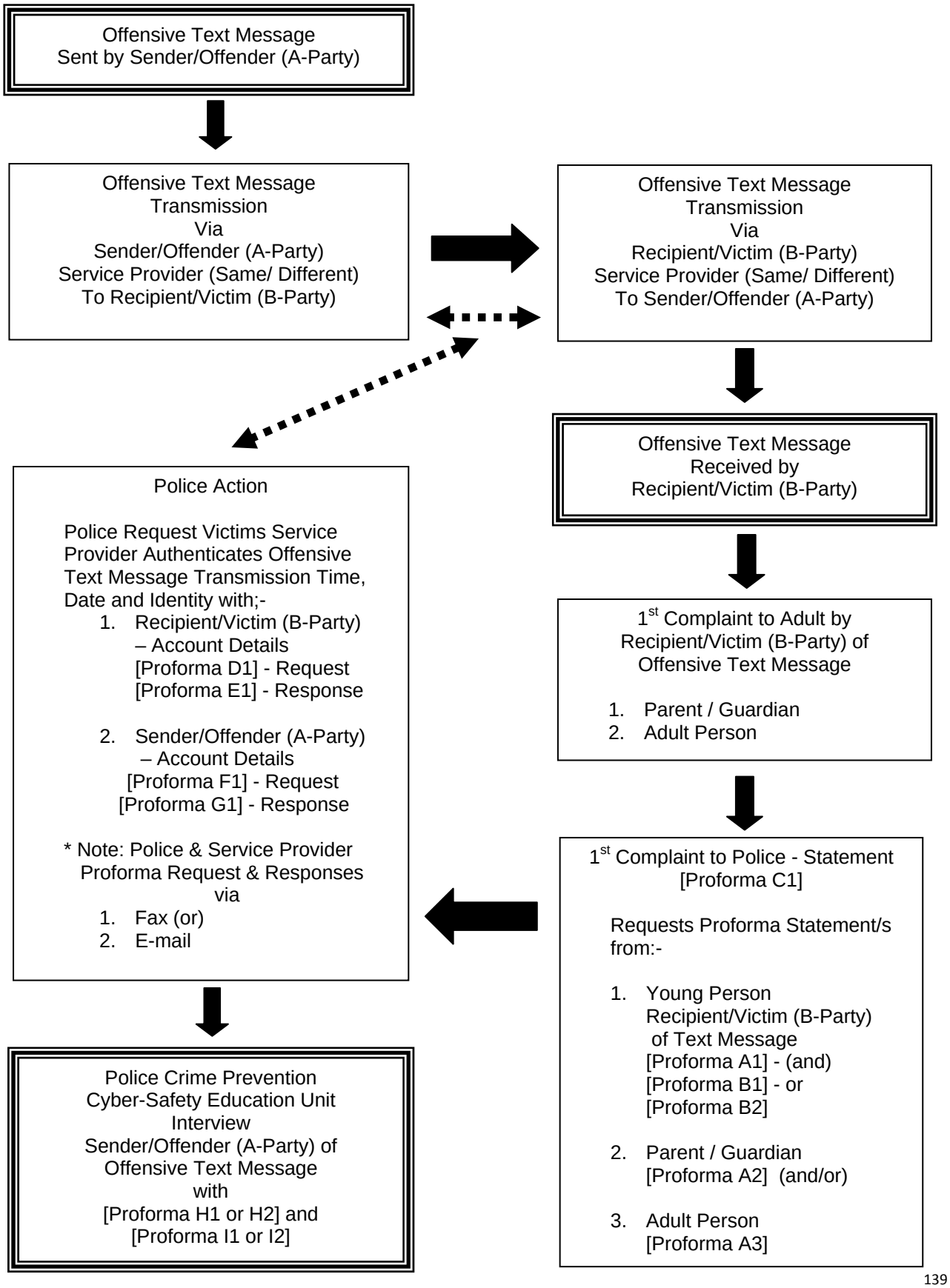
(d) an APS employee in the Attorney-General's Department acting as a National Security Hotline call taker.

Recommendation # 6 *(cont)*

Appendix 10 (cont) **- "Respect It or Lose It"- Cyber Safety Model - Legislation**

Commonwealth Criminal Code Act 1995

Rec 6: Appendix 10 (cont) - "Respect It or Lose It"- Cyber Safety Model - Stage 1A



Rec 6: Appendix 10 (cont) - "Respect It or Lose It"- Cyber Safety Model - Stage 1B

Brief of Evidence

A; **Proforma Statements**:-
1. Recipient/Victim (B-Party) (Young Person) - [Proforma A1]
2. Parent/ Guardian – if 1st Complaint to Adult - [Proforma A2]
3. Adult – 1st Complaint to Adult - [Proforma A3]
(1 x Original + 3 Copies)

B; **Recipient/ Victim Statement advising of Preferred Police Action**
1. Magistrate Court (or) – [Proforma B1]
2. Diversionary Pathway Process E.g. Restorative Justice – [Proforma B2]
Note – if "Eligible Victim"
[Circle Sentencing Process may not be appropriate pathway]
(1 x Original + 3 Copies)

C: **Police Complaint Corroboration Statement**
1. 1st Complaint to Police - [Proforma C1]
(1 x Original + 3 Copies)

D: **Police Request to Service Provider - Proforma for**
1. Recipient/ Victim (B-Party) - Further Particulars – [Proforma D1]
(1 x Original + 3 Copies)

E: **Service Providers Response to Police Request for**
1. Recipient/ Victim (B-Party) - Further Particulars – [Proforma E1]
(1 x Original + 3 Copies)

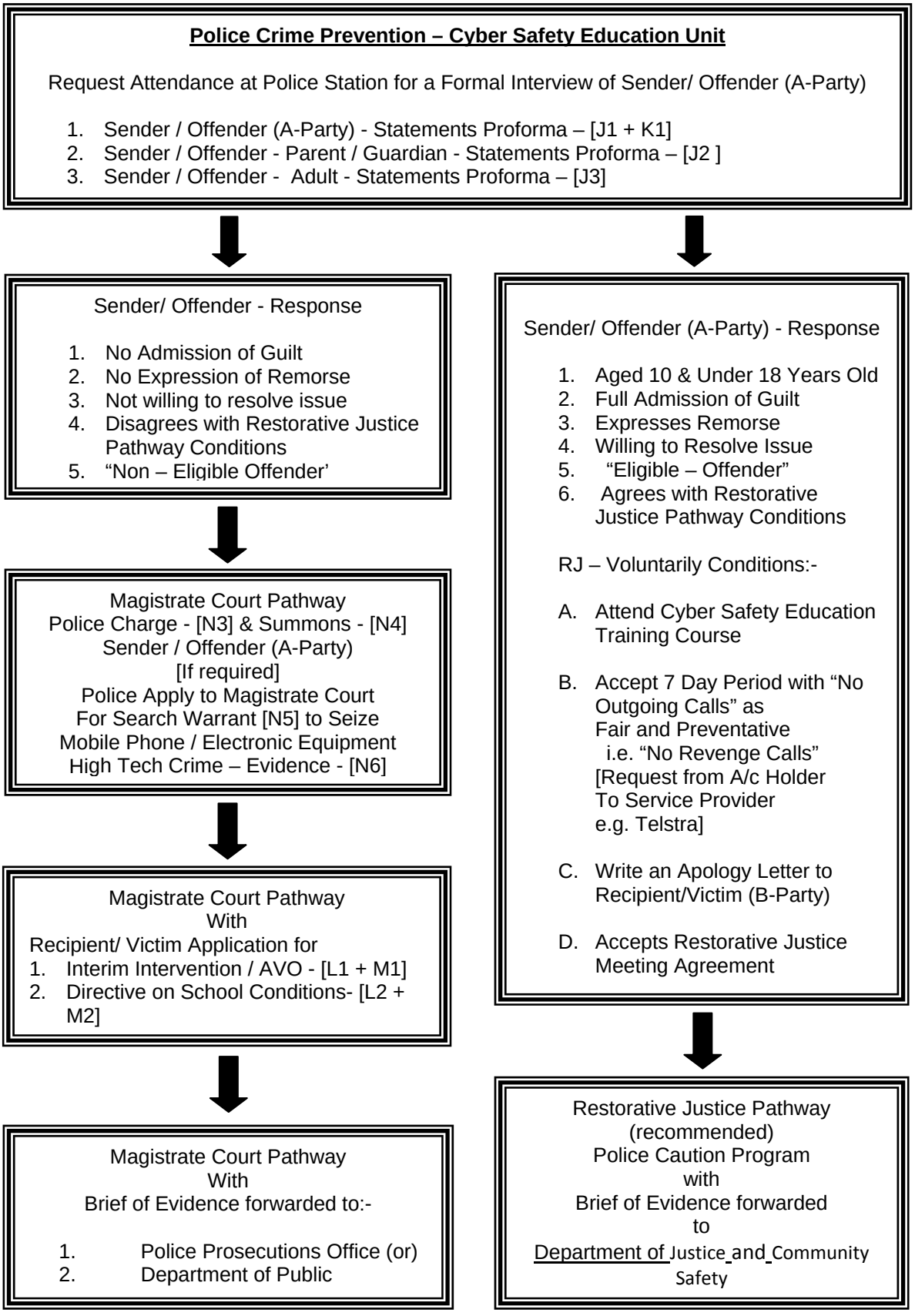
F: **Police Request to Service Provider - Proforma for**
1. Offender/ Sender (A-Party) – Further Particulars – [Proforma F1]
(1 x Original + 3 Copies)

G: **Service Providers Response to Police Request for**
1. Offender/ Sender (A-Party) – Further Particulars – [Proforma G1]
(1 x Original + 3 Copies)

H: **Police Pathway Request Proforma for Matter to be dealt with by**:-
1. Magistrate's Court – Proforma H1]
2. Diversionary Pathway- Eligible Offender (e.g. Age / Priors) OR – [Proforma H2]

I: **Police Request to Police Crime Prevention Unit - Proforma**
Cyber-Safety Education Unit to Interview & Assess
Sender/Offender (A-Party) with the matter to be dealt with by:-
1. Magistrate's Court – [Proforma I1]
2. Diversionary Pathway – if "Eligible Offender" (or) – [Proforma I2]

Rec 6: Appendix 10 (cont) - "Respect It or Lose It"- Cyber Safety Model - Stage 2A



Rec 6: Appendix 10 (cont) - "Respect It or Lose It"- Cyber Safety Model - Stage 2B

Police Crime Prevention – Cyber Safety Education Unit

Brief of Evidence - Case Documents

A – I. Proformas and Police Request for Interview of Sender/Offender (A-Party) with matter dealt with Preferred Police Action by:-

1. Magistrate's Court - [Proforma B1 + H1]
2. Diversionary Pathway – if "Eligible Offender" (or) - [Proforma B2 +H2]

Interview Documents:

J. Proforma Interview Statements:-

1. Sender / Offender (A-Party) - [Statements Proforma - J1]
2. Sender / Offender - Parent / Guardian - [Statements Proforma - J2]
3. Sender / Offender - Adult - [Statements Proforma - J3]

K. Sender / Offender (A-Party) - Statement advising of Preferred Police Action

1. Magistrate Court [Proforma – K1] (or)
2. Diversionary Pathway Process E.g. Restorative Justice [Proforma – K2]
   Note – if "Eligible Offender"
   [Circle Sentencing Process may not be appropriate pathway]
   (1 x Original + 3 Copies) from:-

Magistrate Court Documents:

L. Recipient / Victim (B-Party) - Application to Magistrate Court for

1. Interim Intervention / AVO – [Proforma L1]
2. With Directive on School Conditions – [Proforma L2]

M. Magistrate Court – Documents of Approving / Granting of:

1. Interim Intervention / AVO – [Proforma M1]
2. With Directive on School Conditions – [Proforma M2] – Forwarded to Principal

AFP Police Crime Prevention – Cyber Safety Education Unit - Documents

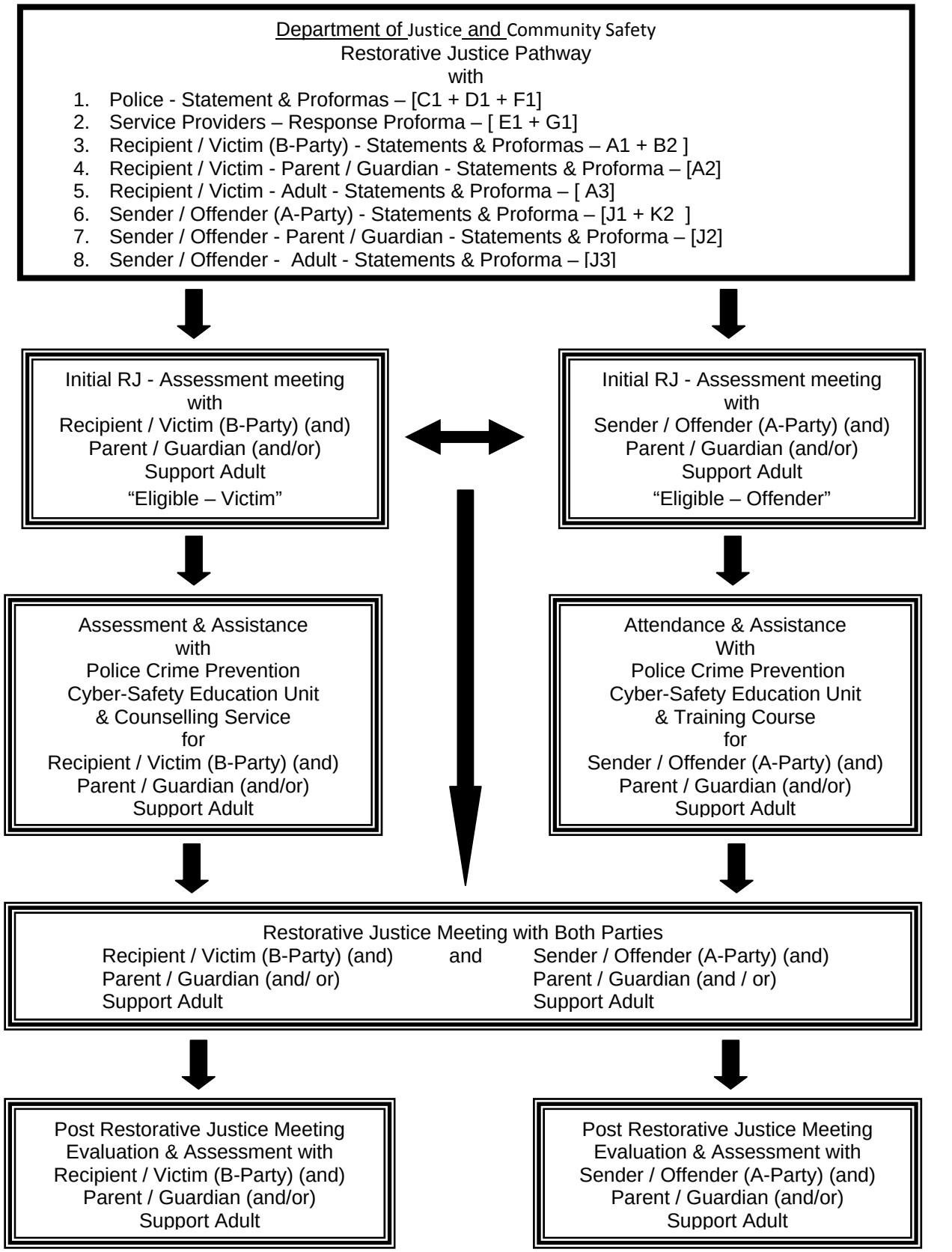
N Assessment of:

2. Recipient / Victim (B-Party) - "Eligible Victim" - Yes / No - Proforma – [N1]
3. Sender / Offender (A-Party) - "Eligible Offender" - Yes / No – Proforma – [N2]
4. Charge Sheet – [N3]
5. Summons – Magistrate Court - Mention Court – [N4]
6. Search Warrant & Search Result – if required – [N5]
7. High Tech Crime Technician – Mobile Phone / Electronic Equipment - Evidence

Brief of Evidence Documents compiled and forwarded to

1. Police Prosecutions Office or DPP for a Magistrate Court Pathway (or)
2. Department of Justice & Community Safety for Restorative Justice Pathway

Rec 6: Appendix 10 (cont) **- "Respect It or Lose It"- Cyber Safety Model - Stage 3A**



Rec 6: Appendix 10 (cont) - "Respect It or Lose It"- Cyber Safety Model - Stage 3B

Department of Justice and Community Safety

Restorative Justice Pathway

Process with Request Proformas from:-

Police – 1st Complaint:

1. Police Proforma - Corroboration Statement – [C1]
2. Police Proforma Request to Recipient/ Victim (B-Party)
   Service Provider for further particulars – [D1]
3. Police Proforma Request to Offender/ Sender (A-Party)
   Service Provider for further particulars – [F1]

Service Provider:

