A Supplementary 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

13th April 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:

My original Submission on the 27th march, 2011, proposed some 12 Recommendations for the Honourable Members of the Joint Select Committee on Cybersafety to consider.

I have been following the Inquiry hearings with great interest and anticipation that some positive and professional reality will emerge from the input of ALL of the learned participants.

However, there are times when I truly feel for the Committee Members, who in spite and despite their passion and enthusiasm to understand what is happening and what could happen to improve things in this area for our vulnerable children; far too often when intelligent and valid questions have been posed at some participants the answer is returned with a negative and rigid "stonewalling" attitude or is calmly and intentionally "sidestepped".

Reading through the Hansard transcripts, I often find myself asking the question "Well this is what is done, but what else could we do to improve the situation"? Where is the Positive and Professional Participation for a "Better Solution?"

Hence, I feel the need to add a Supplementary Submission to help encourage the Members of this Inquiry to continue to make real progress towards implementing some practical solutions for our vulnerable children with new and some effective Cyber Safety initiatives.

To restate my position on Cybersafety, it is my opinion that both Bullying and Cyberbullying should be considered as Acts or Comments of Discrimination; and on this basis I have in my original submission made 12 Recommendations to the Joint Parliamentary Committee on ways to best address these matters.

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.**

The focal point of my Supplementary Submission is to expand on my 4th and 6th Recommendations, which I strongly believe are very achievable and will have an immediate and positive impact in promoting Cybersafety for our vulnerable children.

My 4th and 6th recommendations involve the following initiatives:

4. Establish an **Australian National Cyberbullying 24/7 Helpline** and **Reporting System**

6. Establish appropriate **National "Base Line" Legal Framework Laws,** starting with the original **Commonwealth Criminal Code Act 1995**

While the achievement of these recommendations will require some strong negotiations and dedication, the end result will provide a World Class "Cybersafety Model", hopefully encouraging other Countries to implement and support the building of an "International Cybersafety Model

Kind Regards

Stewart Healley

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

Summary

Using Technology to build Three (3) new "Cyber Safety Weapons":

The advances in Communications Technology have brought some amazing advantages for our society, with the many useful and fun applications.

However one of the main disadvantages has been for some user's to appear "invisible" and 'anonymous', while they have intentionally targeted other users, especially our young and vulnerable children for their own "perverse pleasures".

Some of these "perverse pleasures" are in the pursuit of various predatory and sexual pleasures while still others pursue ways to intimidate and threaten easy targets with various "Bullying" and "Cyberbullying" pleasures, within a range of "Online" and "Offline" scenarios.

Currently some users of various "**Carriage Services**" continue to engage in "Inappropriate Online Behaviour" in order to deliberately and intentionally "**menace, harass and cause offence**" to other users of the same or different "Carriage Services"

Often exploiting a "Technical Blind Spot"; as an "Invisible and Anonymous User" in order to engage in these harmful and illegal activities.

However, new technology and new methods can now challenge these "Invisible and Anonymous Users", to be identified as "Visibility and Accountability User's" with new and innovative "Smart" Cybersafety Weapons.

I would like to encourage the introduction of three new "Cyber Safety Weapons" into the Cyber World in the form of the following two Recommendations:

The First and Second were contained in my two part original submission as Recommendation **# 4**, to be identified now as **4A** and **4B** as follows:.

 # 4A Recommendation is to establish a **24 / 7 Help Line** administered by the **Australian Communication and Media Authority (ACMA)**

 # 4B Recommendation is to establish a **National Cybersafety Reporting System - Data Base**, administered by the **Australian Communication and Media Authority (ACMA)**.

The Third further clarification of my original submission as Recommendation **# 6**, and as is now identified as follows:

#6A Establish appropriate **National "Base Line" Legal Framework Laws**, starting with the existing **Commonwealth Criminal Code 1995** and the **Crimes Legislation Amendment (Telecommunications Offences and Other Measures Bill (N0. 2 2004**

Summary (cont)

Simple Solutions:

What we need to do is to create simple but effective solutions to address the growing problem of bullying and cyberbullying present in our schools and general society in Australia.

Some of these Simple Solutions do require some complex and hard work to introduce and maintain, but the end goal of providing protection and support for our young children and vulnerable citizens is worth fighting for.

Some of these Simple Solutions involve setting up the following:

1. Introduce “Problem Solving” Models like “Shared Concerns” into the schools early, starting in Kindergarten. Working with children who do at that age have a strong sense of “Fair” and can learn how to negotiate the world when it is “Not Fair”. We need these building blocks in place early as these children grow through Primary and Secondary School where they desperately want to be “Everybody’s Friend” and “Fit In”.

2. Introduce more sophisticated “Problem Solving” Models in Primary and Secondary School. Such as, Circle Speak; Mediation and Restorative Practices. Students start to learn and use new social skills to influence others so they are their “Best Friend” over “anyone else”. Unfortunately, deception, lies and cruelty are also some new social skills learnt at this time and many arguments and “dramas” later, with some maturity skills start to slowly evolve. However there have been many scars and bad experiences suffered by all participants during this growth cycle of life and death. Tragically, we do have some children unable to cope with their world and do engage in high risk behavior, self harm and even suicide to stop the pain of a “hurtful world”.

3. Introduce “Social Rules” into children’s world with realistic boundaries and encouragement to grow into “Good Citizens”. These rules and roles need to be supported by Family, Friends, School Staff and Community.

4. Introduce “Behaviour Choices and Social Consequences” into children “Real World” experience with family, School and Community Rules.

   Children need clear, consistent and supportive rules and processes applied to ALL, to help set realistic boundaries. Such as some behaviour choices will result in certain consequences from detention, suspension and even Police Charges for Assaulting another Student or Staff Member.

Summary (cont)

5. Introduce “Behaviour Choices and Social Consequences” into children “Cyber World” experience with family, School and Community Rules.

   Again, children need clear, consistent and supportive rules and processes applied to ALL, to help set realistic boundaries. Such as some behaviour choices will result in certain consequences from being blocked as a “Friend”; excluded from “Social Groups”; to having false Web Site pictures and comments posted about you; being the subject of a “Hate Site” and the Server won’t take it down after three days; Socially attacked by your “Cyber Friends” who 90% of them you don’t even know; to being set-up to pay for unwanted items purchased with stolen financial details; to being the target of some sexual predator.

   Welcome to your “Cyber World”, how safe do you really feel?

   Some Simple but effective Solutions for helping children have a better “Cyber World” experience are as follows:

6. **First**, learn how to operate in a “Cybersafe” way, which there are some wonderful resources available to children to explore, the ACMA have also released some helpful advice with their “Cyber[safe]” initiatives.

7. **Second**, be able to Talk to a “Real” Child Support Person about their Cyber Experience, which I am pleased to report is available through ACMA “Report Button”. Although access to this resource is not that easy nor well publicised.