1. Service Provider Response to Recipient/ Victim (B-Party) details - [E1]
2. Service Provider Response to Senders / Offender details - [G1]

Recipient / Victim (B-Party):

1. Recipient/ Victim (B-Party)- Statements Proforma – [A1]
2. Recipient/ Victim (B-Party)– Preferred Police Action Proforma:
   1. Magistrate Court Proforma – [B1] (or)
   2. Diversionary Pathway Process E.g. Restorative Justice – [B2]
3. Recipient/ Victim (B-Party)- Parent / Guardian - Statement Proforma – [A2]
4. Recipient/ Victim (B-Party)– Adult - Statements Proforma – [A3]

Sender / Offender (A-Party):

1. Sender / Offender (A-Party) - Statements Proforma – [J1]
2. Sender / Offender (A-Party) Proforma choice of:
   1. Magistrate Court [Proforma – [K1] (or)
   2. Diversionary Pathway Process E.g. Restorative Justice – [K2]
3. Sender / Offender (A-Party) - Parent / Guardian - Statements Proforma – [J2]
4. Sender / Offender (A-Party) – Adult - Statements Proforma – [J3]

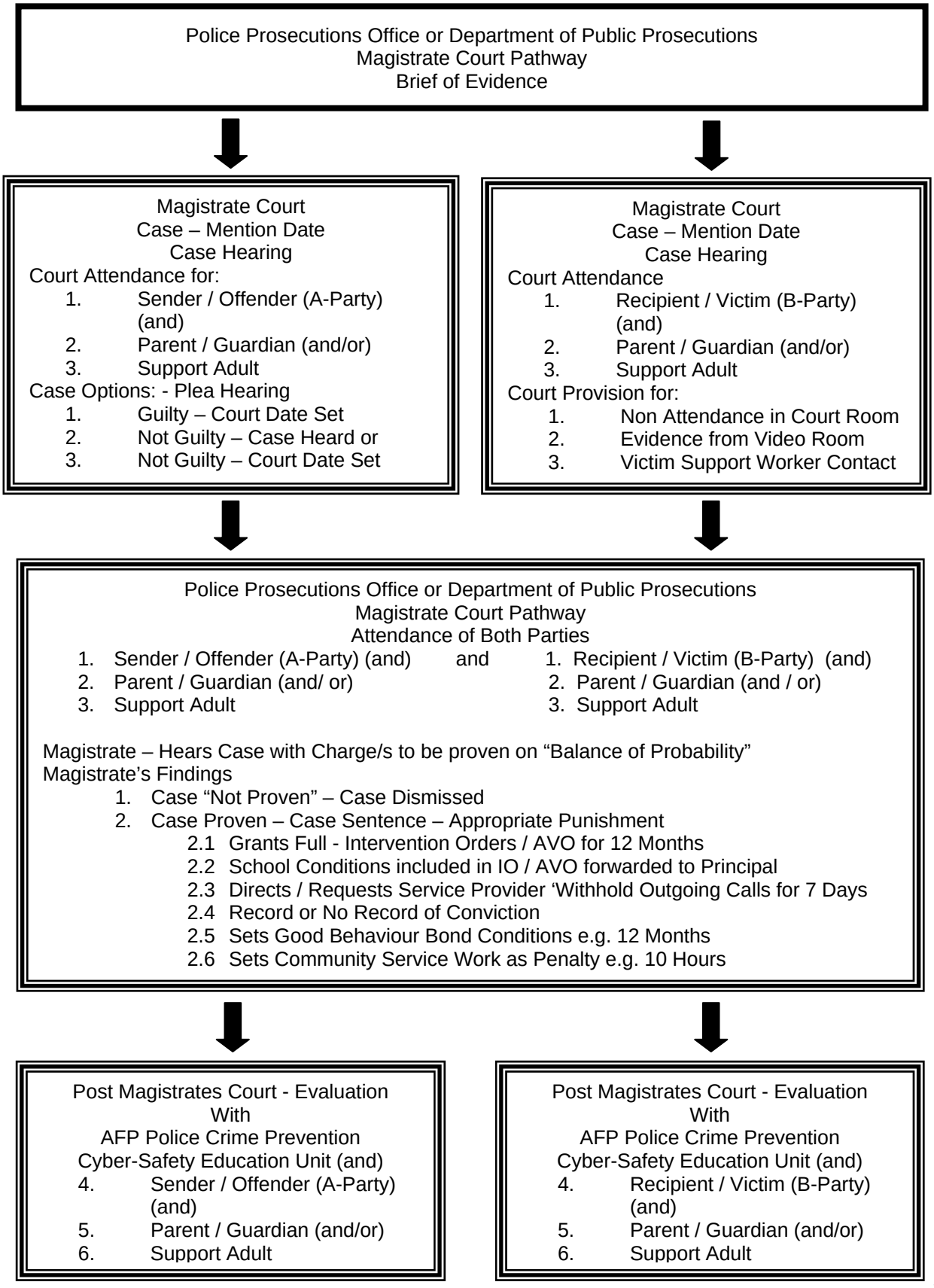
Magistrate Court

1. Interim Intervention / AVO – L1 & M1 (and)
2. With Directive on School Conditions –L2 & M2

Cyber Safety Education Unit:

1. Assessment of Recipient / Victim Proforma – "Eligible Victim" - Yes / No
2. Assessment of Sender / Offender Proforma – "Eligible Offender" - Yes / No

Rec 6: Appendix 10 (cont) - "Respect It or Lose It"- Cyber Safety Model - Stage 4A



Rec 6: Appendix 10 (cont) - "Respect It or Lose It"- Cyber Safety Model - Stage 4B

Brief of Evidence Documents compiled and forwarded to

1. **Police Prosecutions Office or DPP for a Magistrate Court Pathway (or)**

2. **Department of Justice & Community Safety- Restorative Justice Pathway - Monitor**

3. **Police Crime Prevention - Cyber-Safety Education Unit for Evaluation of:**
   Magistrate Court Pathway with:-

   1. **Recipient / Victim (B-Party)** (and)
   2. Parent / Guardian (and/or)
   3. Support Adult
   4. School Principal & Student Welfare Team

   and

   1. **Sender / Offender (A-Party)** (and)
   2. Parent / Guardian (and/or)
   3. Support Adult
   4. Sender / Offender – School Principal & Student Welfare Team

Recommendation # 7

Establish Constructive and Regular Consultation with teachers, parents, and young people

Details of:
Recommendations for Joint Parliamentary Committee on Cybersafety (cont)

Recommendation # 7

Establish Constructive and Regular Consultation with teachers, parents, and young people

The National Child and Young Persons Human Rights Council to seek and maintain an active input from **teachers, parents,** and **young people** through linking with existing groups and organisations

7.1 Establish quality Training in Anti Bullying and Cyber Safety for:

- Teachers
- Parents and
- Young People

.

Comment

I strongly urge The National Child and Young Persons Human Rights Council follow the excellent advice of the Australian Institute of Criminology, Research and Public Policy Series No. 78 Report, by providing ongoing, quality Training for **Teachers, Parents and Young People.**

Appendix 16:

Extracts of the Report: are as follows:

Future directions in technology-enabled crime: 2007-09
Kim-Kwang Raymond Choo, Russell G Smith, Rob McCusker
Australian Institute of Criminology- Research and Public Policy Series No. 78

Training for end-users and the computer-using public *(page 99)*

Although Kerr (2007) has suggested that 'user education was no longer applicable because nothing could be done to prevent infection', information security awareness training courses do help reinforce organisations' information security policies. As Rothke (2007) suggested:

> [b]y all means, we need to run the safest operating system we can, fortify our networks and police the whole thing. But once we've done all that, we're left with one unalterable fact: Users will still make errors galore. Training can help.

Recommendation # 7 *(cont)*

Appendix 17 – Extract (cont)

Information security awareness training courses inform end-users about their accountability for ensuring the integrity, confidentiality, privacy and availability of IT assets within the organisations. For example, in 2007 Microsoft investigated targeted attacks against Microsoft Word using a vulnerability in Microsoft Office 2000 and Office XP that allowed remote code execution when users opened an infected document (Microsoft TechNet 2007).

> It is generally understood by the IT security professional community that people are one of the weakest links in attempts to secure systems and networks. The 'people factor' – not technology – is key to providing an adequate and appropriate level of security. If people are the key, but are also a weak link, more and better attention must be paid to this 'asset'.
>
> A robust and enterprise wide awareness and training program is paramount to ensuring that people understand their IT security responsibilities, organizational policies, and how to properly use and protect the IT resources entrusted to them (NIST 2003).

Information security awareness training courses will also equip employees with the capacity to recognise basic security breaches or threats and respond to a perceived breach or threat (e.g. to whom and how suspicious occurrences should be reported). Although there is growing awareness among end-users of the need for basic security online, constant and ongoing promotion of a culture of security for information systems and networks among end-users is essential to ensure employees (and also the public) are kept abreast of technology-enabled crime developments and how new security measures can be used to their advantage.

The 2006 AusCERT survey (AusCERT 2006) indicated that 53 percent of respondents ranked inadequate staff training and education in security practices and procedures as one of the most common weaknesses within organisations and one they believed contributed to electronic attacks. The escalating complexities of the end-user environments underline the need for continuing training requirements. The Australian Bureau of Statistics estimated that, as at 30 June 2006, approximately 43.8 percent of the population in Australia was aged 40 and above (ABS 2006b). This particular group might not be as IT literate as the younger generation and hence, might be an easier target for criminals. Constant and ongoing training programs are essential in educating this ageing population about the transnational nature of technology-enabled crime.

There is, therefore, a need for coordinated action by government agencies to ensure the most effective crime prevention advice is provided to the community. User education through dissemination of media releases by authoritative institutions, such as the Internet Crime Complaint Center, would enable users to maintain current knowledge of the latest scams and the best fraud prevention measures available.

Recommendation # 8

Establish Constructive and Regular Consultation with Government, Community, Industry and Interest Groups

Details of:
Recommendations for Joint Parliamentary Committee on Cybersafety (cont)

Recommendation # 8

Establish Constructive and Regular Consultation with Government, Community, Industry and Interest Groups

The National Child and Young Persons Human Rights Council to seek and maintain an active input from Government, Community, Industry and Interest Groups through linking with existing **Government, Community, Industry and Interest Groups**

8.1 Establish quality Training in Anti Bullying and Cyber Safety for:

- Government
- Community
- Industry
- Interest Groups

.

Comment

I strongly urge The National Child and Young Persons Human Rights Council follow the excellent advice of the Australian Institute of Criminology, Research and Public Policy Series No. 78 Report, by providing ongoing, quality Training for **Government, Community, Industry and Interest Groups**.

Appendix 16:

Extracts of the Report: are as follows:

Future directions in technology-enabled crime: 2007-09
Kim-Kwang Raymond Choo, Russell G Smith, Rob McCusker
Australian Institute of Criminology- Research and Public Policy Series No. 78

Training for information technology professionals *(page 98)*

IT professionals are becoming more actively involved in the investigation and prosecution of technology-enabled crimes. For example, IT professionals may be called upon to help facilitate compliance with legal obligations, developing and operating secure computer systems to ensure the privacy of protected information is not compromised. Training would equip IT professionals with a working knowledge of key legal challenges and issues they are likely to encounter in the course of professional activities.

Recommendation # 9

Establish a National Accredited Bullying & Cyberbullying Training Program for Teachers

Details of:
Recommendations for Joint Parliamentary Committee on Cybersafety (cont)

Recommendation # 9

Establish a National Accredited Bullying & Cyberbullying Training Program for Teachers

Provide the necessary resources to support **Schools** to minimise bullying and cyberbullying practices by providing **Teachers** with a **National Accredited Bullying & Cyberbullying Training Program** that is independently funded by the Australian Government and validated by the National Child and Young Persons Human Rights Council

9.1 Establish quality Training in Anti Bullying and Cyber Safety for:

- Teachers
- Parents and
- Young People

.

Comment

I strongly urge The National Child and Young Persons Human Rights Council follow the excellent advice of the Australian Institute of Criminology, Research and Public Policy Series No. 78 Report, by providing ongoing, quality Training for Teachers, Parents and Young People.

Appendix 16:

Extracts of the Report: are as follows:

Future directions in technology-enabled crime: 2007-09
Kim-Kwang Raymond Choo, Russell G Smith, Rob McCusker
Australian Institute of Criminology- Research and Public Policy Series No. 78

Training for information technology professionals *(page 98)*

IT professionals are becoming more actively involved in the investigation and prosecution of technology-enabled crimes. For example, IT professionals may be called upon to help facilitate compliance with legal obligations, developing and operating secure computer systems to ensure the privacy of protected information is not compromised. Training would equip IT professionals with a working knowledge of key legal challenges and issues they are likely to encounter in the course of professional activities.

Recommendation # 10

Establish a National Accredited Bullying & Cyberbullying Training Program for AFP & State Police

Details of:
Recommendations for Joint Parliamentary Committee on Cybersafety (cont)

Recommendation # 10

Establish a National Accredited Bullying & Cyberbullying Training Program for AFP & State Police

Provide the necessary resources to support Federal and State Police to minimise bullying and cyberbullying practices by providing Police Members with a **National Accredited Bullying & Cyberbullying Training Program** that is independently funded by the Australian Government and validated by the National Child and Young Persons Human Rights Council.

10.1 Establish quality Training in Anti Bullying and Cyber Safety for:

- Teachers
- Parents and
- Young People

.

Comment

I strongly urge The National Child and Young Persons Human Rights Council follow the excellent advice of the Australian Institute of Criminology, Research and Public Policy Series No. 78 Report, by providing ongoing, quality Training for Teachers, Parents and Young People.

Appendix 16:

Extracts of the Report: are as follows:

Future directions in technology-enabled crime: 2007-09
Kim-Kwang Raymond Choo, Russell G Smith, Rob McCusker
Australian Institute of Criminology- Research and Public Policy Series No. 78

The role of task forces *(page 97)*

Law enforcement agencies, particularly in ICT advanced countries, have recognised the increased interdependence of global markets and have responded to the general risks of technology-enabled crimes by establishing task forces dedicated to investigating technology-enabled crime cases. The task forces need to have adequately trained personnel capable of undertaking the operational demands of the comprehensive role envisaged by public policing agencies. The organisational capacity of law enforcement and other agencies within and across national borders to deal with increasingly complex technology-enabled crime will continue to be

Recommendation # 10 *(cont)*

Appendix 16 – Extract (cont)

constrained. The use of task forces to respond to particularly complex technology-enabled crimes will continue to be beneficial, although this may have the effect of reducing resources for investigating more mundane, low-value computer crimes. The need for task forces to be established quickly also creates difficulties for investigation of new types of technology-enabled crime, where immediate response is invariably needed. Standing investigatory units may, therefore, offer greater benefits than those units convened in response to a specific identified crime.

Training and educational needs *(page 97)*

Technological expertise, computer forensic capabilities, and sufficient investigative powers within government agencies are important. A focus on training a few experts no longer suffices: both generic and specialist training with common standards are now demanded. The need for training in technology-enabled crime legislation, particularly concerning evidence and procedure, will increase as countries enact new legislation to deal with emerging threats.

In fact, it was identified that:

> [i]ncreased funding for law enforcement, including training in cyber forensics, improved vehicles for international cooperation (like the efforts in the G-8 to create national points of contact for cybercrime), and effective national laws (modeled on the Council of Europe Cybercrime Treaty) will also help narrow the opportunities for cybercriminals (McAfee 2005: 17).

Such training should be targeted towards IT professionals, legal professionals and juries, computer forensics professionals and law enforcement officers, as well as end-users and the computer-using public.

Training for computer forensics professionals and law enforcement officers *(page 98)*

Developments in network vulnerabilities will require ongoing training in computer forensics. Although establishment of computer forensics accreditation programs (e.g. Certified Forensic Computer Examiner offered by the International Association of Computer Investigative Specialists) will ensure that standards of training are maintained, problems will arise in ensuring adequate staffing levels of accredited investigators. Use of private sector contractors will continue to be necessary, although risk management will be needed to ensure trained personnel do not misuse their skills for non-policing work. A recent example concerns a 'so-called' computer forensics expert hired to testify at two child pornography court cases in the United States who 'pleaded guilty to federal perjury charges for falsifying his resume and lying in open court, presumably about his credentials' (Goodin 2007b, US DoJ 2007a). The indictment alleged that '[a]t the time he worked on the child porn cases, he had already been qualified as an expert witness in computers and submitted court testimony in several jurisdictions, including federal court in California, and in courts in at least two California counties'.

Recommendation # 10 *(cont)*

Appendix 16 – Extract (cont)

Creation of resources, such as the 'Handbook of Legal Procedures of Computer and Network Misuse in European Union Countries', for police and legal practitioners will continue to be necessary. Australia is well placed to guide training in technology-enabled laws and procedures across the Asia–Pacific region, although any initiatives should be harmonised with activities in Europe and North America.

Increasingly, forensic analysis of computers for law enforcement purposes is being undertaken by well-organised groups of forensic examiners working in government facilities or private sector workplaces. Such groups include leading accounting firms such as KPMG, Deloitte, Ernst & Young and PricewaterhouseCoopers. An emerging issue is the desirability of accreditation both for individual examiners and for forensic laboratories, along with validation of forensic analysis tools. Over the next two years, developments will be needed to ensure that standards of forensic computing are being maintained nationally and internationally.

Technical assistance to less capable (or less ICT advanced) jurisdictions will also be essential as the widespread provision of training will allow the leading ICT advanced countries to manage if not prevent many of the cross-border problems (e.g. rendition of fugitives) now so evident in the delivery of phishing, denial-of-service attacks and other technology-enabled crime.

Recommendation # 11

Establish a National Accredited Bullying & Cyberbullying Training Program for Magistrate Court, DPP & Justice Staff

Details of:
Recommendations for Joint Parliamentary Committee on Cybersafety (cont)

Recommendation # 11

Establish a National Accredited Bullying & Cyberbullying Training Program for Magistrate Court, DPP & Justice Staff

Provide the necessary resources to support Magistrate Court Judges and DPP Staff to minimise bullying and cyberbullying practices by providing Judges and Prosecutors with a **National Accredited Bullying & Cyberbullying Training Program** that is independently funded by the Australian Government and validated by the National Child and Young Persons Human Rights Council.

11.1 Establish quality Training in Anti Bullying and Cyber Safety for:

- Magistrates
- Juries and
- Legal Professionals

.

Comment

I strongly urge The National Child and Young Persons Human Rights Council follow the excellent advice of the Australian Institute of Criminology, Research and Public Policy Series No. 78 Report, by providing ongoing, quality Training for Teachers, Parents and Young People.

Appendix 16:

Extracts of the Report: are as follows:

Future directions in technology-enabled crime: 2007-09
Kim-Kwang Raymond Choo, Russell G Smith, Rob McCusker
Australian Institute of Criminology- Research and Public Policy Series No. 78

Training for legal professionals and juries *(page 98)*

Training targeted towards lawyers, prosecutors, judges and juries involved in technology-enabled crime cases, will help them understand technical terminologies crucial to the case. Such terminology would include spyware, adware, encryption, slack space, file allocation table and date/time stamps.

Recommendation # 5 *(cont)*

Appendix 16 – Extract (cont)

> Crime involving technology is now part of everyday policing and has an effect on all types of crime. A comprehensive training program that reaches the widest audience is therefore essential … Any crime scene could be an electronic crime scene and the correct handling of this type of evidence can positively affect an investigation. However, detections, disruptions, prosecutions and crime reduction/prevention can only be achieved with properly trained personnel who are appropriately equipped to investigate the various aspects of computer-enabled criminality that they encounter in their daily duties (Jones 2005).

Recommendation # 12

Update the National Child Protection Policy to include Mandatory Reporting of Child Abuse from Bullying and Cyberbullying Incidents

Details of:
Recommendations for Joint Parliamentary Committee on Cybersafety (cont)

Recommendation # 12

Update the National Child Protection Policy to include Mandatory Reporting of Child Abuse from Bullying and Cyberbullying Incidents

Provide the necessary resources to support a Training Program for a National Child Protection Policy to include Mandatory Reporting of Child Abuse from Bullying and Cyberbullying Incidents, to minimise bullying and cyberbullying practices. This Training Program is independently funded by the Australian Government and validated by the National Child and Young Persons Human Rights Council.

Comment

Bullying victims will suffer Physical Abuse and Emotional Abuse while Cyberbullying victims only suffer Emotional Abuse. However, it has been reported that this type of Emotional Abuse is far more debilitating than that experienced in Physical face to face Bullying. Unfortunately, both victims suffer Emotional Abuse from serious incidents of Bullying and Cyberbullying and it can be argued, successfully in my opinion, the subject of a Mandatory Report?

Note: While the following extract talks about the interaction of Parents and Care Givers this group can be easily substituted for a Bully or Cyberbully Offender.

Appendix 17

Extract: DHS – ACT: Keeping Children & Young People Safe, January 2009

Emotional Abuse

Emotional abuse is the term used to describe chronic and repetitive ill treatment of a child or young person which causes significant harm to their psychological, social, emotional or cognitive development.

Constant yelling, belittling, ignoring and ridiculing are all examples of emotional abuse.

Emotional abuse also refers to situations where children or young people are exposed to domestic violence by seeing or hearing the physical, sexual or psychological abuse between parents or caregivers; or where they are put at risk of exposure to domestic violence that would cause significant harm to their wellbeing and development.

As with other forms of abuse, all children and young people respond differently, however generally speaking, the more severe and ongoing the abuse, the greater the likelihood that it will negatively impact upon the child or young person's wellbeing and development.

Recommendation # 12 *(cont)*

Appendix 17 – Extract (cont)

It is particularly important to consider the indicators in parents and caregivers when identifying emotional abuse as there are many reasons why children or young people may be emotionally troubled. In situations where there is no emotional abuse, parents usually show concern about their child or young person and seek help

.

The following may be indicators of emotional abuse. One indicator in isolation may not imply emotional abuse.

The following list is not in hierarchical order

Indicators in children and young people [Victim of Bullying & Cyberbullying]	***Indicators in parents and care givers [Offender of Bullying & Cyberbullying]***
• *Over compliant, withdrawn, passive and/or tearful* • *Displaying age-inappropriate behaviours, e.g. overly adult (parenting other children) or overly infantile (thumb sucking, rocking, wetting or soiling)* • *Lack expectations and trust in people* • *Fearful of parent(s) and caregiver(s)* • *Indiscriminate attachment* • *Disruptive or aggressive behaviour towards others* • *Hypervigilance, particularly in pre-school Children* • *Exhibiting extreme attention seeking or risk taking behaviour* • *Withdrawn or seen as a 'loner' – difficulty relating to others* • *Highly anxious* • *Developmental delay*	• *Excessive or unreasonable demands* • *Unrealistic expectations of the child or young person* • *Persistent hostility and severe verbal abuse* • *Rejection, ridiculing and scapegoating* • *Exposure to domestic violence* • *Constant criticism, belittling, teasing and withholding of affection and praise* • *Belief that a particular child or young person is intrinsically 'bad', 'naughty' or 'evil'* • *Using inappropriate social or physical Isolation as punishment*

Recommendation # 12 *(cont)*

Appendix 17 – Extract (cont)

2 Guiding principles

2.1 Protecting children is everyone's business

Under the National Framework for Protecting Australia's Children (2009), protecting children is everyone's responsibility: parents, communities, governments and business all have a role to play. The National Framework represents an unprecedented level of collaboration between Australian State and Territory governments and non-government organisations to protect children. The National Framework provides the foundation for improving the safety and wellbeing of vulnerable children1.

Child Protection policy is based on the principle of partnership and shared responsibility across a broad range of human service professionals, including schools and licensed children's services. Most children are best protected and cared for within their own family; however, when parents, carers or guardians are unwilling or unable to protect their children from significant harm, the protection of the child becomes the responsibility of the wider community and, at times, requires statutory Child Protection intervention.

Licensed children's services and Victorian schools play an important role in the prevention of child abuse and neglect through their access to information about family functioning and the needs of children. When a school or licensed children's service staff member forms a belief that a child has been harmed or is at risk of being harmed, they must take action that is timely, respectful and co-ordinate.

2.2 Best interests principles

The 'every child every chance' reforms are underpinned by principles that promote the right of every child to live a full and productive life in an environment that builds confidence, friendships, security and happiness irrespective of their family circumstances or background.
The Children, Youth and Families Act 2005 is a key building block to support the reform strategy to promote children's safety, wellbeing and development.

The CYFA has a unifying set of 'best interests principles' that require family services, Child Protection and placement services to protect children from harm, protect their rights and promote their development in gender, age and culturally appropriate ways.

Recommendation # 12 *(cont)*

Appendix 17 – Extract (cont)

For the purposes of this protocol, acting in the best interests of the child includes:

- *reporting to Child Protection all allegations or disclosures of physical abuse, sexual abuse, emotional abuse and neglect*
- *reporting to Child Protection when a belief is formed that a child has been harmed or is at risk of being harmed*
- *making the child's ongoing safety and wellbeing the primary focus of decision-making*
- *sharing appropriate information, expertise and resources with other service providers supporting the child*
- *protecting and promoting the cultural and spiritual identity of a child and maintaining their connection to their family or community of origin*
- *enabling the child and the child's family to access appropriate services in order to reduce the long-term effects of abuse or neglect.*

2.3 Collaborative practice

Collaborative work between Child Protection, licensed children's services and Victorian schools an improve outcomes for children, young people and their families. Effective collaboration on the creation of a working relationship based on principles of trust, respect and shared decision making contributes to ensuring the safety and wellbeing of all children and young people by protecting them from significant harm.

2.4 Duty of care

Staff or volunteers working for Child Protection, licensed children's services and Victorian schools have a duty of care to support and protect the children and young people with whom they are professionally involved. When staff members form a reasonable belief that a child or young person has been harmed or is at risk of harm, they are ethically bound to take action to protect the safety and wellbeing of that child or young person. For some staff members this obligation is legally mandated (Refer to Section 4.1).

Recommendation # 12 *(cont)*

Appendix 17 – Extract (cont)

Duty of care is breached if a person:

- *does something that a reasonable person in that person's position would not do in a particular situation,*
- *fails to do something that a reasonable person in that person's position would do in the circumstances,*
- *acts or fails to act in a way that causes harm to someone to whom the person owes a duty of care.*

2.5 Culturally appropriate responses

2.5.1 Aboriginal children

The CYFA specifies decision-making principles for Aboriginal children and young people. Child Protection must consult with an Aboriginal organisation such as the Victorian Aboriginal Child Care Agency (VACCA) when a report regarding an Aboriginal child is received. This is in recognition of the principle of Aboriginal self-management and self-determination.
http://www.vacca.org/home/home

2.5.2 Children from culturally and linguistically diverse (CALD) backgrounds

Culturally respectful approaches and considerations are to be adopted when working with children, young people and families from CALD backgrounds. Cultural differences in child-rearing practices are to be acknowledged and sensitively considered within the relevant cultural context, but should not compromise the child's safety and wellbeing.

2.5.3 Children with refugee backgrounds

Children and families with refugee backgrounds commonly share experiences of trauma, dislocation and loss. Pre-migration experiences coupled with settlement challenges can significantly affect family wellbeing and parenting capacity. While these issues require sensitive consideration, they should not compromise the child's safety and wellbeing.

Recommendation # 12 *(cont)*

Appendix 17 – Extract (cont)

2.5.4 Children with disabilities

The protocol between Child Protection and Disability Services endeavours to promote a best practice approach to children with a disability and their families. While these issues require sensitive consideration, they should not compromise the child's safety and wellbeing.

3.4 Victorian schools

It is the role of Victorian schools under the Education and Training Reform Regulations 2007 to provide school education in Victoria that adheres to the minimum standards detailed in the regulations.

Schools have an important role to play in supporting children and their families and in protecting students who may be at risk of harm due to abuse or neglect. Education staff in close daily contact with students are well placed to observe when a child or young person appears to be at risk of harm.

Under the CYFA, primary and secondary school teachers and principals are prescribed as mandatory reporters. They must make a report to Child Protection if they believe, on reasonable grounds, that a child or a young person is in need of protection. (Refer to Section 4.1).

The role of schools concerning the general welfare of students is outlined in a range of school policies and procedures. This protocol is intended to complement other policies and procedures that already exist in government and non-government schools.

Note: Appendix 18

Extract: DHS – ACT: Keeping Children & Young People Safe, January 2009

A joint protocol of the Department of Human Services Child Protection,
Department of Education and Early Childhood Development,
Licensed Children's Services and Victorian Schools

Published by the Department of Education and Early Childhood Development and
Department of Human Services – Melbourne - Published May 2010

http://www.eduweb.vic.gov.au/edulibrary/public/stuman/wellbeing/Protecting_Children_Protocol_Sep_2010.pdf

Additional Reference Information

Reference 06

Bullying and Cyber-Bullying - *Definitions:*

(Expansion of the National Safe Schools Guidelines, Wikipedia & Cyber Safety)

1. ***Conflict:***
   A disagreement, where the needs of one or both parties are not being met. It does not necessarily involve an abuse of power, even if parties do not have perceived equal power. If handled well, conflict is seen as an opportunity for personal growth.

2. ***Harassment:***
   Negative behaviour intended to annoy or trouble another individual, which may be based on obvious differences such as gender, race, religious or cultural beliefs, physical difference, sexual orientation, ability or disability and socio-economic status. It may be a one-off incident between individuals or groups or may continue over time.

3. **Exclusion:**
   Exclusion is the process of designating who is a member of the "in-group" and who is an "outcast." In some cases, this is done by who has a mobile phone and who has not. Students, particularly girls, will also omit certain other girls from e-mail lists, chat room conversations and so on.

4. **Flaming:**
   Flaming is a heated argument, frequently including offensive or vulgar language, that occur in public communication environments, such as discussion boards or groups, chat, or newsgroups. A Flame may have elements of a normal message, but is distinguished by its intent. A flame is typically not intended to be constructive, to further clarify a discussion, or to persuade other people. The motive for flaming is often not dialectic, but rather social or psychological. Sometimes, flamers are attempting to assert their authority, or establish a position of superiority. Occasionally, flamers wish to upset and offend other members of the forum, in which case they are "trolls." Most often however, flames are angry or insulting messages transmitted by people who have strong feelings about a subject. Finally, some consider flaming to be a great way to let off steam, though the receiving party may be less than pleased.

5. **Outing:**
   this includes the public display, posting, or forwarding of personal communication or images, especially communication that contains sensitive personal information or images that are sexual in nature. Increasingly, images taken using mobile phone cameras and mobile phone text messages are used as part of outing bullying. Reading the saved text messages on other's phones can also be part of the outing process;

Reference 06 *(cont)*

Bullying and Cyber-Bullying - ***Definitions:*** (cont)

6. ***"Sexting":***
   A slay term, combining the words, "sex" and "texting."
   When a person takes a sexually-explicit digital photograph of him or herself or of someone else, and sends it as an MMS and SMS via a mobile phone. These images can then be posted on the internet or forwarded electronically to other people. Once posted on the internet these images can leave a permanent digital footprint and be accessed at any time in the future. It is illegal to take sexual photos or videos of children and young people. It can also refer to text messages of a sexually-charged nature.

7. **Voting/Polling Booths**: Some Web sites offer users the opportunity to create online polling/voting booths, many at no cost. Cyberbullies can use these Web sites to create web pages that allow others to vote online for "The Ugliest , Fattest, Dumbest etc. Boy/Girl at their respective schools.

8. **Impersonation**: in other cases, students may impersonate other students and make unpopular online comments, even set up websites that include hate leading to the impersonated student being ostracized or further bullied in more traditional ways.

9. ***Bullying:***
   A product of social dynamics which can be defined as the repeated negative actions by individuals or groups against a target individual or group, which involves an imbalance of power. Bullying can take different forms – physical, social, or psychological. Actions can be observable (overt) or hidden (covert).

10. ***Cyberbullying:***
    A product of social dynamics which can be defined as the repeated negative comments by individuals or groups against a target individual or group, which involves an imbalance of power. Cyberbullying can take different forms – verbal, social, cyber or psychological. Comments can be observable (overt) or hidden (covert).

Reference 06 *(cont)*

Bullying and Cyber-Bullying - ***Definitions:*** (cont)

11. **Cyberstalking**: includes threats of harm, intimidation and/or offensive comments which are sent through personal communication channels. Frequently with cyberstalking there is a threat, or at least a belief, that the virtual could become real stalking.

12. ***Assault:***
    An intended Physical Assault on an Individual or Group, by another Individual or Group. It could be physically baiting, humiliating or provoking an individuals or group to physically retaliate providing a public opportunity to exploit a power imbalance and or to deliberately provide a opportunity to cause pain and suffering to another less powerful or outnumbered individual or group. It may be a one-off incident between individuals or groups or may continue over time.

13. ***Attack:***
    An intended Social Attack on an Individual or Group, by another Individual or Group.
    It could be posting comments on Mobile Phone, Web Sites & Social Web Pages
    It could be posting or distributing personal images un-altered or altered, it could be "Happy Slapping Events, considered to be child abuse or child pornographic video material. It may be a one-off incident between individuals or groups or may continue over time

14. ***Violence:***
    Incidents where a person or group is intimidated, abused, threatened, physically assaulted or where property is deliberately damaged by another person or group. It is an extreme use of force often resulting in injury or destruction. Violence does not necessarily involve an imbalance of power.

15. **"Happy slapping":**
    A fad starting in 2004, in which someone deliberately assaults an unwitting victim, while others record the assault, commonly with a camera phone or a Smartphone. Though the name usually refers to relatively minor acts of violence such as hitting or slapping the victim, more serious crimes such as murder, rape, and sexual assault have been classified as "happy slapping" by the media.