8. **Third**, being able to easily and confidentially Report “Cyber Behaviour” that is inappropriate and offensive to a responsible Adult and Authority,

   Some excellent studies have revealed that children are reluctant to tell any adult about any conflicts as they fear being excluded from the “Offensive” Cyber World, so about 1 in 4 children actually tell an adult.

   Unfortunately, Parents, School Staff, Carriage Services, Government Agencies, Education and Police Departments and the ACMA just don’t get the fact that children desperately want to be accepted by their “friends” even when those friends bully and Cyberbully them. They do not want to be excluded from any social group and want to know what their “friends’ are saying about them – every minute of the day, at this age it is life and death in twenty four hours stuff.

Summary (cont)

So, the result of this scenario is that the existing Cyberbullying measures are “NOT HELPFUL” as they cut children off from their “Good Friends” as well as their “Bad Friends” and therefore will not be very protective nor will it foster good citizenship as there is NO REAL ACCOUNTABILITY or CONSEQUENCES”.

Telling children to Block their “Friend” for offensive or cruel comments presents the child with the following problems and social dilemmas:

You can only block your “Friend” if you first “Un-Friend” them and then you can block them as not a “Friend” and report them to the Service Provider, e.g. Facebook. Who may or may not, decide to block them or remove their comments, depending on their interpretation and only if they break the company rules in their “Rights and Responsibilities” Policy.

In more serious cases the Carriage Service is obliged to block access and report them to a Police Agency. Although I have been advised this action can remove evidence before the Police Agency can properly investigate the complaint.

However, the child has a dilemma, if you “Un-Friend them you cannot see what they are saying about you, because you have blocked them?

So in this case the Carriage Services advise the child to get another “friend” to check on the site and report if any more offensive or cruel comments are posted. Your “friend” will also have to first “Un-friend” them and then report them. This move also helps to further divide and separate the social group and will be visible to all as the “friends” become “Un-Friends”

This current system is not very user friendly nor encouraging to report inappropriate “Online Behaviour”, which may be the desired result from an industry perspective, however, our children deserve a better System!

9. **Fourth**, The ACMA, are the best suited Agency to establish a 24 / 7 Helpline and Complaints Line with an Australian National Reporting System – Data Base. The ACMA have some 650 staff with a wealth of experience and transferable skills to help set up and monitor complaints of Cyberbullying.

The ACMA currently promote the phone number for the Kids Helpline Counsellors, who offer a “Safe and Neutral” contact for children to “Talk About” material that makes them feel scared or worried. They will also learn that Police will ONLY take **action** to protect them if they “Choose” to invite them to help with a Bullying and Cyberbullying situation.

Summary (cont)

10. **Fifth**, Recent discussions with **Kids Helpline Counsellors** have proven to strengthen my view that a practical element to my recommendation for a Australian National Reporting System – Data Base; would be to include the Helpline Counsellors to:

(i) Continue to offer someone "**Friendly**" to "*talk to" a counsellor about cyberbullying or anything that has worried or upset you*"

(ii) Someone to give details regarding any **Cyberbullying incidents** during the phone conversation instead of trying to lodge a **"Scary" Web Page Complaint**; so the children are helped to feel empowered to "Do Something" about being Cyberbullied.

(iii) The Helpline Counsellors can also enter the relevant details into the **ACMA Data Base** with a **recommendation** as to the need to send a **1st Warning Notice** or to **refer the complaint to the AFP** for further investigation due to the seriousness of the Act or Comment of Discrimination and also to the **impact** this has had on the Victim and their Family.

11. **Sixth**, Depending on the success of this Cyberbullying "Online Program" it would be foreseeable to expand this service to another area of major concern for Cyberbullying, being on the "Mobile Phone" - Carriage Services..

ALL Complaints from the ACMA Help Line about **inappropriate Online Behaviour** will be investigated by ACMA Investigators and recorded on the National Cybersafety Reporting System – Data Base and classified as either:

12. (i) An **Invalid Complaint** of a critical, malicious, vengeful, spiteful or frivolous nature.

13. (ii) A **Valid Complaint** of a Inappropriate Online Behaviour, with and Act or Comment of Discrimination; Classified as a **Minor Offence Case** with a **Maximum Penalty** of **3 Years Imprisonmen**t.

14. (iii) A Valid Complaint of Inappropriate Online Behaviour, with an Act or Comment of Discrimination; Classified as a **Serious Offence Case** with a **Minimum Penalty** of **5 Year Imprisonment.**

Summary (cont)

Reference 01:

For Valid Complaints of a Minor Offence Case the ACMA will be issued a
1st Warning Notice, advising the user the following:

1st Warning Notice - ACMA

This Service has been used to send inappropriate material to another - using a Carriage Service.

This Behaviour is now a Criminal Offence in Australia and the Sender may be charged and imprisoned for up to 3 Years, under the:

Commonwealth Crimes Act 1995 Section 474.17 which states it is an offence to:

"Use a carriage service to menace, harass or cause offence"

This Service Account and Electronic Device Identification Number now have a 1st Warning Record on the National Cybersafety Reporting System - Data Base

Summary (cont)

Reference 01:

The ACMA may also issue a **2nd Warning Notice** if applicable such as:

2nd Warning Notice - ACMA

This Service has been used to send inappropriate material to another - using a Carriage Service.

This Behaviour is now a Criminal Offence in Australia and the Sender may be charged and imprisoned for up to 3 Years, under the:

Commonwealth Crimes Act 1995 Section 474.17 which states it is an offence to:

"Use a carriage service to menace, harass or cause offence"

This Service Account and Electronic Device Identification Number now have a 2nd Warning Record on the National Cybersafety Reporting System - Data Base

A **3rd Complaint** about a particular Sender / User or a particular Electronic Device used in a Complaint will be automatically referred to the Australian Federal Police for further investigations and possible Charge / Caution of the Sender or User.

Summary (cont)

15. **Seventh**, All Valid Complaints of a **Serious Offence Case** will be automatically referred from ACMA to the Australian Federal Police for further investigations with a possible Charge / Caution to be recorded against the Sender or User on the Data Base.

The AFP should be encouraged to investigate ALL **Minor Complaint Cases** and take some proactive Police Intervention to Charge children as young as 10 -14 Years Old ONLY if they understand the severity of their Actions or Comments of Discrimination and their "**Intention**" was to deliberately cause harm to their intended "Victim" and not just as a "**Reckless**" Act or Comment.

The AFP should be encouraged to charge young Offenders with a "Base Line" Offence against the

The Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill (No. 2) 2004 No.2.2004

Being,

16. **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.

17. Consideration for the ACMA and AFP staff in assessing Classification of Acts or Comments of Discrimination with Online Content or Material as:

1. **Prohibited Online Content and / or**

2. **Prohibited Online Behaviour**

Summary (cont)

The Guidelines for the Telecommunication Offences contains the following:

18. **<u>473.4 Determining whether material is offensive</u>**

The matters to be taken into account in deciding for the purposes of this Part whether reasonable persons would regard particular material, or a particular use of a carriage service, as being, in all the circumstances, offensive, include:

(a) the standards of morality, decency and propriety generally accepted by reasonable adults; and

(b) the literary, artistic or educational merit (if any) of the material; and

(b) the general character of the material (including whether it is of a medical, legal or scientific character).

After **Charging** and **Caution**, the AFP should assess the parties involved for their suitability for a Restorative Justice Pathway. This assessment requires both an "**Eligible Victim**" and an "**Eligible Offender**".

19. The three advantage of the Restorative Justice Pathway approach is that it ensures:

1. **Professional counselling** help for Victim through Victims of Crime Support.

2. Professional counselling help for Offender with a One Day Training Course **challenging** the **Offenders beliefs** and **understanding** of the negative impacts that Bullying and Cyberbullying create.

3. The Restorative Justice "**face to face**" meeting and apology has proven a very powerful medium for help in restoring confidence and respect for the Victim and equally restoring forgiveness and respect to the Offender and their Family and support persons.

The process of introducing structured "**conflict resolution**" into the discussion around Bullying and Cyberbullying is an essential one.

Children will continue to push boundaries in all matters as part of learning the reality of Behaviour Choices verses Consequences and for some it is a direct challenge to others with an attitude of ***"well who's going to stop me then?"***

Unfortunately, the rules and boundaries regarding Bullying and Cyberbullying have not been clearly defined nor invoked to protect our vulnerable children.

Summary (cont)

20. While some experts warn us from longitudinal studies, that a child displaying Bully Behavior at **8 years** old will still be bullying at **age 14** and will probably have a criminal conviction by the age of **24 years**, there is a need to act now.

21. Regrettably, we have some people involved in this inquiry agreeing with some experts that it is all too hard and that you cannot legislate against "**mean behaviour**".

22. However I would strongly argue that while it is true to say it is hard and yes we cannot legislate against "mean behavior" …….

23. BUT we CAN and MUST ACT with our current Legislation on Cyberbullying with inappropriate Online Behavior when it is done as a clear **Act or Comment of Discrimination**, with a clear intent to harm another person with **Prohibited Online Content** and / or **Prohibited Online Behaviour** and when it involves:

24. **"Using a carriage service to menace, harass or cause offence"**

25. **It is a clear "<u>BREACH of the LAW</u>", being**

26. **<u>474.17 Using a carriage service to menace, harass or cause offence</u>**

27. Reference to the Explanatory Memorandum of the Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill (No.2) 2004 attest to the purpose and spirit of the Members proposing and accepting the application of this Offence (se Appendix 03)

28. Extract: The proposed offence also broadens the coverage of the existing offence in relation to use of a carriage service that is offensive. Existing subsection 85ZE(2) provides that the offence dealing with use of a carriage service in an offensive manner does not apply to 'Internet content', as defined in Schedule 5 to the *Broadcasting Services Act 1992* (Broadcasting Services Act). This exception has been removed under the proposed amendments, so that use of a carriage service, by way of the Internet, in an offensive manner will be covered by the offence

29. **With a legal precedence, being used by the AFP on ONLY three occasions in the last 7 years, in 2004, 2006 and 2011** (see Reference 08)

30. **My comment to this scenario is to encourage ALL involved in this Cybersafety Inquiry, is that "WE CAN DO BETTER?"**

Contents:

Contents:

Contents (cont):

Appendix Reference

Contents (cont):

Reference Information

Contents (cont):

Additional Reference Information

Details of Original and Supplementary Recommendation:

Original Recommendation # 4

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

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

Original 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).

Original 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*

Supplementary Recommendation # 4A

Appoint the Australian Communications and Media Authority (ACMA) responsible for establishing a Australian National Cyberbullying 24/7 Helpline

Supplementary Recommendation # 4A

Appoint the Australian Communications and Media Authority (ACMA) responsible for establishing a Australian National Cyberbullying 24/7 Helpline

Preface to Recommendations 4A &4B

I would like to strongly recommend that the ACMA be given the financial and legal support to take a "Key Role" in this area.

That is, while the ACMA takes a proactive role with:

1. "**Prohibited Online Content**" under the Broadcasting Services Act 1992

The ACMA needs to expand their activities with a new proactive role to also include:

2. "**Prohibited Online Behavior**" under the Criminal Code Act, Telecommunications Offences.

I believe the ACMA to be the best placed organisation to co-ordinate a:

1. **"24 / 7 - "Help Line**" that actually takes reports directly from children and adult about inappropriate Telecommunication Content and Behavior, and

2. **Australian National Cyberbullying Reporting System** to co-ordinate **ALL** complaints about

    - **"Prohibited Online Content"**

        and

    - **"Prohibited Online Behavior"**

I will deal with the concept of a more effective ACMA: **24 / 7 - "Help Line** in this recommendation identified as **Recommendation 4A**

I will then deal with the concept of a new role with an effective ACMA: **Australian National Cyberbullying Reporting System** in the next recommendation identified as **Recommendation 4B**

Supplementary Recommendation # 4A (cont)

The ACMA, are the best suited Agency to establish a 24 / 7 Helpline and Complaints Line with an Australian National Reporting System – Data Base. The ACMA have some 650 staff with a wealth of experience and transferable skills to help set up and monitor complaints of Cyberbullying.

The ACMA currently promote the phone number for the Kids Helpline Counsellors, who offer a "Safe and Neutral" contact for children to "Talk About" material that makes them feel scared or worried. They will also learn that Police will ONLY take **action** to protect them if they "Choose" to invite them to help with a Bullying and Cyberbullying situation.

Recent discussions with **Kids Helpline Counsellors** have proven to strengthen my view that a practical element to my recommendation for a Australian National Reporting System – Data Base; would be to include the Helpline Counsellors to:

(iv) Continue to offer someone "**Friendly**" to "*talk to" a counsellor about cyberbullying or anything that has worried or upset you*"

(v) Someone to give details regarding any **Cyberbullying incidents** during the phone conversation instead of trying to lodge a **"Scary" Web Page Complaint**; so the children are helped to feel empowered to "Do Something" about being Cyberbullied.

(vi) The Helpline Counsellors can also enter the relevant details into the **ACMA Data Base** with a **recommendation** as to the need to send a **1st Warning Notice** or to **refer the complaint to the AFP** for further investigation due to the seriousness of the Act or Comment of Discrimination and also to the **impact** this has had on the Victim and their Family.

Depending on the success of this Cyberbullying "Online Program" it would be foreseeable to expand this service to another area of major concern for Cyberbullying, being on the "Mobile Phone" - Carriage Services..

A background of the current situation can be obtained by a review of the following documents:

1. Reference 02 - Extract of ACMA Web Page – Online Regulations
2. Extract of ACMA Fact Sheet – Prohibited Content
3. The ACMA "Help Button"
4. "Cybersafety Help Button – Report Button Information Page"
5. Example of one Carriage Service Statements Regarding Online Material:
6. Extract of "Facebook" Web Page – Statement of Rights and Responsibilities
7. ACMA - Internet Service Providers and Law Enforcement and National Security fact sheet

Supplementary Recommendation # 4A (cont)

Reference 02 - Extract of ACMA Web Page – Online Regulations

http://www.acma.gov.au/WEB/STANDARD/pc=PC_90154

Online regulation

The ACMA administers a 'co-regulatory' scheme for online content, including internet and mobile phone content. The scheme aims to address community concerns about offensive and illegal material online and, in particular, to protect children from exposure to material that is unsuitable for them.