Reference 07

GuardingKids.com
A Practical Guide to Keeping Kids Out of High-Tech Trouble

Cyberbullying - By Russell A. Sabella, Ph.D.

GuardingKids.com
http://www.education.com/reference/article/cyberbullying-internet-online-safety/

Cyberbullying

Cyberbullying involves the use of information and communication technologies such as e-mail, cell phone, text messaging, instant messaging, defamatory personal Web sites, and defamatory online personal polling Web sites, to support deliberate, repeated, and hostile behavior by an individual or group, that is intended to harm others." It seems to be even worse than live bullying because the perpetrators are not bound my time or space, and the audience can be much, much bigger. With the power of technology, the offenses can be much more cruel as they can incorporate a rich array of media (sounds, altered graphics, text, video, slide shows, and photos) to deliver the attacks. Consider the following real situations among cyberbullying victims as reported in one national newspaper:

- When Joanne had a row with a longtime friend last year, she had no idea it would spill into cyberspace. But what started as a spat at a teenage sleep over swiftly escalated into a three-month harangue of threatening e-mails and defacement of her weblog. "It was a non-stop nightmare," says Joanne, 14, a freshman at a private high school in Southern California. "I dreaded going on my computer."

- Ashlee, a former elementary school teacher in Birmingham, Ala., says she was "sickened" by the manner girls manipulated one another with instant messages. "I grew to hate that," she said.

- "If I find you, I will beat you up," one message read. Frightened, Michael blocked their IM addresses but didn't tell his parents for two weeks. "It scared me," he recalls. "It was the first time I was bullied."

- At one Elementary School in Fairfax, Va. last year, sixth-grade students conducted an online poll to determine the ugliest classmate, school officials say.

- Cyberbullying is so pervasive in one New York county that officials held a half-day conference last month for students, parents, teachers and law-enforcement officials. Six hundred attended.

- "The person was pretending it was me, and using it to call people names," the 14-year-old Seattle student said. "I never found out who it was."

In a startling case that occurred in June 2003 a twelve-year-old Japanese girl killed her classmate because she was angry about messages that had been posted about her on the Internet. In another example, Canadian teenager David Knight's life became hell when a group of his school mates established a "Hate David Knight" website and posted denigrating pictures and abuse and invited the global community to join in the hate campaign. In another case right her in Florida, a boy named Jeffrey was the target of relentless bullying. The perpetrators used

***Reference 07** (cont)*

Cyberbullying - By Russell A. Sabella, Ph.D. (cont)

the computer to launch attacks at Jeff and even destroyed a video game he and his friend worked on all summer. After two years of this persistent bullying and harassment, Jeff committed suicide by hanging. These are only a few examples of this significant and growing problem among children (Studies about the frequency of cyberbullying suggest that cyberbullying is affecting a significant minority of school-age children, with nearly 25 to 35 percent of respondents claiming to have been bullied in chat rooms, e-mail, and via text messages.)

Researchers across various disciplines have collected a rich array of anecdotal examples for how high-tech bullying takes place which highlights the complexity of the problem. Here is how kids bully each other in a high-tech world.

- **Exclusion**: Exclusion is the process of designating who is a member of the "in-group" and who is an "outcast." In some cases, this is done by who has a mobile phone and who has not. Students, particularly girls, will also omit certain other girls from e-mail lists, chat room conversations and so on.

- **Flaming**: Flaming is a heated argument, frequently including offensive or vulgar language, that occur in public communication environments, such as discussion boards or groups, chat, or newsgroups. Flamers may use capitol letters and a range of visual images and symbols to add emotional intensity and anger to their messages. According to the Wikipedia (see http://en.wikipedia.org/wiki/Flame_war), a flame may have elements of a normal message, but is distinguished by its intent. A flame is typically not intended to be constructive, to further clarify a discussion, or to persuade other people. The motive for flaming is often not dialectic, but rather social or psychological. Sometimes, flamers are attempting to assert their authority, or establish a position of superiority. Occasionally, flamers wish to upset and offend other members of the forum, in which case they are "trolls." Most often however, flames are angry or insulting messages transmitted by people who have strong feelings about a subject. Occasionally a flame can also be used as a zenslap (see http://en.wikipedia.org/wiki/Zenslap). Finally, some consider flaming to be a great way to let off steam, though the receiving party may be less than pleased.

- **Outing**: this includes the public display, posting, or forwarding of personal communication or images, especially communication that contains sensitive personal information or images that are sexual in nature. Increasingly, images taken using mobile phone cameras and mobile phone text messages are used as part of outing bullying. Reading the saved text messages on other's phones can also be part of the outing process;

- **Cyberstalking**: includes threats of harm, intimidation and/or offensive comments which are sent through personal communication channels. Frequently with cyberstalking there is a threat, or at least a belief, that the virtual could become real stalking.

- **E-mail**: One student sends a threatening e-mail to another, then forwards it to additional people.

Reference 07 *(cont)*

Cyberbullying - By Russell A. Sabella, Ph.D. (cont)

- **Harassment**: Sending hurtful messages to someone in a severe, persistent, or pervasive manner.

- **Instant Messaging (IM)**: several students log on to an IM platform (e.g., America Online's Instant Messenger) and simultaneously "slam" another.

- **Websites**: bullies set up derogatory Web sites dedicated to one or more victims.

- **Impersonation**: in other cases, students may impersonate other students and make unpopular online comments, even set up websites that include hate leading to the impersonated student being ostracized or further bullied in more traditional ways.

- **Voting/Polling Booths**: Some Web sites offer users the opportunity to create online polling/voting booths, many at no cost. Cyberbullies can use these Web sites to create web pages that allow others to vote online for "The Ugliest , Fattest, Dumbest etc. Boy/Girl at their respective schools.

Children seem to view the real world and the online or virtual world as part of a seamless continuum. Conversations with friends may begin at school and pick up again, on a child's computer, after dinner, or vice versa. Unfortunately, this is also true of bullying behaviors. What begins as a flame war in an Instant Messaging conversation can carry over to the lunch room the next day and include many of the same group members witnessing the electronic conversation the night before.

Reference 08

www.stopcyberbullying.org

Why do kids cyberbully each other?

Who knows why kids do anything? When it comes to cyberbullying, they are often motivated by anger, revenge or frustration. Sometimes they do it for entertainment or because they are bored and have too much time on their hands and too many tech toys available to them. Many do it for laughs or to get a reaction. Some do it by accident, and either send a message to the wrong recipient or didn't think before they did something. The Power-hungry do it to torment others and for their ego. Revenge of the Nerd may start out defending themselves from traditional bullying only to find that they enjoy being the tough guy or gal. Mean girls do it to help bolster or remind people of their own social standing. And some think they are righting wrong and standing up for others.

Because their motives differ, the solutions and responses to each type of cyberbullying incident has to differ too. Unfortunately, there is no "one size fits all" when cyberbullying is concerned. Only two of the types of Cyberbullies have something in common with the traditional schoolyard bully. Experts who understand schoolyard bullying often misunderstand cyberbullying, thinking it is just another method of bullying. But the motives and the nature of cyber communications, as well as the demographic and profile of a cyberbully differ from their offline counterpart.

Reference 09

www.stopcyberbullying.org (cont)

What is cyberbullying, exactly?

"Cyberbullying" is when a child, preteen or teen is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another child, preteen or teen using the Internet, interactive and digital technologies or mobile phones. It has to have a minor on both sides, or at least have been instigated by a minor against another minor. Once adults become involved, it is plain and simple cyber harassment or cyberstalking. Adult cyber-harassment or cyberstalking is NEVER called cyberbullying.

It isn't when adult are trying to lure children into offline meetings, that is called sexual exploitation or luring by a sexual predator. But sometimes when a minor starts a cyberbullying campaign it involves sexual predators who are intrigued by the sexual harassment or even ads posted by the cyberbullying offering up the victim for sex.

The methods used are limited only by the child's imagination and access to technology. And the cyberbully one moment may become the victim the next. The kids often change roles, going from victim to bully and back again.

Children have killed each other and committed suicide after having been involved in a cyberbullying incident.

Cyberbullying is usually not a one time communication, unless it involves a death threat or a credible threat of serious bodily harm. Kids usually know it when they see it, while parents may be more worried about the lewd language used by the kids than the hurtful effect of rude and embarrassing posts.

Cyberbullying may arise to the level of a misdemeanor cyber harassment charge, or if the child is young enough may result in the charge of juvenile delinquency. Most of the time the cyberbullying does not go that far, although parents often try and pursue criminal charges. It typically can result in a child losing their ISP or IM accounts as a terms of service violation. And in some cases, if hacking or password and identity theft is involved, can be a serious criminal matter under state and federal law.

When schools try and get involved by disciplining the student for cyberbullying actions that took place off-campus and outside of school hours, they are often sued for exceeding their authority and violating the student's free speech right. They also, often lose. Schools can be very effective brokers in working with the parents to stop and remedy cyberbullying situations. They can also educate the students on cyber ethics and the law. If schools are creative, they can sometimes avoid the claim that their actions exceeded their legal authority for off-campus cyberbullying actions. We recommend that a provision is added to the school's acceptable use policy reserving the right to discipline the student for actions taken off-campus if they are intended to have an effect on a student or they adversely affect the safety and well-being of student while in school. This makes it a contractual, not a constitutional

Reference 09 *(cont)*

www.stopcyberbullying.org (cont)

Direct Attacks

1. Instant Messaging/Text Messaging Harassment
2. Stealing Passwords
3. Blogs
4. Web Sites
5. Sending Pictures through E-mail and Cell Phones
6. Internet Polling
7. Interactive Gaming
8. Sending Malicious Code
9. Sending Porn and Other Junk E-Mail and IMs
10. Impersonation

1. Instant Messaging/Text Messaging Harassment

a) Kids may send hateful or threatening messages to other kids, without realizing that while not said in real life, unkind or threatening messages are hurtful and very serious.

b) Warning wars - Many Internet Service Providers offer a way of "telling on" a user who is saying inappropriate things. Kids often engage in "warning wars" which can lead to kicking someone offline for a period of time. While this should be a security tool, kids sometimes use the Warn button as a game or prank.

c) A kid/teen may create a screen name that is very similar to another kid's name. The name may have an additional "i" or one less "e". They may use this name to say inappropriate things to other users while posing as the other person.

d) Text wars or text attacks are when kids gang up on the victim, sending thousands of text-messages to the victims cell phone or other mobile device. The victim is then faced with a huge cell phone bill and angry parents.

e) Kids send death threats using IM and text-messaging as well as photos/videos (see below)

2. Stealing passwords

a) A kid may steal another child's password and begin to chat with other people, pretending to be the other kid. He/she may say mean things that offend and anger this person's friends or even strangers. Meanwhile, they won't know it is not really that person they are talking to.

b) A kid may also use another kid's password to change his/her profile to include sexual, racist, and inappropriate things that may attract unwanted attention or offend people.

c) A kid often steals the password and locks the victim out of their own account.

d) Once the password is stolen, hackers may use it to hack into the victim's computer.

Reference 09 *(cont)*

www.stopcyberbullying.org (cont)

3. Blogs

Blogs are online journals. They are a fun way for kids and teens to messages for all of their friends to see. However, kids sometimes use these blogs to damage other kids' reputations or invade their privacy. For example, in one case, a boy posted a bunch of blogs about his breakup with his ex-girlfriend, explaining how she destroyed his life, calling her degrading names. Their mutual friends read about this and criticized her. She was embarrassed and hurt all because another kid posted mean, private, and false information about her. Sometimes kids set up a blog or profile page pretending to be their victim and saying things designed to humiliate them.

4. Web sites

a) Children used to tease each other in the playground; now they do it on Web sites. Kids sometimes create Web sites that may insult or endanger another child. They create pages specifically designed to insult another kid or group of people.

b) Kids also post other kids' personal information and pictures, which put those people at a greater risk of being contacted or found.

5. Sending Pictures through E-mail and Cell Phones

a) There have been cases of teens sending mass e-mails to other users, that include nude or degrading pictures of other teens. Once an e-mail like this is sent, it is passed around to hundreds of other people within hours; there is no way of controlling where it goes.

b) Many of the newer cell phones allow kids to send pictures to each other. The kids receive the pictures directly on their phones, and may send it to everyone in their address books. After viewing the picture at a Web site, some kids have actually posted these often pornographic pictures on Kazaa and other programs for anyone to download.

c) Kids often take a picture of someone in a locker room, bathroom or dressing room and post it online or send it to others on cell phones.

6. Internet Polling

Who's Hot? Who's Not? Who is the biggest slut in the sixth grade? These types of questions run rampant on the Internet polls, all created by yours truly - kids and teens. Such questions are often very offensive to others and are yet another way that kids can "bully" other kids online.

Reference 09 *(cont)*

www.stopcyberbullying.org (cont)

7. Interactive Gaming

Many kids today are playing interactive games on gaming devices such as X-Box Live and Sony Play Station 2 Network. These gaming devices allow your child to communicate by chat and live Internet phone with anyone they find themselves matched with in a game online. Sometimes the kids verbally abuse the other kids, using threats and lewd language. Sometimes they take it further, by locking them out of games, passing false rumors about them or hacking into their accounts.

8. Sending Malicious Code

Many kids will send viruses, spyware and hacking programs to their victims. They do this to either destroy their computers or spy on their victim. Trojan Horse programs allow the cyberbully to control their victim's computer remote control, and can be used to erase the hard drive of the victim.

9. Sending Porn and Other Junk E-Mail and IMs

Often Cyberbullies will sign their victims up for e-mailing and IM marketing lists, lots of them, especially to porn sites. When the victim receives thousands of e-mails from pornographers their parents usually get involved, either blaming them (assuming they have been visiting porn sites) or making them change their e-mail or IM address.

10. Impersonation

Posing as the victim, the cyberbully can do considerable damage. They may post a provocative message in a hate group's chat room posing as the victim, inviting an attack against the victim, often giving the name, address and telephone number of the victim to make the hate group's job easier. They often also send a message to someone posing as the victim, saying hateful or threatening things while masquerading as the victim. They may also alter a message really from the victim, making it appear that they have said nasty things or shared secrets with others.

Reference 10

www.stopcyberbullying.org (cont)

Cyberbullying by proxy

Cyberbullying by proxy is when a cyberbully gets someone else to do their dirty work. Most of the time they are unwitting accomplices and don't know that they are being used by the cyberbully. Cyberbullying by proxy is the most dangerous kind of cyberbullying because it often gets adults involve in the harassment and people who don't know they are dealing with a kid or someone they know.

"Warning" or "Notify Wars" are an example of cyberbullying by proxy. Kids click on the warning or notify buttons on their IM screen or e-mail or chat screens, and alert the ISP or service provider that the victim has done something that violates their rules. If the victim receives enough warnings or notifications, they can lose their account. The service providers are aware of this abuse, and often check and see if the warning were justified. But all the cyberbully has to do is make the victim angry enough to say something rude or hateful back. Then, BINGO! they warn them, making it look like the victim had started it. In this case, the ISP or service provider is the innocent accomplice of the cyberbully.

Sometimes the victim's own parents are too. If the cyberbully can make it look like the victim is doing something wrong, and the parents are notified, the parents will punish the victim. Alyssa, one of our Teenangels, had this happen to her. To learn more about her cyberbullying problem, read Alyssa's story.

Cyberbullying by proxy sometimes starts with the cyberbully posing as the victim. They may have hacked into their account or stolen their password. They may have set up a new account pretending to be the victim. But however they do it, they are pretending to be the victim and trying to create problems for the victim with the help of others.

The most typical way a cyberbullying by proxy attack occurs is when the cyberbully gets control of the victim's account and sends out hateful or rude messages to everyone on their buddy list pretending to be the victim. They may also change the victim's password so they can't get into their own account. The victim's friends get angry with the victim, thinking they had sent the messages without knowing they have been used by the cyberbully. But it's not always this minor. Sometimes the cyberbully tries to get more people involved.

For example...Mary wants to get Jennifer back for not inviting her to her party. She goes online and, posing as Jennifer, posts "I hate Brittany, she is so stupid, ugly and fat!" on buddyprofile.com. Mary may tell Brittany and her friends that she read the post on buddyprofile.com and blames Jennifer for being mean. Brittany and her friends now start attacking Jennifer, and may report her to buddyprofile.com or her school. They are doing Mary's dirty work for her. Mary looks like the "good guy" and Jennifer may be punished by her parents, lose her account with buddyprofile.com and get into trouble at school. And Brittany and her friends may start to cyberbully Jennifer too.

Reference 10 *(cont)*

www.stopcyberbullying.org (cont)

Cyberbullying by proxy (cont)

Sometimes it is much more serious than that. When Cyberbullies want to get others to do their dirty work quickly, they often post information about, or pose as, their victim in hate group chat rooms and on their discussion boards. Cyberbullies have even posted this information in child molester chat rooms and discussion boards, advertising their victim for sex. They then sit back and wait for the members of that hate group or child molester group to attack or contact the victim online and, sometimes, offline.

For this to work, the cyberbully needs to post offline or online contact information about the victim. Real information, not the account they used to impersonate the victim (if they are posing as the victim to provoke an attack). For example...Jack is angry that Blake was chose as captain of the junior varsity basketball team. Blake is black. Jack finds a white supremist group online and posts in their chat room that Blake said nasty things about whites and their group in particular. He then posts Blake's cell phone number and screen name. People from the group start calling and IMing Blake with threats and hateful messages. Jack has no idea how much danger he has placed Blake in, and Blake doesn't know why he in under attack. In cases of cyberbullying by proxy, when hate or child molester groups are involved, they victim is in danger of physical harm and law enforcement must be contacted immediately.

Reference 11

www.stopcyberbullying.org (cont)

What methods work with the different kinds of Cyberbullies?

The four types of Cyberbullies include:

- The Vengeful Angel
- The Power-Hungry or Revenge of the Nerds
- The "Mean Girls"
- The Inadvertent Cyberbully or "Because I Can"

Some methods of cyberbullying are unique to a certain kinds of Cyberbullies. And so are the ways the cyberbully maintain their secrecy or broadcast their actions to others. Some are secretive, some require an audience and some are entirely inadvertent.

Because the motives differ from each type of cyberbully, the solutions need to address their special issues. There is no "one size fits all" when cyberbullying is concerned. But understanding more about why they cyberbully others will help. You have to address the motives. That's why awareness campaigns need several different messages to address the problem.

"The Vengeful Angel": In this type of cyberbullying, the cyberbully doesn't see themselves as a bully at all. They see themselves as righting wrongs, or protecting themselves or others from the "bad guy" they are now victimizing. This includes situations when the victim of cyberbullying or offline bullying retaliates and becomes a cyberbully themselves They may be angry at something the victim did and feel they are taking warranted revenge or teaching the other a lesson. The "Vengeful Angel" cyberbully often gets involved trying to protect a friend who is being bullied or cyberbullied. They generally work alone, but may share their activities and motives with their close friends and others they perceive as being victimized by the person they are cyberbullying.

Vengeful Angels need to know that no one should try and take justice into their own hands. They need to understand that few things are clear enough to understand, and that fighting bullying with more bullying only makes things worse. They need to see themselves as bullies, not the do-gooder they think they are. It also helps to address the reasons they lashed out in the first place. If they sense injustices, maybe there really are injustices. Instead of just blaming the Vengeful Angel, solutions here also require that the situation be reviewed to see what can be done to address the underlying problem. Is there a place to report bullying or cyberbullying? Can that be done anonymously? Is there a peer counseling group that handles these matters? What about parents and school administrators. Do they ignore bullying when it occurs, or do they take it seriously? The more methods we can give these kinds of Cyberbullies to use official channels to right wrongs, the less often they will try to take justice into their own hands.

Reference 11 *(cont)*

www.stopcyberbullying.org (cont)

The "Power-Hungry" and "Revenge of the Nerds": Just as their schoolyard counterparts, some Cyberbullies want to exert their authority, show that they are powerful enough to make others do what they want and some want to control others with fear. Sometimes the kids want to hurt another kid. Sometimes they just don't like the other kid. These are no different than the offline tough schoolyard bullies, except for their method. Power-Hungry" Cyberbullies usually need an audience. It may be a small audience of their friends or those within their circle at school. Often the power they feel when only cyberbullying someone is not enough to feed their need to be seen as powerful and intimidating. They often brag about their actions. They want a reaction, and without one may escalate their activities to get one.

Interestingly enough, though, the "Power-Hungry" cyberbully is often the victim of typical offline bullying. They may be female, or physically smaller, the ones picked on for not being popular enough, or cool enough. They may have greater technical skills. Some people call this the "Revenge of the Nerds" cyberbullying. It is their intention to frighten or embarrass their victims. And they are empowered by the anonymity of the Internet and digital communications and the fact that they never have to confront their victim. They may act tough online, but are not tough in real life. They are often not a bullying but "just playing one on TV."

Revenge of the Nerds Cyberbullies usually target their victims one-on-one and the cyberbully often keeps their activities secret from their friends. If they share their actions, they are doing it only with others they feel would be sympathetic. The rarely appreciate the seriousness of their actions. They also often resort to cyberbullying-by-proxy. Because of this and their tech skills, they can be the most dangerous of all Cyberbullies.

"Mean Girls": The last type of cyberbullying occurs when the cyberbully is bored or looking for entertainment. It is largely ego-based and the most immature of all cyberbullying types. Typically, in the "Mean Girls" bullying situations, the Cyberbullies are female. They may be bullying other girls (most frequently) or boys (less frequently).

"Mean Girls" cyberbullying is usually done, or at least planned, in a group, either virtually or together in one room. This kind of cyberbullying is done for entertainment. It may occur from a school library or a slumber party, or from the family room of someone after school. This kind of cyberbullying requires an audience. The Cyberbullies in a "mean girls" situation want others to know who they are and that they have the power to cyberbully others. This kind of cyberbullying grows when fed by group admiration, cliques or by the silence of others who stand by and let it happen. It quickly dies if they don't get the entertainment value they are seeking.

Reference 11 *(cont)*

www.stopcyberbullying.org (cont)

What methods work with the different kinds of Cyberbullies? (cont)

The Inadvertent Cyberbullying: Inadvertent Cyberbullies usually don't think they are Cyberbullies at all. They may be pretending to be tough online, or role playing, or they may be reacting to hateful or provocative messages they have received. Unlike the Revenge of the Nerds Cyberbullies, they don't lash out intentionally. They just respond without thinking about the consequences of their actions.

They may feel hurt, or angry because of a communication sent to them, or something they have seen online. And they tend to respond in anger or frustration. They don't think before clicking "send."

Sometimes, while experimenting in role-playing online, they may send cyberbullying communications or target someone without understanding how serious this could be. They do it for the heck of it "Because I Can." They do it for the fun of it. They may also do it to one of their friends, joking around. But their friend may not recognize that it is another friend or make take it seriously. They tend to do this when alone, and are mostly surprised when someone accuses them of cyber abuse.

Reference 12

www.stopcyberbullying.org (cont)

"Because I can" - When kids act out violent fantasies online

All kids act out fantasies online, pretending to be someone or something they're not. But sometimes they act out violent fantasies online, too. Twenty seventh-graders sat quietly in the library, not quite sure who I was or why they were seated there. I looked around at the group. These were typical suburban, well-mannered kids. They lived in a town with good schools, safe streets, and PTA bake sales. I didn't expect any surprises. (Now, for you parents and teachers out there, you know what happened next.)

I asked them how often they used the Internet and what they did online. Each responded that they used it daily. Most admitted to chatting online, surfing music and sports sites, and sending instant messages and e-mail to friends. Some had set up their own Web sites. I received typical responses to my typical questions.

Then I asked them what they did online that their parents wouldn't want them to do. (I am always amazed how many kids confess outrageous things to me, just to be helpful.) That's when it got interesting. A few kids admitted to setting up a Web site that made fun of an overweight girl in the school. They told others in school about the site, and the girl was very upset, understandably. They put up a fake profile on AOL, pretending to be her. (These kids had way too much time on their hands.)

A few others admitted to using a parent's credit card to access adult sites. (It had somehow never occurred to them that a bill would eventually arrive for the pornography service.) Some had been thrown off AOL for using vulgar language or provoking fights online. But the one story I will always remember was from a soft-spoken, shy and intelligent boy, with sandy-colored hair. He was a top student, the kind of kid you knew never got into trouble. He raised his hand and confessed to sending out death threats via e-mail. This got my attention quickly.

We talked a bit about his life. He said that he doesn't get into trouble in "rl" (real life, for us non-geeks). His homework is turned in on time, and he comes straight home after school and listens to his parents. But he sends out death threats online. When I probed more, he said that he would never do anything wrong, because he's afraid of getting caught and getting into trouble. He also likes being a "good kid."

He thought that it might be fun to act out his fantasies online. He also was convinced that he couldn't get caught. When I asked him why he did it, he said simply, "Because I can." He is a good kid. He's the kind of kid that you'd want your children to be friends with, the one we refer to when we say "Why can't you be more like...?" He never forgets to say please or thank you. He'd never dream of threatening anyone offline. But online he's not a well-mannered honors student. Online he's the tough and violent kid he always fantasized about being. He plays at being someone else. It's the cyberspace version of Dr. Jekyll and Mr. Hyde. And he does it from the safety of his bedroom, after his homework is finished.

The only problem is that when a death threat arrives via e-mail, the recipient doesn't know that this innocuous honors student sent it—to the recipient, it's a serious threat. It's also a serious threat when law enforcement traces him to his house and knocks on the door.

Reference 12 *(cont)*

www.stopcyberbullying.org (cont)

"Because I can" - When kids act out violent fantasies online (cont)

"Dear Jennifer, I am going to kill you."

At WiredSafety.org, we help cyberstalking victims find their stalkers and prosecute them. They usually come to us when they are already hysterical with fear. One case, where the stalker threatened to kill a terrified mother and her teenage daughter, became a personal quest for Kelley Beatty, my former deputy executive director and former head of our cyberstalking team.

The mother sent us a frantic e-mail. She had been stalked online. The stalker threatened to kill her and her daughter. The stalker also knew personal details about her—offline details, such as her address and full real name. He also knew her telephone number. She had already been to her local police, but they didn't seem to take her fears seriously. She was afraid for her safety and that of her teenage daughter. She had missed several days of work, and was under medical treatment for the stress.

It didn't take Kelley long to figure out how the stalker had this information about the mother. She had included it in her ICQ profile. Getting her telephone number was as easy as accessing the White Pages online and looking her up, using the name and address she had voluntarily supplied to the world—and her stalker. She had also mentioned her daughter in chats, and the stalker apparently had picked up this information. (The mother was immediately advised of this, and removed the personal information. Kelley taught her how to surf anonymously.)

When an online stalking reveals that the stalker has offline information, the case is taken very seriously by us, and should be taken very seriously by law enforcement. Kelley stepped up the investigation. Luckily, the stalker had left a trail of personal information as well. This allowed Kelley and her cyberstalking team to identify him easily. Kelley contacted the stalker and confronted him with the fact that WiredSafety knew who he was, and that what he had done was a crime. He lived in Canada, and the victim lived in the United States. But it's against the law in both countries. (I warn parents not to do this yourselves. Don't contact the cyber stalker. It almost always escalates the stalking. Instead, contact law-enforcement agencies, groups like WiredSafety or their ISP for help.)

He immediately was contrite. He admitted that he was a teenager and was just fooling around. He thought it was fun to try to scare people, and didn't consider it a serious problem since he had no intention of acting on his threats. He promised never to do it again. Kelley shared this information with the victim, who called the home of the stalker. (Again, I advise against doing this.) His grandmother answered and immediately understood the seriousness of her grandson's actions. The victim and Kelley were both satisfied that the matter would be dealt with appropriately, and didn't think that legal intervention was necessary.

Reference 13

www.stopcyberbullying.org (cont)

Are you a cyberbully?
Often, people who are victims are also bullies. Before you feel too bad for yourself, take the quiz below to find if you, too, are part of the cyberbullying problem! Rate yourself on the following point scale according to if, and how many times, you have done the below activities. Give yourself 0 points if you've never done it, 1 point if you have done it 1 or 2 times, 2 points if you have done it 3-5 times, 3 points if you have done it more than 5 times.

Have you ever...

___Signed on with someone else's screen name to gather info?

___Sent an e-mail or online greeting card from someone's account?

___Impersonated someone over IM or online?

___Teased or frightened someone over IM?

___Not told someone who you really are online, telling them to "guess"?

___Forwarded a private IM conversation or e-mail without the permission of the other person?

___Changed your profile or away message designed to embarrass or frighten someone?

___Posted pictures or information about someone on a Web site without their consent?

___Created an Internet poll, either over IM or on a Web site, about someone without their consent?

___Used information found online to follow, tease, embarrass or harass someone in person?

___Sent rude or scary things to someone, even if you were just joking?

___Used bad language online?

___Signed someone else up for something online without their permission?

___Used an IM or e-mail address that looked like someone else's?

___Used someone else's password for any reason without their permission?

___Hacked into someone else's computer or sent a virus or Trojan horse to them?

___Insulted someone in an interactive game room?

___Posted rude things or lies about someone online?

___Voted at an online bashing poll or posted to a guestbook saying rude or mean things?

Reference 13 *(cont)*

www.stopcyberbullying.org (cont)

Are you a cyberbully?(cont)

Now calculate your total score:

0 – 5 Points: Cyber Saint

Congratulations! You're a cyber saint! Your online behavior is exemplary! Keep up the good work!

6-10 Points: Cyber Risky

Well, you're not perfect, but few people are. Chances are you haven't done anything terrible and were just having fun, but try not to repeat your behaviors, since they are all offenses. Keep in mind the pain that your fun might be causing others!

11-18 Points: Cyber Sinner

You're online behavior needs to be reproached! You have done way too many cyber no-no's! Keep in mind that these practices are dangerous, wrong, and punishable and try to be clean up that cyber record!

More than 18: Cyber Bully

Put on the breaks and turn that PC/MAC/text-messaging device around! You are headed in a very bad direction. You qualify, without doubt, as a cyberbully. You need to sign off and think about where that little mouse of yours has been clicking before serious trouble results for you and/or your victim(s), if it hasn't happened already!

Reference 14
www.stopcyberbullying.org (cont)

Take a stand against cyberbullying
Education can help considerably in preventing and dealing with the consequences of cyberbullying. The first place to begin an education campaign is with the kids and teens themselves. We need to address ways they can become inadvertent Cyberbullies, how to be accountable for their actions and not to stand by and allow bullying (in any form) to be acceptable. We need to teach them not to ignore the pain of others.

Teaching kids to “Take 5!” before responding to something they encounter online is a good place to start. Jokingly, we tell them to “Drop the Mouse! And step away from the computer and no one will get hurt!” We then encourage them to find ways to help them calm down. This may include doing yoga, or deep-breathing. It may include running, playing catch or shooting hoops. It may involve taking a bath, hugging a stuffed animal or talking on the phone with friends. Each child can find their own way of finding their center again. And if they do, they will often not become a cyberbully, even an inadvertent cyberbully. Teaching them the consequences of their actions, and that the real “Men in Black” may show up at their front door sometimes helps. Since many cyberbullying campaigns include some form of hacking or password or identity theft, serious laws are implicated. Law enforcement, including the FBI, might get involved in these cases.

But we need to recognize that few cyberbullying campaigns can succeed without the complacency and the often help of other kids. If we can help kids understand how much bullying hurts, how in many cases (unlike the children’s chant) words can hurt you, fewer may cooperate with the Cyberbullies. They will think twice before forwarding a hurtful e-mail, or visiting a cyberbullying “vote for the fat girl” site, or allowing others to take videos or cell phone pictures of personal moments or compromising poses of others. Martin Luther King, Jr. once said that in the end we will remember not the words of our enemies, but the silence of our friends. We need to teach our children not to stand silently by while others are being tormented. While it is crucial that we teach them not to take matters into their own hands (and perhaps become a "vengeful angel" cyberbully themselves) they need to come to us. And if we expect them to trust us, we need to be worthy of that trust. (Read more about this at “Goldilocks and the Cyberbullies...not too hot and not too cold,” a guide for parents.)

And, in addition to not lending their efforts to continue the cyberbullying, if given an anonymous method of reporting cyberbullying Web sites, profiles and campaigns, kids can help put an end to cyberbullying entirely. School administration, community groups and even school policing staff can receive these anonymous tips and take action quickly when necessary to shut down the site, profile or stop the cyberbullying itself.

They can even let others know that they won’t allow cyberbullying, supporting the victim, making it clear that they won’t be used to torment others and that they care about the feelings of others is key. Martin Luther King, Jr. once said “In the end, we will remember not the words of our enemies, but the silence of our friends.”

We need to teach our children that silence, when others are being hurt, is not acceptable. If they don’t allow the Cyberbullies to use them to embarrass or torment others, cyberbullying will quickly stop. It’s a tall task, but a noble goal. And in the end, our children will be safer online and offline. We will have helped create a generation of good cybercitizens, controlling the technology instead of being controlled by it.

Take 5!

Put down the mouse and step away from the computer…and no one will get hurt!

The Internet and mobile technology are very powerful. But if misused, they can also be dangerous to yourself and others. Most of the time we make sure that people are old enough and pass special tests before they drive cars, operate heavy machinery or otherwise use potentially powerful technology. This is for their safety and the safety of others.

But the Internet is different. It's kids who show the adults how to use it. And kids who learn quickly how to abuse it as well. Unfortunately, the abuses are limited only by their limitless imaginations and tech skills.