The scheme is established under Schedule 5 and Schedule 7 of the *Broadcasting Services Act 1992*. In accordance with the scheme the ACMA administers the following functions:

- Investigation of complaints about online content;
- Encouraging the development of codes of practice for the online content service provider industries as well as registering, and monitoring compliance with such codes;
- Providing advice and information to the community about online safety issues, especially those relating to children's use of the internet and mobile phones;
- Undertaking research into internet and mobile phone usage issues and informing itself and the Minister of relevant trends;
- Liaising with relevant overseas bodies.

The **Australian Communications and Media Authority (ACMA**) does offer some good assistance with complaints of Cyberbullying with the new down loadable “Help Button.

A **background** look at what the ACMA are currently offer on their Web Site:

Supplementary Recommendation # 4A (cont)

Extract of ACMA Fact Sheet

http://www.acma.gov.au/WEB/STANDARD/pc=PC_90102

Prohibited Online Content

Under the *Broadcasting Services Act 1992*, the following categories of online content are prohibited:

- Any online content that is classified RC* or X 18+* by the Classification Board (formerly the Office of Film and Literature Classification). This includes real depictions of actual sexual activity, child pornography, depictions of bestiality, material containing excessive violence or sexual violence, detailed instruction in crime, violence or drug use, and/or material that advocates the doing of a terrorist act.

- Content which is classified R 18+* and not subject to a restricted access system that prevents access by children. This includes depictions of simulated sexual activity, material containing strong, realistic violence and other material dealing with intense adult themes.

- Content which is classified MA 15+*, provided by a mobile premium service or a service that provides audio or video content upon payment of a fee and that is not subject to a restricted access system. This includes material containing strong depictions of nudity, implied sexual activity, drug use or violence, very frequent or very strong coarse
  language, and other material that is strong in impact.

* Classifications are based on criteria outlined in the *Classification (Publications, Films and Computer Games) Act 1995*, National Classification Code and the Guidelines for the Classification of Films and Computer Games 2005.

Comment: The Note:

Supplementary Recommendation # 4A (cont)

What types of online content can the ACMA investigate?
The ACMA can only investigate content provided by:

- **Hosting services** – content provided by hosting services includes stored internet content, such as material on WWW, postings made to newsgroups and bulletin boards, files accessible from peer-to-peer applications and content delivered to mobile phones.

- **Live content services** – content provided by live content services includes 'live' streamed video or audio content available on the internet or mobile phones.

- **Links services** – content provided by links services includes links on websites that provide access to other websites that contain prohibited or potentially prohibited content.

Ready to make a complaint?

First, you should review the complaint checklist:

- I am an Australian resident or a company that carries on activities in Australia

- I can provide an internet address and/or sufficient access details to enable the ACMA to access the online content

- I can provide reasons as to why I believe the online content is prohibited

If you can answer yes to each item in the checklist, you are ready to proceed to the Online Content Complaint Form

Complaint Form

Report your complaint

Note: the ACMA "Cybersafety Help Button" Downloadable "Set-Up" instructions can be view on Reference 00 – "They are reasonable complex and beyond a newbie"

Supplementary Recommendation # 4A (cont)

The ACMA "Help Button" activates a further three Active "Oval Shapes with the words of:

1. Talk
2. Report
3. Learn

……..

If you are in danger call '000' or tell an adult you trust

What would you like to do?

Talk Report Learn

1. The Talk oval – ***"Talk to a counsellor about cyberbullying or anything That has worried or upset you"***

Shows a Kids Helpline Button
Do you need to talk to someone about *cyberbullying*, or something that has happened online that has made you uncomfortable, scared or sad?

call Kids Helpline on 1800 55 1800 .

2. The Report oval – ***"Report cyberbullying or anything you've seen online That isn't right"***

3. The Learn oval – ***"Learn how to stay safe online"***

……..

Supplementary Recommendation # 4A (cont)

Reference 03:

Reproduction of ACMA Web Page
Department of Broadband, Communications and the Digital Economy

"Cybersafety Help Button – Report Button Information Page"

Report cyberbullying or anything you've seen online that isn't right.

Uncomfortable with someone or something on a popular social or online game site?

Tell

Found something offensive online that the website will not take down?

Australian Government

acma
Australian Communications and Media Authority

Report offensive online content to the Australian Communications and Media Authority

Found something that may be an online scam or fraud?

SCAMwatch

Report it to

Is someone behaving in A sexual way online that makes you feel uncomfortable?

REPORT ABUSE

Report it to

Supplementary Recommendation # 4A (cont)

Example of one Carriage Service Statements Regarding Online Material:

Appendix 00:

Extract of "Facebook" Web Page – Statement of Rights and Responsibilities

How do I report abuse?

Because of the diversity of our community, it's possible that something could be disagreeable or disturbing to you without meeting the criteria for being removed or blocked. For this reason, we also offer personal controls over what you see, such as the ability to block, hide or unfriend people, Pages, or applications that offend you. Content that does violate our terms may be removed from our site and (in some cases) subject to legal or other action

What happens when I report someone?

All abuse reports on Facebook are confidential. The user that you are reporting will not know that you have reported them. After the report is submitted, Facebook investigates the issue and makes a determination as to whether or not the content should remain on the site based on our Statement of Rights and Responsibilities. In certain situations, the circumstances require more severe action. For instance, users who repeatedly violate our Statement of Rights and Responsibilities can be permanently banned from the site.

Please be aware that not all reported content will be removed. A Facebook administrator looks into each report thoroughly in order to decide the appropriate course of action. If no violation of our Statement of Rights and Responsibilities has occurred, then no action will be taken.

Where else can I report inappropriate or objectionable actions that have been taken against children?

Facebook takes the safety of its users very seriously and takes significant efforts to make sure that the interactions encountered on the site are done so in a safe manner. We strongly urge all users to report suspicious people and inappropriate content when they come across it on the site. You can notify Facebook of any inappropriate people or content by clicking on the "Report" link located throughout the site. Users under the age of 18 are also encouraged to talk to a parent or a responsible adult immediately if someone online says or does something to make them feel uncomfortable or threatened in any way.

Extract of "Facebook" Web Page – Statement of Rights and Responsibilities (cont)

If you are living in the United Kingdom, under 18, and believe that an adult is acting inappropriately towards you on Facebook, please submit an online report to the Child Exploitation and Online Protection Centre (CEOP):

(If you are a parent or other adult and concerned about a minor, you can also submit a report by clicking on the link above.)

More information about safety on Facebook can be found here.

Report a convicted sex offender.