Our kids use the Internet the way we used the phone when we were young. They "talk" using text-messaging and instant messaging, often at the same time they are chatting on the phone with the same people. It may be hard for parents to conceive of the ways our kids use technologies as part of their everyday lives.

I was talking to some middle school students recently, and asked them how they would feel if they didn't have the Internet anymore. They told me that the Internet is their "life!" It's how the learn, how they communicate, how they socialize and how they share information.

But the casual nature of the way they use the technology leads to abuse and mistakes. The typed word doesn't clarify tone. It doesn't, without more (like an emoticon :oP or an acronym like "jk" which is the short form for "just kidding"), convey the kind of information we obtain when we hear the person's voice or watch their body-language or eye-contact. We make judgments based on how the words appear to us. And those judgments are often wrong. They are often taken out of context and misunderstood.

That results in hurt feelings, anger, frustration and feeling threatened. And when people, especially kids, act out of anger, frustration or fear things get out-of-hand quickly. Like drinking and driving, emotions and the Internet should never be mixed. Emotions create a situation where we click before thinking. We don't think about how the person on the other end may misunderstand our message or our intentions. We don't think at all.

The best way to counter this problem is by teaching our children (and ourselves) to Take 5! - put down the mouse and step away from the computer. By not reacting and taking the time to calm down, we can avoid becoming a cyberbullying ourselves. What can we do for 5 minutes to help us calm down? Kids have suggested: throwing a baseball or shooting hoops, baking cookies, reading, napping, taking a walk or a run, watching TV, talking to a friend and hugging a stuffed animal.

What would you do to Take 5!? Think about it. Now. It may be too late later.

Reference 16

www.stopcyberbullying.org (cont)

WIRED SAFETY - Reporting Terms of Service Violations
Often, the only recourse you have to stop an online bully is to report them to their e-mail service provider, social network, IM service, or ISP. (Cell phone providers are much easier to find and deal with.) If the actions violate the terms of service of that provider, they may lose their account or have it
suspended temporarily. This is frequently enough to stop the bully in their virtual tracks. You start by visiting their ISP or e-mail service provider's terms of service or terms of use section. Read the policy carefully. Make notes about which sections you believe were violated and how.

In the majority of cases, there is also a link for abuse reports. Copy yourself on the communication so you have a record of what you sent, where you sent it, and when.

Don't expect too much, though. It has been our experience that most ISPs are reluctant to act on a first contact, if at all. They have good reasons for this: Sometimes the cyberbully poses as the victim in an attempt to get the ISP to unknowingly assist in the harassment. It is also typical that some of the "evidence" being provided has been fabricated or "enhanced" to be more serious than it actually is. There are also privacy and legal considerations that they must consider. Additionally, they receive hundreds of thousands of TOS reports and have to prioritize them.

The likelihood of getting a response and the provider taking any disciplinary action depends on how well you make your case. All reports should follow the rules the ISP or e-mail provider sets out in their report TOS information. Check and double check to make sure you have it all and have clearly identified whatever you have.

Most ISPs require the following information:

- Date and time that the violations of their TOS took place (keep each violation separate in the report). Let them know your time zone.

- Copies of e-mails, complete with headers. (We teach you how to do that at WiredSafety.org if you don't know. Your e-mail application's "help" instructions may walk you through it also, step-by-step.).

- Alternately, the full and correct URLs of newsgroup or bulletin board postings (copy the exact address in your browser when you read it and paste it "as is" into the report).

- Screen shots of offending IMs (save these also to your computer, as the site may change and you will need proof of what used to be there).

- A timeline of how the situation developed, including copies of all communications. (Using a monitoring application like SpectorSoft Pro can be very helpful here. It can be found at SpectorSoft.com.)

- Any information you can provide as to what steps, if any, you have taken to try to alleviate the situation.

Reference 17

www.stopcyberbullying.org (cont)

What's the Parents' Role in This?

Parents need to be the one trusted place kids can go when things go wrong online and offline. Yet they often are the one place kids avoid when things go wrong online. Why? Parents tend to overreact. Most children will avoid telling their parents about a cyberbullying incident fearing they will only make things worse. (Calling the other parents, the school, blaming the victim or taking away Internet privileges). Unfortunately, they also sometimes under react, and rarely get it "just right."(You can read more about this in "Not Too Hot, Not Too Cold! Goldilocks and the Cyber Parents")

Parents need to be supportive of your child during this time. You may be tempted to give the "stick and stones may break your bones, but words will never hurt you" lecture, but words and cyber attacks can wound a child easily and have a lasting effect. These attacks follow them into your otherwise safe home and wherever they go online. And when up to 700 million accomplices can be recruited to help target or humiliate your child, the risk of emotional pain is very real, and very serious. Don't brush it off.

Let the school know so the guidance counselor can keep an eye out for in-school bullying and for how your child is handling things. You may want to notify your pediatrician, family counselor or clergy for support if things progress. It is crucial that you are there to provide the necessary support and love. Make them feel secure. Children have committed suicide after having been cyberbullied, and in Japan one young girl killed another after a cyberbullying incident. Take it seriously.

Parents also need to understand that a child is just as likely to be a cyberbully as a victim of cyberbullying and often go back and forth between the two roles during one incident. They may not even realize that they are seen as a cyberbully. (You can learn more about this under the "Inadvertent Cyberbully" profile of a cyberbully.)

We have a quick guide to what to do if your child is being cyberbullied: Your actions have to escalate as the threat and hurt to your child does. But there are two things you must consider before anything else. Is your child at risk of physical harm or assault? And how are they handling the attacks emotionally?

If there is any indication that personal contact information has been posted online, or any threats are made to your child, you must run. do not walk, to your local law enforcement agency (not the FBI). Take a print-out of all instances of cyberbullying to show them, but note that a print-out is not sufficient to prove a case of cyber-harassment or cyberbullying. You'll need electronic evidence and live data for that. (You may want to answer the questions on our checklist for helping spot the difference between annoying communications and potentially dangerous ones. But remember, if in doubt, report it.)

Reference 18

www.stopcyberbullying.org (cont)

What's the School's Role in This?

Preventing cyberbullying
Educating the kids about the consequences (losing their ISP or IM accounts) helps. Teaching them to respect others and to take a stand against bullying of all kinds helps too.

How can you stop it once it starts?
Because their motives differ, the solutions and responses to each type of cyberbullying incident has to differ too. Unfortunately, there is no "one size fits all" when cyberbullying is concerned. Only two of the types of Cyberbullies have something in common with the traditional schoolyard bully. Experts who understand schoolyard bullying often misunderstand cyberbullying, thinking it is just another method of bullying. But the motives and the nature of cyber communications, as well as the demographic and profile of a cyberbully differ from their offline counterpart.

What is the school's role in this?
When schools try and get involved by disciplining the student for cyberbullying actions that took place off-campus and outside of school hours, they are often sued for exceeding their authority and violating the student's free speech right. They also, often lose. Schools can be very effective brokers in working with the parents to stop and remedy cyberbullying situations. They can also educate the students on cyber ethics and the law. If schools are creative, they can sometimes avoid the claim that their actions exceeded their legal authority for off-campus cyberbullying actions. We recommend that a provision is added to the school's acceptable use policy reserving the right to discipline the student for actions taken off-campus if they are intended to have an effect on a student or they adversely affect the safety and well-being of student while in school. This makes it a contractual, not a constitutional, issue.

Reference19

www.stopcyberbullying.org (cont)

Telling the difference between flaming, cyber-bullying and harassment and cyberstalking (A guide for law enforcement)

It's not always easy to tell these apart, except for serious cases of cyberstalking, when you "know it when you see it." And the only difference between "cyberbullying" and cyber-harassment is the age of both the victim and the perpetrator. They both have to be under-age. When you get a call, your first response people need to be able to tell when you need to get involved, and quickly, and when it may not be a matter for law enforcement. It might help to start by running through this checklist. If the communication is only a flame, you may not be able to do much about it. (Sometimes ISPs will consider this a terms of service violation.) But the closer it comes to real life threats the more likely you have to get involved as law enforcement. We recommend that law enforcement agents ask parents the following questions. Their answers will help guide you when to get involved and when to recommend another course of action.

The kind of threat:

- The communication uses lewd language
- The communication insults your child directly ("You are stupid!")
- The communication threatens your child vaguely ("I'm going to get you!")
- The communication threatens your child with bodily harm. ("I'm going to beat you up!")
- There is a general serious threat. ("There is a bomb in the school!" or "Don't take the school bus today!")
- The communication threatens your child with serious bodily harm or death ("I am going to break your legs!" or "I am going to kill you!")

The frequency of the threats:

- It is a one-time communication
- The communication is repeated in the same or different ways
- The communications are increasing
- Third-parties are joining in and communications are now being received from (what appears to be) additional people

The source of the threats:

- Your child knows who is doing this
- Your child thinks they know who is doing this
- Your child has no idea who is doing this
- The messages appear to be from several different people

Reference 19 *(cont)*

www.stopcyberbullying.org (cont)

Telling the difference between flaming, cyber-bullying and harassment and cyberstalking (A guide for law enforcement) (cont)

The nature of the threats:

- Repeated e-mails or IMs
- Following the child around online, into chat rooms, favorite Web sites, etc.
- Building fake profiles, Web sites or posing as your child's e-mail or IM
- Planting statements to provoke third-party stalking and harassment
- Signing your child up for porn sites and e-mailing lists and junk e-mail and IM.
- Breaking in to their accounts online
- Stealing or otherwise accessing their passwords
- Posting images of the child online (taken from any source, including video and photo phones)
- Posting real or doctored sexual images of the child online
- Sharing personal information about the child
- Sharing intimate information about the child (sexual, special problems, etc.)
- Sharing contact information about the child coupled with a sexual solicitation ("for a good time call …" or "I am interested in [fill in the blank] sex…")
- Reporting the child for real or provoked terms of service violations ("notify wars" or "warning wars")
- Encouraging that others share their top ten "hit lists," or ugly lists, or slut lists online and including your child on that list.
- Posting and encouraging others to post nasty comments on your child's blog.
- Hacking your child's computer and sending your child malicious codes.
- Sending threats to others (like the president of the United States) or attacking others while posing as your child.
- Copying others on your child's private e-mail and IM communications.
- Posting bad reviews or feedback on your child without cause.
- Registering your child's name and setting up a bash Web site or profile.
- Posting rude or provocative comments while posing as your child (such as insulting racial minorities at a Web site devoted to that racial minority).
- Sending spam or malware to others while posing as your child.
- Breaking the rules of a Web site or service while posing as your child.
- Setting up a vote for site (like "hot or not?") designed to embarrass or humiliate your child.
- Masquerading as your child for any purpose.
- Posting your child's text-messaging address or cell phone number online to encourage abuse and increase your child's text-messaging or cell phone charges.
- Launching a denial of service attack on your child's Web site
- Sending "jokes" about your child to others or mailing lists.

The more repeated the communications are, the greater the threats (or enlarging this to include third-parties) and the more dangerous the methods, the more likely law enforcement or legal process needs to be used. If personal contact information is being shared online, this must be treated very seriously.

Reference 19 *(cont)*

www.stopcyberbullying.org (cont)

Telling the difference between flaming, cyber-bullying and harassment and cyberstalking (A guide for law enforcement) (cont)

If the child thinks they know who is doing this, that may either make this more serious, or less. But once third-parties are involved (hate groups, sexually-deviant groups, etc.) it makes no difference if the person who started this is a young seven year old doing it for a laugh. It escalates quickly and can be dangerous.

It's best to work out relationships with the big ISPs in your area well before you need them. Find their offline contact information, including off hours. Learn how to track an IP address and preserve evidence. And make sure that you issue your subpoenas in the form they need, using your time zone for tracking the dynamic IP addresses of record. Many ISPs discard the subscriber/IP data after a week to thirty day period. So time is crucial. If you need to get your paperwork together, send them a quick note asking them to preserve the records pending your formal subpoena. They will usually do this on a less formal request on law enforcement letterhead.

Reference 20

Dr. Sameer Hinduja, is an assistant professor in the Department of Criminology and Criminal Justice at Florida Atlantic University

Dr. Justin W. Patchin, is an assistant Professor of Criminal Justice in the Department of Political science at the University of Wisconsin-Eau Claire

Together, they lecture across the United States on the causes and consequences of cyberbullying and offer comprehensive workshops for parents, teachers, counselors, mental health professionals, law enforcement, youth and others concerned with addressing and preventing online aggression.

Their book, Bullying Beyond the Schoolyard: Preventing, and Responding to Cyberbullying, is available from Sage Publications (Corwin Press)
Website: www.cyberbullying.us.

The Cyberbullying Research Center is dedicated to providing up-to-date information about the nature, extent, causes, and consequences of cyberbullying among adolescents.

Research

In 2010, a sample study of 4441 10-18 year olds revealed the **Teens Use of Technology** in the USA in weekly activities includes the

Reference 21

Teens Use of Technology

According to Sameer Hinduja & Justin W. Patchin, 2010, a sample study of 4441; 10-18 year olds revealed the **Teens Use of Technology** in the USA in weekly activities includes the following:–

Cell phones	83.0%
Sent text message	77.3%
Internet for schoolwork	50.8%
Facebook	50.1%
Console games(Xbox, Playstation)	50.0%
Used cell phone at school	47.1%
Email	46.2%
Instant messaging	40.7%
Took pictures with cell phone	40.5%
Online games	38.6%
MySpace	37.7%
Gone online with cell phone	31.5%
Chat rooms	16.8%
Webcam	14.5%
YouTube	11.5%
Twitter	6.5%
Virtual worlds(Gaia, Second Life)	6.5%

Sameer Hinduja & Justin W. Patchin, 2010 – Teens Use of Technology (N=4441)

Reference 22

Cyberbullying Victimization

According to Sameer Hinduja & Justin W. Patchin, 2010, a sample study of 4441; 10-18 year olds revealed the **Cyberbullying Victimization** in lifetime and in previous 30 day period was as follows:–

Lifetime	
1. I have been cyberbullied (lifetime)	20.8%
Last 30 Days	
1. I have been cyberbullied (last 30 days)	7.5%
2. Mean or hurtful comments online	14.3%
3. Rumours online	13.3%
4. Threatened to hurt me through a cell phone text	8.4%
5. Threatened to hurt me online	7.2%
6. Pretended to be me online	6.7%
7. Posted a mean or hurtful picture online of me	5.0%
8. One or more or more times	17.0%

Cyberbullying Offending

According to Sameer Hinduja & Justin W. Patchin, 2010, a sample study of 4441; 10-18 year olds revealed the **Cyberbullying Offending** in lifetime and in previous 30 day period was as follows:–

Lifetime	
1. I have cyberbullied others (lifetime)	19.4%
Last 30 Days	
1. I have cyberbullied others (last 30 days)	8.6%
2. One or more of the forms, two or more times	11.2%
3. I posted mean or hurtful comments about someone online	8.8%
4. I spread rumours about someone online through text messages, or emails	6.8%
5. I threatened to hurt someone through a cell phone text message	5.4%
6. I threatened to hurt someone while online	5.2%
7. I pretended to be someone else online and acted in a way that was mean or hurtful to them	4.6%
8. I posted a mean or hurtful picture online of someone	3.9%
9. I posted a mean or hurtful video online of someone	3.10%
10. I created a mean or hurtful web page about someone	2.90%

Reference 23

Cyberbullying by Gender

According to Sameer Hinduja & Justin W. Patchin, 2010, a sample study of 4441; 10-18 year olds (2212 Male & 2162 Female) revealed the **Cyberbullying by Gender** in lifetime and in previous 30 day period was as follows:–

As Victim

Lifetime

1. I have been cyberbullied (lifetime) 16.6% - (Male)
2. I have been cyberbullied (lifetime) 25.1% - (Female)

Last 30 Days

1. I have been cyberbullied (last 30 days) 7.0% - (Male)
2. I have been cyberbullied (last 30 days) 7.9% - (Female)

3. Someone posted mean or hurtful comments online 10.5% - (Male)
4. Someone posted mean or hurtful comments online 18.2% - (Female)

5. Someone posted mean video about me online 3.6% - (Male)
6. Someone posted mean video about me online 2.3% - (Female)

As Bully

Lifetime

1. I have cyberbullied others (lifetime) 17.5% - (Male)
2. I have cyberbullied others (lifetime) 21.3%- (Female)

Last 30 Days

3. I have cyberbullied others (last 30 days) 9.3% - (Male)
4. I have cyberbullied others (last 30 days) 7.9% - (Female)

5. I spread rumours online about others 6.3%- (Male)
6. I spread rumours online about others 7.4%- (Female)

7. I posted a mean / hurtful picture online 4.6% - (Male)
8. I posted a mean / hurtful picture online 3.1% - (Female)

Reference 24

Cyberbullying Glossary – Hinduja & Patchin, 2010 - USA

Anonymizer: An intermediary Web site that hides or disguises the IP address associated with the Internet user. Generally, these sites allow a person to engage in various Internet activities without leaving an easily traceable digital footprint.

Acceptable Use Policy (AUP): A policy that organizations create to define the responsibilities and appropriate behaviors of computer and network users.

Bash Board: An online bulletin board on which individuals can post anything they want. Generally, posts are malicious and hateful statements directed against another person.

Blocking: The denial of access to particular parts of the Internet. Usually a message will be shown on screen to say that access has been denied. For example, instant message users can block other screen names from sending them messages.

Blog: Interactive Web journal or diary, the contents of which are posted online where they are viewable by some or all individuals. The act of updating a blog is called "blogging." A person who keeps a blog is referred to as a "blogger." The term was created by combining *web* and *log.*

Buddy List: A collection of names or handles (also known as screen names) that represent friends or "buddies" within an instant messaging or chat program. They are useful in informing a user when that person's friends are online and available to chat.

Bullying: Repeated and deliberate harassment directed by one in a position of power toward one or more. Can involve physical threats or behaviors, including assault, or indirect and subtle forms of aggression, including rumor spreading. The term *bullying* is usually reserved for young people and most often refers to these behaviors as they occur at or near school.

Cell Phone: A wireless handheld device that allows for telephone communications.

Chat: An online conversation, typically carried out by people who use nicknames instead of their real names. A person can continually read messages from others in the chat room and then type and send a message reply.

Chat Room: A virtual online room where groups of people send and receive messages on one screen. Popular chat rooms can have hundreds of people all communicating at the same time. What you type appears instantly as a realtime conversation. All of the people in the room are listed on the side of the screen with their screen names.

Computer: An electronic device that stores and processes information and facilitates electronic communication when connected to a network.

Reference 24 *(cont)*

Cyberbullying Glossary – Hinduja & Patchin, 2010 – USA (cont)

Cookie: A file on a computer that records user information when visiting a Web site. Cookies are often used to identify the Web sites that the computer has visited, save login information and customization preferences, and enable the presentation of more personalized information or content.

Cyberbullicide: Suicide stemming directly or indirectly from cyberbullying victimization.

Cyberbullying: Intentional and repeated harm inflicted through the use of computers, cell phones, and other electronic devices.

Cyberspace: The electronic "universe" created by computer networks in which individuals interact.

Cyberstalking: Repeated harassment that includes threats of harm or that is highly intimidating and intrusive upon one's personal privacy.

Cyberthreats: Electronic material that either generally or specifically raises concerns that the creator may intend to inflict harm or violence to him- or herself or others.

Digital Footprint: Evidence of a person's use of the Internet. This includes anything that can be linked to his or her existence, presence, or identity.

Digital Immigrant: A person who has not grown up with digital technology, such as computers, cell phones, and the Internet, but has adopted it later. Many adults are referred to as digital immigrants, because they have known a time when the Internet and cell phones didn't exist

Digital Native: A person who has grown up with digital technology, such as computers, cell phones, and the Internet. Many adolescents or young adults would be classified as digital natives, because they have not known a time without the Internet or cell phones.

Email:
Electronic mail. Allows Internet users to send and receive electronic text to and from other Internet users.

Facebook: The second-most popular social networking Web site with over 70 million active users. Users create personal "profiles" to represent themselves, listing interests and posting photos and communicating with others through private or public messages.

Filtering: The act of restricting access to certain Web sites (usually using software programs). For example, a filter might check the text on a Web page with a list of forbidden words. If a match is found, that Web page may be blocked or reported through a monitoring process. Generally
speaking, a filter lets data pass or not pass based on previously specified rules.

Reference 24 *(cont)*
Cyberbullying Glossary – Hinduja & Patchin, 2010 – USA (cont)

Flaming: Sending angry, rude, or obscene messages directed at a person or persons privately or an online group. A "flamewar" erupts when "flames" are sent back and forth between individuals repeatedly.

Firewall: Hardware or software that restricts and regulates incoming and outgoing data to or from computer systems. Firewalls to allow or disallow using certain Web sites or certain Web-based software programs.

Friending: The act of requesting another person to be your friend (and thereby formally connect with you) on a social networking Web site (like MySpace or Facebook).

Gaming: Participation in online games, which often involve individuals adopting roles of fictional characters, thereby directing the outcome of the game.

Happy Slapping: An extreme form of bullying where physical assaults are recorded on mobile phones or digital cameras and distributed to others.

Harassment: Unsolicited words or actions intended to annoy, alarm, or abuse another individual.

Harm: Physical or emotional injury to someone.

Instant Messaging: The act of real-time communication between two or more people over a network such as the Internet. This can occur through software such as AOL Instant Messenger, Microsoft Instant Messenger, or Google Talk. This can also occur while logged into social networking Web sites or via cellular phone.

Internet: A worldwide network of computers communicating with each other via phone lines, satellite links, wireless networks, and cable systems.

IP Address: "Internet Protocol" address. A unique address assigned to a computing device that allows it to send and receive data with other computing devices that have their own unique addresses.

IRC: "Internet Relay Chat." A network over which real-time conversations take place among two or more people in a "channel" devoted to a specific area of interest. *See also* chat or chat room.

ISP: "Internet Service Provider." The company that provides an Internet connection to individuals or companies. ISPs can help with identifying an individual who posts or sends harassing or threatening words.

MMORPG: "Massively multiplayer online role-playing game." A game in which large numbers of individuals from disparate locations connect and interact with each other in a virtual world over the Internet.

Monitoring: The recording and reporting of online activity, usually through software, which may record a history of all Internet use or just of inappropriate use. A person can also serve this function.

Reference 24 *(cont)*

Cyberbullying Glossary – Hinduja & Patchin, 2010 – USA (cont)

MySpace: The most popular social networking Web site with over 230 million accounts created. It allows individuals to create an online representation or "profile" of themselves to include biographical information, personal diary entries, affiliations, likes and dislikes, interests, and multimedia artifacts (pictures, video, and audio). Blogging, messaging, commenting, and "friending" are the primary methods of interacting with others.

Netiquette: "Network etiquette." The unofficial rules of accepted, proper online social conduct.

Network: Two or more computers connected so that they can communicate with each other.

Newbie: Someone who is new to, and inexperienced with, an Internet activity or technology. Also referred to as a newb, n00b, nob, noob, and nub.

Offender: The one who instigates online social cruelty. Also known as the "aggressor."

Profile: When considered in the context of online social networking, this is a user-created Web page—the design of which can be customized—where a person's background, interests, and friends are listed to reflect who that person is or how that person would like to be seen. Streaming
music, video, and digital pictures are often included as well.

Proxy: Software or a Web site that allows one's Internet connection to be routed or tunneled through a different connection or site. If a user's computer is blocked from accessing certain Web sites or programs, the user could employ a proxy to redirect the connection to that site or program. For example, if a software filter prohibits a user from visiting MySpace, a proxy Web site could be used to circumvent the filter and provide access.

Shoulder Surfing: Peering over the shoulder of someone to see the contents on that person's computer or cell phone screen.

SMS: "Short message service." A communications protocol that allows short (160 characters or less) text messages over cell phone.

Social Networking Web Sites: Online services that bring together people by organizing them around a common interest and providing an interactive environment of photos, blogs, user profiles, and messaging systems. Examples include Facebook and MySpace.

Spam: Unsolicited electronic mail sent from someone unknown to the recipient.

Texting: Sending short messages via cell phone.

Threat: Making a statement of taking an action that indicates harm to another.

Trolling: Deliberately and disingenuously posting information to entice genuinely helpful people to respond (often emotionally). Often done to inflame or provoke others.

Reference 24 *(cont)*

Cyberbullying Glossary – Hinduja & Patchin, 2010 – USA (cont)

Victim: The person who is on the receiving end of online social cruelty. Also known as the "target."

VoIP: "Voice over Internet Protocol." The transmission of voice over an Internet connection.

Web: Short for "World Wide Web" or pages linked together via the Internet.

Wireless: Communications in which electromagnetic waves carry a signal through space rather than along a wire.

Wireless Device: Cell phones, personal digital assistants, handheld PCs, and computers that can access the Internet without being physically attached by a cable or data line.

Reference 25

This review looks at understanding the 3 Stages of Components required for a successful Anti-Bullying & Cyber-Safety Intervention.

Three Stages of Anti-Bullying & Cyber-Safety Intervention

1. **Stage 1: - The Common Components**
2. **Stage 2: - Critical Components and**
3. **Stage 3: - Essential Components**

This review offers a typical "Hour Glass' Model Research Review with three distinct Stages with a Broad, Narrow and Detailed Focus.

- **Stage 1: Common Components**

  A broad focus on the most **Common Components** that impact on Individuals and our Community to produce Bullying and Cyber-Bullying with the need for Anti Bullying and Cyber-Safety Intervention
  E.g. Individual and Community - Attitudes and Behaviour Choices

  1.1 Reference 26; Maslow's Hierarchy of Needs – Triangle
  1.2 Reference 27: Resources & Support Matrix - Stewart Healley (2000)
  1.3 Reference 28 – Nature V's Nurture
  1.4 Reference 29 - Nature V's Nurture V's Neurosis – Stewart Healley (2000)
  1.5 Reference 30 -The Positive & Negative Behaviour Choice Continuum, Stewart Healley (2007)

- **Stage 2: Critical Components**

  A narrow focus on the **Critical Components** that will help our Cyber Safety Components to protect Individuals and our Community from Unwanted Bullying and Cyber-Bullying Threats
  E.g. Individual and Community – Mandatory Child Protection Choices

  2.1 The Selfish to Selfless Continuum of Interaction Choices: from Common to Local, State, Federal and International Levels 1-14
  2.2 Problem Solving and Conflict Resolution: The 6 Models

- **Stage 3: Essential Components**

  A detailed focus on the **Essential Components** that will help our Cyber Safety Components to protect Individuals and our Community from Unwanted Bullying and Cyber-Bullying Threats
  E.g. Individual and Community - Education and Legal Pathway Choices

  3.1 Problem Solving and Conflict Resolution: The 6 Models
  3.2 Reference 32 - The Negotiating Conflict Continuum – Stewart Healley (2006)
  3.3 Reference 32 – A Human Rights Guide - Stewart Healley (2006)

Components that Impact on Anti-Bullying and Cyber-Safety Intervention

Stage 1: Common Components

A broad focus on the most **Common Components** that impact on Individuals and our Community to produce Bullying and Cyber-Bullying and the need for Anti Bullying and Cyber-Safety Intervention
E.g. Individual and Community - Attitudes and Behaviour Choices

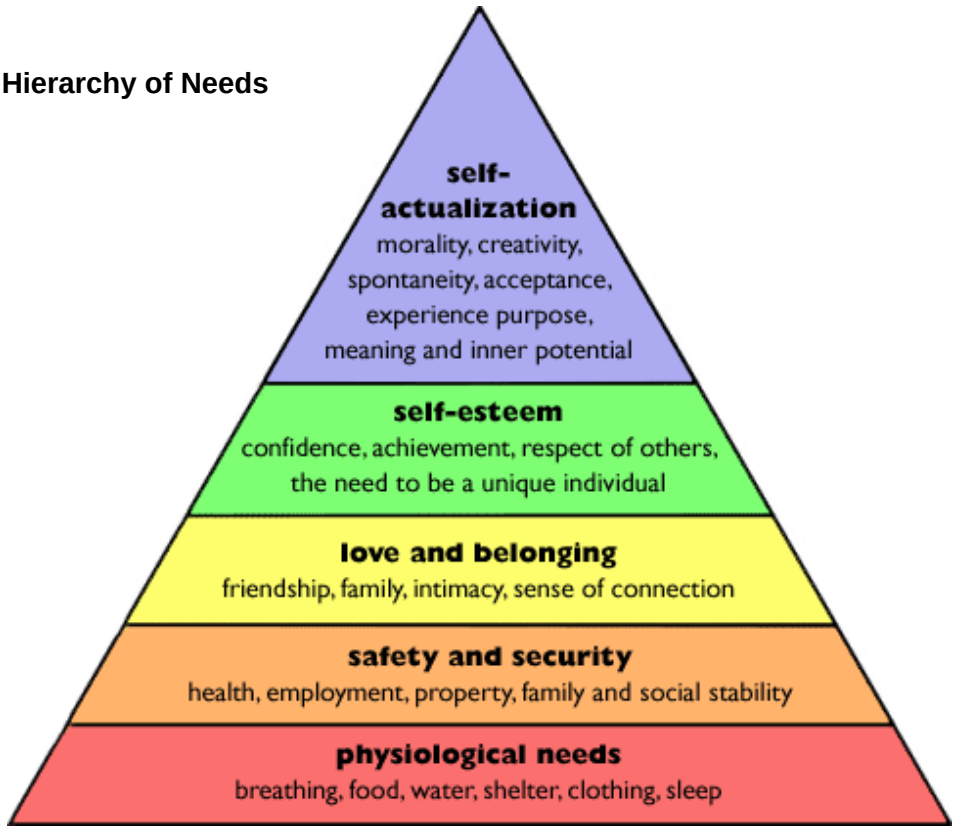
1.1 Reference 26; Maslow's Hierarchy of Needs – Triangle
1.2 Reference 27: Resources & Support Matrix - Stewart Healley (2000)
1.3 Reference 28 – Nature V's Nurture
1.4 Reference 29 - Nature V's Nurture V's Neurosis – Stewart Healley (2000)
1.5 Reference 30 -The Positive & Negative Behaviour Choice Continuum, Stewart Healley (2007)

1.1 Behaviour Choices: *"People with High Needs"* - Maslow's Needs Hierarchy

As a Community we will be forever debating the issue of Sharing of Resources. Unfortunately in Australia, we have continued with the traditional view that the role of providing people less fortunate, less powerful and less informed are "Labeled" as a burden on society, with a "High Level of Needs" rather than people with "Low Resources".

This traditional view of "High Needs People" was first proposed in 1943 with Maslow's Hierarchy of Needs – Triangle.

Maslow's Hierarchy of Needs Triangle



Reference 26: Hierarchy of Needs – Abraham Maslow (1943)

Common Components that Impact on Anti-Bullying and Cyber-Safety Intervention (cont)

Stage 1: **Common Components** (cont)

1.2 Behaviour Choices: *"People with High Needs" = "People with Low Resources"*

However I would like to challenge this accepted concept of thinking of "People with High Needs" with a broader approach to thinking in terms of "People with Low Resources".
I.e. What is a Resource in Australia = e.g. being a White Male; University Educated; Professionally Employed; Young and Healthy; Married with close Family Support; etc.

Sharing in Resources can be best understood when we start to lose access to them or they are being shared with someone else. Our behaviour choices and attitude are proportionally driven by our level of Sharing of Resources & Support or Non – Sharing of Resources & Support
.
Best illustrated in the following Resource & Support Matrix Diagram, Stewart Healley (2000)
.

Resources	Not-Sharing In Resources & Support	Sharing in Resources & Support
High (Low) (Needs)	➢ Feeling Bad ➢ Helpless ➢ Conflict ➢ Unsupported ➢ Out of Control ➢ Disconnecting ➢ Outcast of Society ➢ Aggressive ➢ Covert Power ➢ Angry	➢ Feeling Good ➢ Helping ➢ Confident ➢ Supporting ➢ In-Control ➢ Connecting ➢ Building of Society ➢ Resilient ➢ Overt Power ➢ Alive
Low (High) (Needs)	➢ Feeling Sad ➢ Hopeless ➢ Confused ➢ No Support ➢ No Control ➢ Disconnected ➢ Burden on Society ➢ Stressed ➢ Powerlessness ➢ Suicidal	➢ Feeling Happy ➢ Helped ➢ Comfortable ➢ Supported ➢ Shared Control ➢ Connected ➢ Part of Society ➢ Content ➢ Power Sharing ➢ Euthanistic
Support	Individual	Community

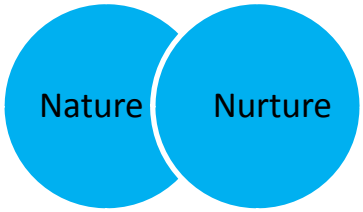
Reference 27 – Resources & Support Matrix - Stewart Healley (2000)

Stage 1:

Common Components that Impact on Anti-Bullying and Cyber-Safety Intervention (cont)

1.3 Behaviour Choices: Nature V's Nurture - Model

The "Old" '2 N' Theory, proposes that we are influenced equally by our experiences of two areas, being Nature and Nurture.



Reference 28 – Nature V's Nurture

This Model reinforces the "ONE SIZE FITS - ALL" approach, and lacks the inclusion and understanding of an individual's life experiences and perspectives.

This Model does not acknowledge how a person's perception of themselves is impacted on by their life experiences, especially ones that may include some traumatic or life threatening events as can be associated with being the victim of Acts or comments of Bullying and Cyber-bullying.