As stated in our Statement of Rights and Responsibilities, convicted sex offenders are prohibited from registering for our service. Once we are able to verify a user's status as a sex offender, we immediately disable their account. When an account is disabled, the profile and all information associated with it are immediately made inaccessible to other Facebook users. What this means is that the user effectively disappears from the Facebook service and will not be able to reactivate their account.

We are only able to remove the accounts of convicted sex offenders if we are able to verify their status with valid documentation. We accept the following forms of documentation: a link to a listing in a national sex offender registry, a link to an online news article, or court document uploaded to this form. If you do not provide valid documentation, we may not be able to process your report.

If you have encountered a profile that may belong to a convicted sex offender, please report it here and we will review the information.

Supplementary Recommendation # 4A (cont)

Appendix 00:

Extract of "Facebook" Web Page – Statement of Rights and Responsibilities

http://www.facebook.com/terms.php

Help Center

Example: What is the Like button? Security: How do I report abuse? Expand All

Account Security Abuse

How do I report abuse?

If you see something on Facebook that you believe violates our terms, you can report it to us.

If you see something on Facebook that you believe violates our terms, you can report it to us. To make a report, find the "Report" link that is nearest to what you want to report:

- **Report a profile:** Go to the profile. Scroll down to the bottom of the left column, under the friend list. Click the "Report/Block This Person" link.
- **Report a photo**: Click on the photo you want to report. Then, click the "Report This Photo" link that's located in the bottom left corner.
- **Report a message:** Open the message and click the "Report" link. Note that you can only report messages from non-friends.
- **Report a group:** Go to the group. Scroll down to the very bottom of the group Wall and click the "Report Group" link.
- **Report an event:** Go to the event. Scroll down to the very bottom of the event Wall and click the "Report Event" link.
- **Report a Page:** Go to the Page. Scroll down to the bottom of the left column, under the Likes list. Click the "Report Page" link.

Because of the diversity of our community, it's possible that something could be disagreeable or disturbing to you without meeting the criteria for being removed or blocked. For this reason, we also offer personal controls over what you see, such as the ability to block, hide or unfriend people, Pages, or applications that offend you. Content that does violate our terms may be removed from our site and (in some cases) subject to legal or other action.

Extract of "Facebook" Web Page – Statement of Rights and Responsibilities (cont)

For information about what we allow and don't allow on Facebook, please read our Community Standards.

How do I report abuse if I don't have an account on Facebook?

You can report any abuse here.

How do I report abusive behavior from a friend on Facebook?

If you are noticing inappropriate behavior from someone on your friend list, you can:

- **Unfriend** the person to remove them from your friend list.
- **Block** the person from contacting you.
- **Report** the person if their behavior is abusive.

What can I do to prevent or address cyberbullying?

We want Facebook to remain an environment where people can connect and share comfortably. Cyberbullying is defined as the use of any new technology to harass or intimidate someone, and there are steps you can take to prevent this kind of behavior if it occurs.

1. Accept Friend Requests Safely

In order to prevent harassment from strangers, be careful to accept friend requests only from people you know in real life. Also, remember to report any messages or profiles that look suspicious. Facebook is based on a real-name culture, and fake profiles are regularly disabled when they're reported to us. Please also keep in mind that only confirmed friends can post to your Wall or contact you via Facebook Chat, so if you're worried that someone will make inappropriate posts or send offensive messages, just ignore that person's friend request.

2. Use the "Block" Feature to Stop Abusive Behavior

Blocking someone prevents them from viewing your profile. When you block people, any ties you currently have with them will be broken, and they won't be able to contact you on Facebook. If you receive inappropriate or abuse communication, you can block the person by going to the Block Lists section on the bottom of the Privacy Settings page.

Extract of "Facebook" Web Page – Statement of Rights and Responsibilities (cont)

3. Report Abusive Behavior Directly to Facebook

The most efficient way to report abuse is to do it in the same place it occurs on Facebook. For example, if you receive a harassing message in your Inbox, you can report the message by clicking on the "Report" link next to the sender's name as you are reading the message. If you receive a harassing message from a person who is a Facebook friend of yours, you should remove the person as a friend and report the message. Reporting the message as harassing will automatically add this person to your Block list. You can also use the "Report/Block person" link that appears at the bottom of the abusive user's profile. If you learn that someone is continuing to make abusive comments about you even after you've blocked them, you can ask a friend to report that person on your behalf. Reports are confidential and the user being reported does not know that they have been reported. After a report is submitted, we will investigate the issue and make a determination as to whether or not the content should remain on the site based on our Statement of Rights and Responsibilities. A Facebook administrator looks into each report thoroughly before taking action. Please note that our team makes it a priority to respond to reports of harassing messages on the site.

4. Restrict Privacy Settings

To restrict the amount of information that potential bullies may have access to, customize your privacy settings so that certain people can't access information like your Wall, photos, or profile. You can also change your privacy settings if you are uncomfortable being found in searches or having your profile viewed publicly. Privacy on Facebook is controlled primarily from the Privacy Settings page. This page is always available by navigating to the "Privacy Settings" option in the Account drop-down menu available from the top of every page. Please note that minors do not have public search listings created for them, so they do not appear in outside search engines until they have turned 18.

5. Respond to Abusers in the Right Way

Cyberbullies often seek a reaction from the people they harass. When they fail to get one, they often give up gradually. Rather than responding to a bully via Inbox, a Wall post, or Facebook Chat, you can use the "Block" or "Report" functions to resolve the issue safely. Remember, only confirmed friends can post to your Wall or send you a message through Chat. If you are receiving posts and Chat messages you don't like, you should consider removing the sender from your friends list. Please note that you should also contact the authorities if you ever feel threatened by something you see on the site.

Facebook is a founding member of the Stop Cyberbullying Coalition affiliated with stopcyberbullying.org.

Extract of "Facebook" Web Page – Statement of Rights and Responsibilities (cont)

What can I do to protect the security of my account?

1. **Never click suspicious links:** It is possible that your friends could unwillingly send spam, viruses...

Never click suspicious links: It is possible that your friends could unwillingly send spam, viruses, or malware through Facebook if their accounts are infected. Do not click this material and do not run any ".exe" files on your computer without knowing what they are. Also, be sure to use the most current version of your browser as they contain important security warnings and protection features. Current versions of Firefox and Internet Explorer warn you if you have navigated to a suspected phishing site, and we recommend that you upgrade your browser to the most current version. You can also find more information about phishing and how to avoid it at http://www.antiphishing.org/consumer_recs.html and http://onguardonline.gov/phishing.html.

Phishing is an online attempt to trick a user by pretending to be an official login page or an official email from an organization that you would have an account with, such as a bank or an email provider, in order to obtain a user's login and account information. In the case of a phishing login page, the login page may look identical to the login page you would normally go to, but the website does not belong to the organization you have an account with (the URL web address of the website should reflect this). In the case of a phishing email, the email may look like an email you would get from the organization you have an account with and get emails from, but the link in the email that it directs you to takes you to the above phishing login page, rather than a legitimate login page for that organization.