Unfortunately, most people are often challenged and overwhelmed by "traumatic situations" and "terrifying stories" of "real life" experiences of Bullying and Cyber-bullying. Some of these people then tend to hide behind broad protective attitudes, beliefs and "blame the victim" statements like the following:

- *"Toughen up"*
- *"Get over it"*
- *"They didn't really mean it"*
- *"It was a joke"*
- *"What a cry baby"*
- *"Why didn't you fight back"*
- *"Why didn't you tell someone"*

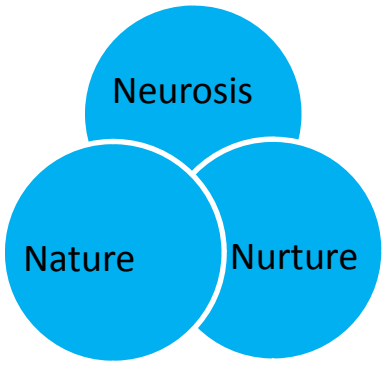
Stage 1:

Common Components that Impact on Anti-Bullying and Cyber-Safety Intervention (cont)

1.4 Behaviour Choices: Nature V's Nurture V's Neurosis (cont)

An alternative approach to this traditional view is offered by a new 3N – Theory, first proposed by the author, Stewart Healley (2000)

This Model proposes that we are influenced equally by our experiences of three areas, being Nature, Nurture and Neurosis.



Reference 29 - Nature V's Nurture V's Neurosis – Stewart Healley (2000)

Where Neurosis, acknowledges the sometimes common, but also the unique differences that each individual possesses and portrays. These personal differences can be described as attitudes, habits and even the "odd quirk or two" that we all posses and that make "us" who we are. Some of these "quirks" we may not be conscious or aware of, but just ask your friends and family, they will easily tell you the things that are different or "unique" about you.

In a friendly and supporting world these personal differences help add the vibrant colours of our world and I believe in Australia our acceptance of Multiculturalism is a public celebration promoting our "Positive Behaviour Choice in Sharing Resources'' by seeking to unit individuals and communities together by sharing our similarities and celebrating our differences.

However, in a World also populated by people who do not share the same appreciation for our differences, there is also a promoting of "Negative Behaviour Choices by Controlling our Resources'' by seeking to divide individuals and communities with overt and covert acts of discrimination.

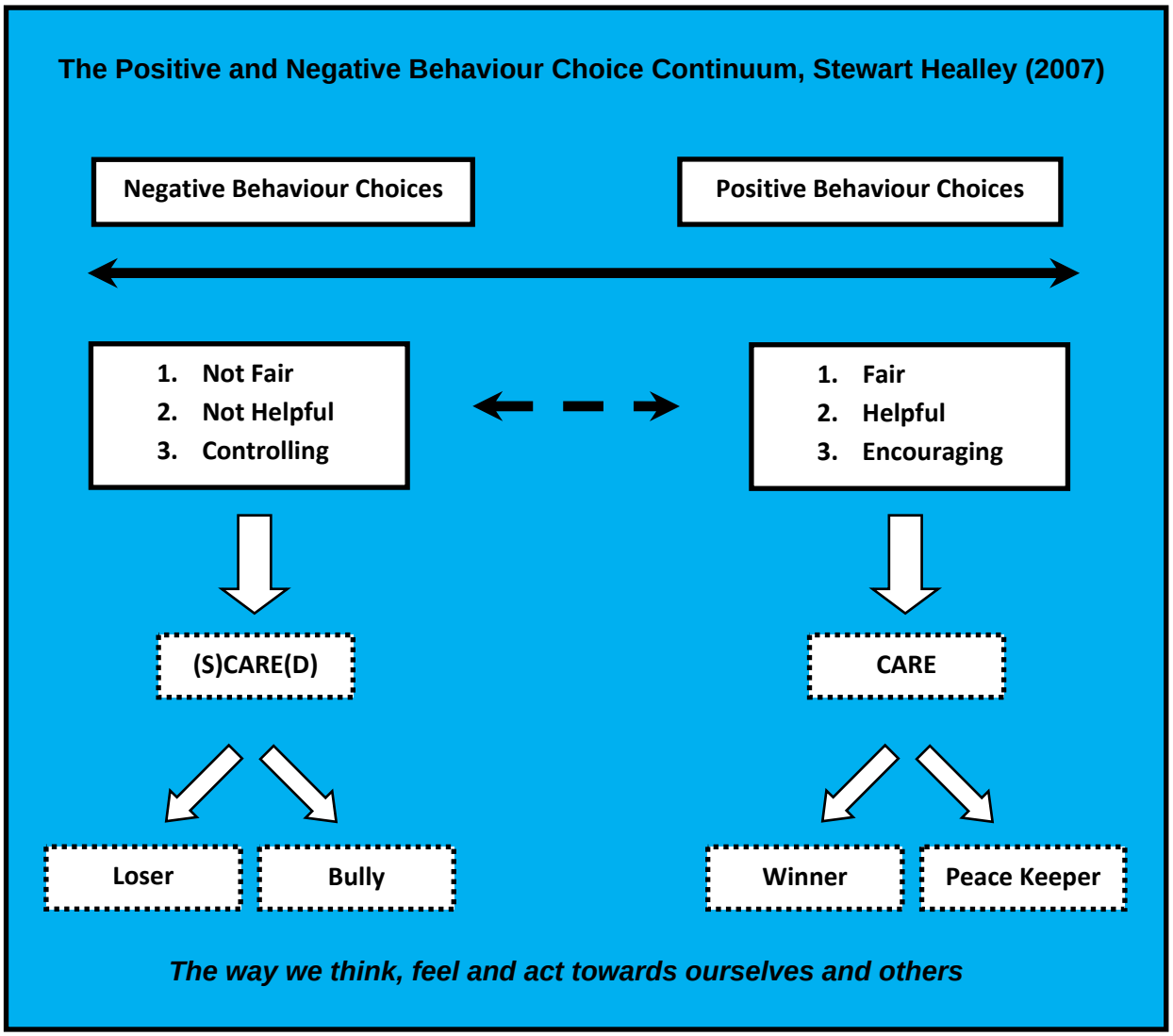
In my opinion, these "Positive" and "Negative Behaviour Choices" are at the **very heart of this debate over Bullying and Cyber-Bullying,** grounded in the strong influences of Nature, Nurture and Neurosis, from cradle to coffin.

Stage 1:

Common Components that Impact on Anti-Bullying and Cyber-Safety Intervention

1.5 **<u>Behaviour Choices</u>**: - Positive & Negative Choice Continuum

The Positive and Negative Behaviour Choices Continuum



Reference 30 - The Positive and Negative Behaviour Choice Continuum, Stewart Healley (2007)

In an ideal world we hope that an individual's immediate family and community will help inspire Positive Citizenship Role Models with **"Positive Behaviour Choices"** and **"Sharing of Resources"**. However, in the real world we are constantly challenged by examples of **Negative Behaviour Choices** and **Non-Sharing of Resources**, encountered at an individual, family, community, State, Nation and even at International levels.

Stage 2:

Specific Components that Impact on Anti-Bullying and Cyber-Safety Intervention (cont)

2.1 <u>The Continuum of Acts of Selfishness and Selflessness</u> -Stewart Healley (2011)

Some behaviour choices can be considered on a continuum with one end appearing to be an extremely selfish position extending to the other end of the continuum with an extremely selfless or heroic position, for example:

The Continuum of Acts of Selfishness and Selflessness
i.e. between Negative and Positive Behaviour Choices:

Reference 31: <u>The Continuum of Acts of Selfishness and Selflessness</u>
Stewart Healley (2011)

Every day we consciously and unconsciously make behaviour choices in different social settings with different consequences for those choices..

An example of Problem Solving and Conflict Resolution areas in our lives can be illustrated by looking at the 14 Levels of interaction that ALL individuals encounter on a daily basis.

<u>Level 1</u> – the **immediate Family level**
<u>Level 2</u> – the **local Neighbourhood level**
<u>Level 3</u> – the **local Community level**
<u>Level 4</u> – the **Kindergarten level**
<u>Level 5</u> – the **Primary School level**.
<u>Level 6</u> – the **High School level**
<u>Level 7</u> – the **College level**
<u>Level 8</u> – the **University level**,.
<u>Level 9</u> – the **Sporting level**
<u>Level 10</u> – the **Work level**
<u>Level 11</u> – the **Commercial level**
<u>Level 12</u> – the **State Government level**
<u>Level 13</u> – the **Federal Government level**
<u>Level 14</u> – the **International level**

Stage 2:

Specific Components that Impact on Anti-Bullying and Cyber-Safety Intervention (cont)

Reference 32

2.2 The 14 Levels of Behaviour Choices in Problem Solving and Conflict Resolution
Stewart Healley (2011)

Level 1 – the **immediate Family level** - parents, siblings and relatives.
1. How do different children and families resolve conflict – within their Family?

Level 2 – the **local Neighbourhood level**, - next door neighbours, street neighbours.
2. How do different children and families resolve conflict – within their Local neighbours?

Level 3 – the **local Community level** – Facilities, Services and Area Socio-Economics
3. How do different children and families resolve conflict – within Local community?

Level 4 – the **Kindergarten level** - Facilities, Standards, Staff and Student Management.
4. How do Students, Families and Staff resolve conflict – within School community?

Level 5 – the **Primary School level** - Facilities, Standards, Student Management.
5. How do Students, Families and Staff resolve conflict – within School community?

Level 6 – the **High School level** – Subjects, Standards, Student Management
6. How do Students, Families and Staff resolve conflict – within School community?

Level 7 – the **College level** – Education Standards, Work Load and Facilities
7. How do Students and Staff resolve conflict – within College community?

Level 8 – the **University level**, - Entry Level, Fees, Education Standards
8. How do different Students and Staff resolve conflict – within University community?

Stage 2: (cont)

Specific Components that Impact on Anti-Bullying and Cyber-Safety Intervention (cont)

2.1 <u>Behaviour Choices: "Problem Solving and Conflict Resolution</u>" (cont)

<u>Level 9</u> – the **Sporting level** – Professional Career, Entertainment and Rules

- School Sport
- District Sport
- State Sport
- National Sport
- Professional Sport
- International Sport

9. How do Players and Clubs resolve conflict – within Sporting community?

<u>Level 10</u> – the **Work level** – Working Conditions and Benefits

- Unskilled Labour
- Skilled Trades
- Professionals
- Management
- Directors
- Company
- Shareholders
- Stock Market

10. How do Workers and Employers resolve conflict – within Working community?

<u>Level 11</u> – the **Commercial level** – Employment, Banking and Finances.

- Public Transport
- Road Transport
- Retail Consumer Protection
  - Water
  - Gas
  - Electricity
  - Petrol
  - Insurance
  - Banking

11. How do Consumers and Businesses resolve conflict – within Business community?

<u>Level 12</u> – the **State Government level** - Taxation, Services and Laws.

12. How do the Public and Politicians resolve conflict – within their State community?

Stage 2 (cont)

Specific Components that Impact on Anti-Bullying and Cyber-Safety Intervention (cont)

2.1 <u>Behaviour Choices: "Problem Solving and Conflict Resolution</u>" (cont)

<u>Level 13</u> – the **Federal Government level** – Taxation, Benefits and Laws

13. How do the Public and Politicians resolve conflict – within their National community?

<u>Level 14</u> – the **International level** – Refugees, Foreign Aid and Military Involvement

14. How do the Public and Politicians resolve conflict – within their International community?

From the above list we can see that a host of various **Common, Local, State and Federal and International Laws** have been developed to assist with Problem Solving and help with Conflict Resolution in the above areas.

However, returning to the main topic of **Bullying and Cyber-bullying**, what laws are available to assist with **Problem Solving** and help with **Conflict Resolution** in this area.

Unfortunately, there are no clear answers, in spite of some very useful and effective Models being promoted within some Schools and Work Places, there is an urgent need for a new **Systematic Approach** to challenge **ALL TYPES** of **Bullying and Cyber-bullying Behaviour**.

Stage 3:

Essential Components that Impact on Anti-Bullying and Cyber-Safety Intervention (cont)

3.1 <u>Behaviour Choices: "Problem Solving and Conflict Resolution</u>" (cont)

Problem Solving and Conflict Resolution

There are various Models available for teaching people how to problem solve with an aim for conflict resolution.

Some of these Models are as follows:

1. **Glasser**
2. **Shared Concerns**
3. **Circle Time**
4. **Mediation**
5. **Restorative Justice**
6. **Negotiating Conflict Continuum - Stewart Healley (2006)**

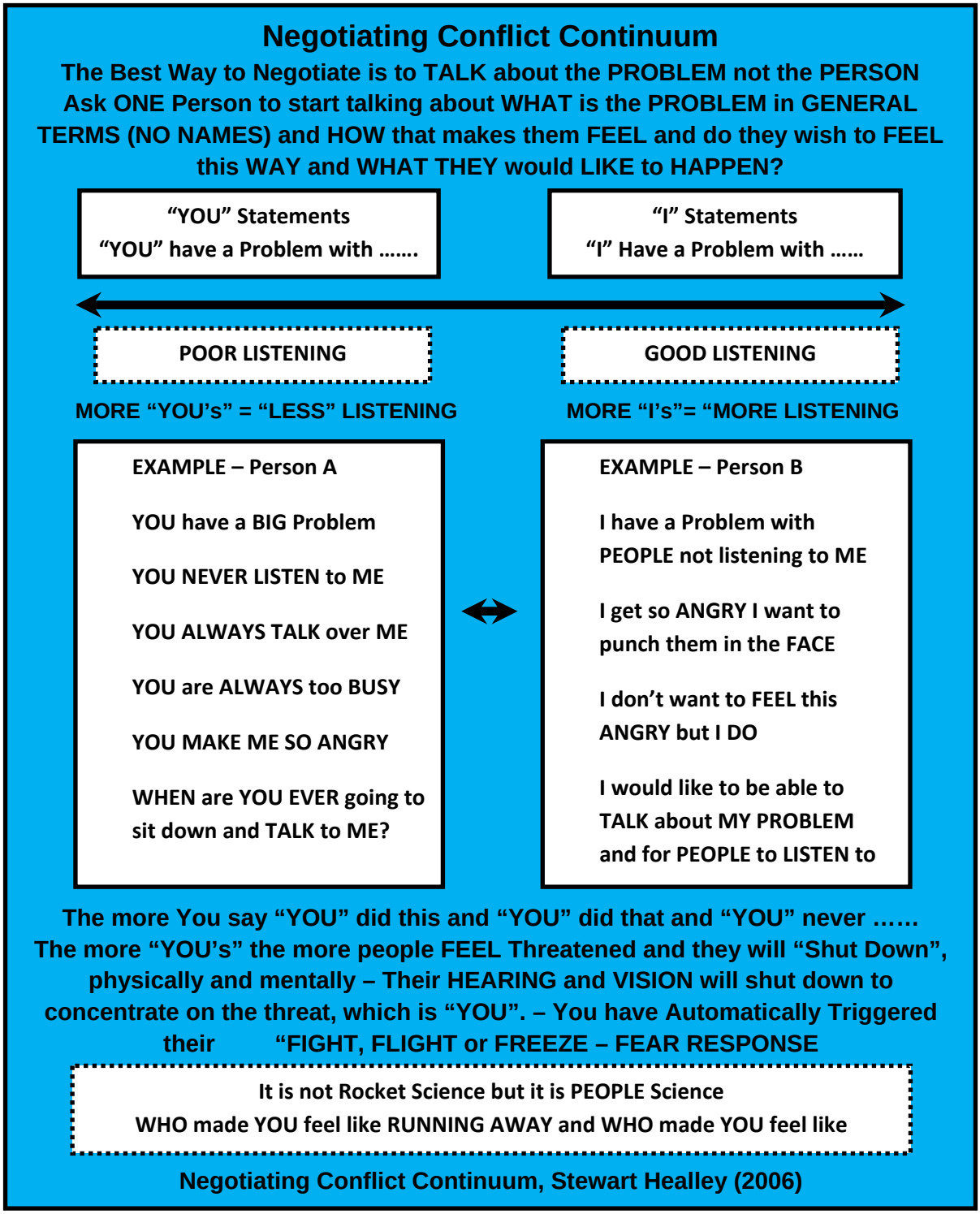
3.2: <u>Reference 33 - The Negotiating Conflict Continuum – Stewart Healley (2006)</u>

3.3: <u>Reference 34 - A Human Rights Guide - Stewart Healley (1996)</u>

<u>Comment:</u>

In my opinion we need to **Negotiate Conflict** and promote which ever **Problem Solving** and **Conflict Resolution Model** that fits and works, supported by a **Restorative Justice Cautioning Pathway Program** when needed.

Stage 3.2: Reference 33 - The Negotiating Conflict Continuum – Stewart Healley (2006)



I AM YOUR EQUAL

I am your Equal

as

You are Mine

No Better no Worse, just Equal

I will Respect your Rights

and

You WILL Respect Mine

Cheers

Stewart Healley (1996)

The End

"Good Things Happen when Good Women & Good Men Do Something"

Stewart Healley

2011