To prevent your account information from being obtained in a phishing scheme, only log in to legitimate pages of the websites you have an account with. For example, "www.facebook.example.com" is not a legitimate Facebook page on the "www.facebook.com" domain, but "www.facebook.com/example" is a legitimate Facebook page because it has the "facebook.com" domain. When in doubt, you can always just type in "facebook.com" into your browser to return to the legitimate Facebook site.

2. **Have a unique, strong password:** From the Account Settings page, be sure to use a different password than you use for other sites or services, made up of a complex string of numbers, letters, and punctuation marks that is at least six characters in length. Do not use words found in the dictionary.

Extract of "Facebook" Web Page – Statement of Rights and Responsibilities (cont)

3. Run anti-virus software: If your computer has been infected with a virus or with malware, you will need to run anti-virus software to remove harmful programs and keep your information secure.

- For Windows:

http://www.microsoft.com/protect/viruses/xp/av.mspx

http://www.microsoft.com/protect/computer/viruses/default.mspx

- For Apple/Mac OS:

http://support.apple.com/kb/HT1222

For more information about keeping your account secure, please visit our Security Page.

My account was compromised, phished, or is sending messages that I didn't send.

To take immediate steps to regain control of your account, click here.

To learn more about these threats and how to keep your account secure, click here.

My friend's account was compromised, phished, or is sending me spam or advertisements that he/she didn't send.

If your friend's account is sending spam or advertisement messages or links, it is possible that malicious software was downloaded to your friend's computer or that their login information was stolen in an attempt to send spam from their profile. Please encourage your friend to view the phishing page of our Help Center. For detailed information about this matter, please click here.

If your friend's account has been taken over by another person, you can also report this to us by clicking here. Unfortunately, we cannot release information regarding a user's account to anyone but the account holder. If you would like us to investigate this issue further, please have your friend view the Privacy and Security pages of the Help Center from their own account or email address.

Extract of "Facebook" Web Page – Statement of Rights and Responsibilities (cont)

My account was compromised and my Zynga poker chips were stolen.

Unfortunately, Facebook did not develop this poker application and cannot assist you in restoring any lost poker chips. This application is developed and operated by an external developer that uses their own technical resources, and we do not have access to this data.

Please reset your password immediately for security reasons, then contact the developer of this application in regards to your situation.

If you are unable to access your Facebook account, click here.

In order to contact the developer who created this application, please go to the application's About Page and click on the "Contact Developer" link at the bottom of the page. Please note that Facebook is not responsible for the support provided by this developer.

If you continue to have problems with this application, please note that you can remove and restrict applications from the "Applications" section of the Privacy page.

I've selected "Keep me logged in" but want to get rid of this.

You can reset this feature by choosing "Logout" from the Account drop-down menu located in the top right corner of any Facebook page.

I received an email that I created a new Facebook account, even though I didn't sign up for a new account.

If you have received a Facebook account confirmation email in error, it's likely that someone has mistakenly attempted to register using your email address. As long as you do not click the link contained in the email, this account will remain unconfirmed. An unconfirmed account can remain on the site for a maximum of three days. While this account is unconfirmed, it will not be able to send messages, write on friends' Walls, post in discussions, poke, tag friends in photos or notes, comment on content, join groups, or like Pages. After three days without confirmation from the owner of the email address, the account will become inaccessible.

If someone has created an account to impersonate or imitate you, please go to the impostor profile and click "Report/Block this person" at the bottom of the left column. Check the "Report this Person" box, choose "Fake Profile" as the reason, and add "Impersonating me or someone else" as the report type. Be sure to add a valid web address (URL) leading to the real profile so that we can review the information.

Extract of "Facebook" Web Page – Statement of Rights and Responsibilities (cont)

How do I reset my password and make sure it's secure?

You can reset your password here. When choosing a new password, be sure to use a different password than you use for other sites or services, made up of a complex string of numbers, letters, and punctuation marks that is at least six characters in length. Do not use words found in the dictionary.

Never click suspicious links: It is possible that your friends could unwillingly send spam, viruses, or malware through Facebook if their accounts are infected. Do not click this material and do not run any ".exe" files on your computer without knowing what they are. Also, be sure to use the most current version of your browser as they contain important security warnings and protection features. Current versions of Firefox and Internet Explorer warn you if you have navigated to a suspected phishing site, and we recommend that you upgrade your browser to the most current version. You can also find more information about phishing and how to avoid it at http://www.antiphishing.org/consumer_recs.html and http://onguardonline.gov/phishing.html

Phishing is an online attempt to trick a user by pretending to be an official login page or an official email from an organization that you would have an account with, such as a bank or an email provider, in order to obtain a user's login and account information. In the case of a phishing login page, the login page may look identical to the login page you would normally go to, but the website does not belong to the organization you have an account with (the URL web address of the website should reflect this). In the case of a phishing email, the email may look like an email you would get from the organization you have an account with and get emails from, but the link in the email that it directs you to takes you to the above phishing login page, rather than a legitimate login page for that organization.

To prevent your account information from being obtained in a phishing scheme, only log in to legitimate pages of the websites you have an account with. For example, "www.facebook.example.com" is not a legitimate Facebook page on the "www.facebook.com" domain, but "www.facebook.com/example" is a legitimate Facebook page because it has the "facebook.com" domain. When in doubt, you can always just type in "facebook.com" into your browser to return to the legitimate Facebook site.

Run anti-virus software: If your computer has been infected with a virus or with malware, you will need to run anti-virus software to remove harmful programs and keep your information secure.

- For Windows:

http://www.microsoft.com/protect/viruses/xp/av.mspx
http://www.microsoft.com/protect/computer/viruses/default.mspx

- For Apple/Mac OS:

http://support.apple.com/kb/HT1222

For more information about keeping your account secure, please visit our Security Page.

Extract of "Facebook" Web Page – Statement of Rights and Responsibilities (cont)

Personal Privacy Abuse

Someone made a fake profile pretending to be a friend or me. How do I report this?

Impostor profiles — fake profiles created to imitate real people — are not allowed on Facebook. To report an impostor:

Go to the profile.

Scroll to the bottom of the left column and click "Report/Block This Person."

As long as you're not friends with the profile, you'll see an option for "This profile is impersonating someone or is fake." Choose this option as the report type. If you don't see this option, unfriend the profile and then try again.

How do I report a fake or impostor profile if I don't have an account on Facebook?

You can report this by clicking here.

How do I report harassment on Facebook if I don't have an account?

You can report any form of harassment here.

What do I do if someone is attacking me in a public forum?

We suggest that you block the person by listing his or her name in the "Blocking People" box at the bottom of the Privacy Settings page. If this does not resolve the problem, please report the user by clicking the 'Report/Block this Person' link that appears at the bottom of the user's profile.

What do I do if someone is attacking me in Facebook Chat?

Only your confirmed friends can contact you through chat. If you're uncomfortable with a chat conversation, you can unfriend that person. If necessary, you can also block the person from contacting you.

Extract of "Facebook" Web Page – Statement of Rights and Responsibilities (cont)

A friend has informed me of abuse from a user whom I have blocked or who has blocked me.

Please ask your friend to report this user. Your friend can submit a report by clicking the "Report/Block this person" link at the bottom of the left column on the abuser's profile. Rest assured that this report will be kept confidential.

What if my current or ex-boyfriend, girlfriend, or spouse is controlling or monitoring what I do on Facebook?

If your current or ex-boyfriend, girlfriend or spouse is controlling or monitoring your activity on Facebook, this could be a sign of relationship abuse. If you think this might be happening to you, please call the National Domestic Violence hotline at 1-800-799-SAFE to find out about resources in your community and get additional safety information.

You may also want to consider restricting privacy on your Facebook account so that certain people can't access information like your Wall, photos, or profile. Remember that computer usage can be monitored. If you're afraid that your computer isn't safe, use a friend's computer or a computer in a public place, or visit http://stoprelationshipabuse.org/techsafe.html to learn more about computer safety.

How do I request the removal of my image for privacy law reasons?

If you are attempting to request the removal of an image of your child, you can take the appropriate steps here to receive additional support.

Facebook removes photos or videos that violate our Statement of Rights and Responsibilities in some way. You can report an abusive photo or video by using the "Report" links located near most pieces of content on the Facebook to report offensive material. If you're tagged in a photo or video you don't like, you can remove the tag by clicking the "remove tag" link next to your name. Your name will be removed, and the photo or video will no longer be associated with your profile.

If you have a copyright complaint in any jurisdiction, you can find more information here.

If you think a photo should be removed because it violates your rights according to a privacy law (originating outside the United States of America), please explain in detail how it violates this law here, and we'll investigate further.

If you think non-photo content (i.e., a video) should be removed because it violates your rights according to a local and national privacy law (originating outside the United States of America), please explain in detail how it violates this law here, and we'll investigate further.

Extract of "Facebook" Web Page – Statement of Rights and Responsibilities (cont)

We will remove photos that you report as unauthorized if this is required by relevant privacy laws provided that you are pictured in the photo and you have filled out the appropriate contact form in its entirety. If you're not the person pictured in the content you wish to report, or their legal representative, please advise that individual to view this page and make the request.

If you live in a country where the law does not require the removal of unauthorized photos for privacy reasons, including the United States, we will not remove unauthorized photos at your request. You may want to consider contacting the user who posted the photo in order to request that it be removed.

Abusive Content

How do I report pornographic content on Facebook?

You can report any photo that violates our Statement of Rights and Responsibilities by using the "Report this Photo" link provided in the bottom right corner underneath the photo. Facebook will monitor these complaints and remove photos as necessary. All reports will be kept confidential.

How do I report pornographic content on Facebook if I don't have an account?

If you're logged into an account, you can report any photo that you feel is offensive by using the "Report" link provided underneath the image. Facebook will monitor these complaints and remove photos as necessary. All reports will be kept confidential. If you don't have an account, you can also report this here.

I need to report a fake profile.

You can report a profile that violates Facebook's Statement of Rights and Responsibilities by clicking the "Report/Block this Person" link in the bottom left column of the profile, selecting "Fake profile" as the reason, and adding the appropriate information. The following categories of profiles are prohibited on the site:

- Profiles that impersonate you or someone else
- Profiles that use your photos
- Profiles that list a fake name
- Profiles that do not represent a real person
- Profiles that have been compromised

Extract of "Facebook" Web Page – Statement of Rights and Responsibilities (cont)

Be sure to choose the correct report type to help us verify the information. Facebook reviews every report we receive in order to determine whether or not the content violates our Statement of Rights and Responsibilities, and will take appropriate action. Rest assured that these reports will be kept confidential.

How do I report an abusive application? What can I do if I believe an application is violating Facebook policies?

You can report an application for abuse by clicking "Report/Contact this Application" at the bottom of any canvas page within the application.

If you are not currently using the application but would like to report it, simply go to the application's Profile Page on Facebook, and click "Report Application" towards the bottom of the left column. To get to the Profile Page, follow these steps:

Enter the application's name in Search.

Scroll down and click to see more results. (Do not click on the application's "Game" result — this will take you to the application's Canvas Page rather than its Profile Page.)

You should be able to locate the application that you're looking for under Applications. Click the "View Application" to the right of the search result to view the application's Profile Page.

In addition, we'd recommend that you contact the developer who created the application directly so they're aware of your report. You can report this to the developer by going to the application's Profile Page and clicking "Contact Developer" towards the bottom of the left column, or by clicking "Report/Contact this Application" at the bottom of any canvas page within the application.

How do I report an objectionable advertisement running in an external application?

If you see an objectionable advertisement and the web address (URL) in your browser window begins with "http://apps.facebook.com/", this is most likely an advertisement running within an external application and not through Facebook. However, Facebook believes that ads are most effective when they are relevant and meet user expectations for a valuable and trusted experience.

Facebook is committed to providing the best user experience possible and we continue to investigate ads that violate our policies. We also encourage developers and ad networks to maintain high quality applications and advertising practices and may take further action against developers who host ads that violate our policy.

If you have confirmed that the advertisement is running within an external application, you can report this to the developer by going to the application's Profile Page and clicking

"Contact Developer" towards the bottom of the left column, or by clicking "Report" at the bottom of any canvas page within the application. You will then see an option to contact the developer directly.

If the advertisement is on Facebook, please follow the instructions listed here to report the advertisement.

A friend has posted something I don't like. What can I do?

You can always block someone who is posting content you don't like. If someone is posting abusive content, please use the report links in the site to report it to Facebook. To learn more about how to report something, click here.

We now also have a system that allows you to give friends feedback on content that you don't like. To let your friends know you don't like something they posted:

- Use the report links and choose "I don't like this post."
- Choose to "Send a message" to your friend.
- Write a message to ask your friend to remove the post.

I clicked to report a photo, but now it is asking me to send a message to my friend. Will my friend be notified that I reported the photo?

No, Facebook does not send a notification to your friend if you choose to report the photo.

Instead of reporting the content to Facebook, you can now use the report links to choose to send a message to you friend directly, and ask them to remove it. This does not generate a report to Facebook, but it does give feedback to your friend who can remove something you don't like.

Sensitive Account Reports

My friend's/son's/daughter's account has been removed from the site.

Unfortunately, we cannot release any information regarding a user's account to anyone but the account holder. If you would like us to look into this issue, please tell this individual to contact us directly from his or her login email address and include a brief description of the problem. We apologize for any inconvenience.

Extract of "Facebook" Web Page – Statement of Rights and Responsibilities (cont)

Where else can I report inappropriate or objectionable actions that have been taken against children?

Facebook takes the safety of its users very seriously and takes significant efforts to make sure that the interactions encountered on the site are done so in a safe manner. We strongly urge all users to report suspicious people and inappropriate content when they come across it on the site. You can notify Facebook of any inappropriate people or content by clicking on the "Report" link located throughout the site. Users under the age of 18 are also encouraged to talk to a parent or a responsible adult immediately if someone online says or does something to make them feel uncomfortable or threatened in any way.

If you are living in the United Kingdom, under 18, and believe that an adult is acting inappropriately towards you on Facebook, please submit an online report to the Child Exploitation and Online Protection Centre (CEOP):

(If you are a parent or other adult and concerned about a minor, you can also submit a report by clicking on the link above.)

More information about safety on Facebook can be found here.

Report a convicted sex offender.

As stated in our Statement of Rights and Responsibilities, convicted sex offenders are prohibited from registering for our service. Once we are able to verify a user's status as a sex offender, we immediately disable their account. When an account is disabled, the profile and all information associated with it are immediately made inaccessible to other Facebook users. What this means is that the user effectively disappears from the Facebook service and will not be able to reactivate their account.

We are only able to remove the accounts of convicted sex offenders if we are able to verify their status with valid documentation. We accept the following forms of documentation: a link to a listing in a national sex offender registry, a link to an online news article, or court document uploaded to this form. If you do not provide valid documentation, we may not be able to process your report.

If you have encountered a profile that may belong to a convicted sex offender, please report it here and we will review the information.

Extract of "Facebook" Web Page – Statement of Rights and Responsibilities (cont)

How do I report a deceased user or an account that needs to be memorialized or deleted?

Memorializing the account: Please report this information here, so we can memorialize this person's...

Memorializing the account:

Please report this information here, so we can memorialize this person's account. Memorializing the account restricts profile access to confirmed friends only. Please note that in order to protect the privacy of the deceased user, we cannot provide login information for the account to anyone.

Removing the account:

Verified immediate family members may request the removal of a loved one's account. This will completely remove the account from Facebook, so no one can view it. We will not restore the account or provide information on its content unless required by law. If you are requesting a removal and are not an immediate family member of the deceased, your request will not be processed. In this case, the account will be memorialized.

If you are an immediate family member and would like to request that we remove your loved one's account from the site, click here. You may also use this form if you have a special request regarding a deceased user's account.

How do I report terrorist activity or support?

If you find material that promotes terrorist behavior or that raises funds for a terrorist organization, Facebook strongly encourages you to report this here.

Facebook investigates these reports and determines whether to take action based on our Statement of Rights and Responsibilities. All abuse reports on Facebook are confidential.

How do I help someone who may have an eating disorder or has posted worrisome content related to eating disorders?

If you have encountered content or photos that indicate someone is in immediate physical danger related to an eating disorder, please contact 911 or local law enforcement for help. If the threat is not immediate, you should call a family member or loved one who is close by the person you are worried about to try to help. We also recommend that you contact a local helpline to find out more information about how you can help a friend or loved one with a possible eating disorder.

Extract of "Facebook" Web Page – Statement of Rights and Responsibilities (cont)

Facebook is working with the National Eating Disorders Association to provide resources to our users and to support those struggling with an eating disorders, to find treatment referrals and how to help a friend. If you want to find out more about eating disorders, how to educate others and how to prevent them, visit the National Eating Disorders Association website: www.NationalEatingDisorders.org

In the United States, contact the National Eating Disorders Association: 1-800-931-2237; info@myneda.org; www.NationalEatingDisorders.org

In the United Kingdom, contact beat (beating eating disorders), 0845 634 1414 or (beat youthline: 0845 634 7650); help@b-eat.co.uk; www.b-eat.co.uk

In Canada, contact the National Eating Disorder Information Centre (NEDIC), Toll Free: 1-866-NEDIC-20 (1-866-633-4220); Toronto: 416-340-4156; www.nedic.ca

How do I help someone who has posted suicidal content on the site?

If you have encountered a direct threat of suicide on Facebook, please immediately contact law enforcement or a suicide hotline.

For help contacting your local suicide prevention organization, click here.

To report suicidal content to Facebook, click here.

For resources about identifying and responding to suicide warning signals, click here.

I need to find a suicide hotline for myself or a friend.

Suicide hotlines can provide help if you need it, or help you get support for a friend.

For reports in the US, you can contact the National Suicide Prevention Lifeline, a 24/7 hotline, at 1-800-273-TALK (8255). If possible, please encourage the person who posted the content to contact this hotline as well.

For reports in the United Kingdom and Ireland, we recommend that you contact Samaritans at 08457 90 90 90 (UK) or 1850 60 90 90 (Republic of Ireland), or email jo@samaritans.org.

For reports in Norway, we recommend that you encourage the person who posted the content to contact Kirkens SOS at http://www.kirkens-sos.no/ or call 815 33 300.

View a list of suicide prevention hotlines in other countries by visiting http://www.befrienders.org and choosing from the drop-down menu at the top of the page.

Extract of "Facebook" Web Page – Statement of Rights and Responsibilities (cont)

Where can I find resources for identifying and helping a friend who may be suicidal?

Learn more about how to identify and respond to warning signs of suicidal behavior online at the following addresses:

Visit the National Suicide Prevention Lifeline website:
http://www.suicidepreventionlifeline.org/GetHelp/WhatifSomeoneIKnowNeedsHelp.aspx

Visit the Samaritans website:
http://www.samaritans.org/your_emotional_health/worried_about_someone.aspx

If you are concerned about an LGBT person who has posted suicidal content on Facebook, click here.

I want to retract my report now.

Unfortunately, there is no way to retract a report after you have submitted it. Please be aware a Facebook administrator looks into each report thoroughly in order to decide the appropriate course of action. If no violation of our Statement of Rights and Responsibilities has occurred, then no warning will be sent. If a violation has occurred, then a warning or more severe actions are taken.

What happens when I report someone?

All abuse reports on Facebook are confidential. The user that you are reporting will not know that you have reported them. After the report is submitted, Facebook investigates the issue and makes a determination as to whether or not the content should remain on the site based on our Statement of Rights and Responsibilities. In certain situations, the circumstances require more severe action. For instance, users who repeatedly violate our Statement of Rights and Responsibilities can be permanently banned from the site.

Please be aware that not all reported content will be removed. A Facebook administrator looks into each report thoroughly in order to decide the appropriate course of action. If no violation of our Statement of Rights and Responsibilities has occurred, then no action will be taken.

Supplementary Recommendation # 4A (cont)

Reference 04: - Extract of ACMA Fact Sheet

http://www.acma.gov.au/WEB/STANDARD/pc=PC_100072

Internet Service Providers and Law Enforcement and National Security fact sheet

How does the Telecommunications Act apply to Internet service providers and Internet access providers?

The *Telecommunications Act 1997* (the Act) does not refer specifically to internet service providers (ISPs) or internet access providers (IAPs). The Act applies to ISPs and IAPs because they fall into the category of carriage service providers (CSPs). CSPs supply services for carrying communications to the public using a carrier's network. All obligations that apply to CSPs apply to ISPs, including registration with the Telecommunications Industry Ombudsman under Part 10 of the Act, but some may not be relevant. This fact sheet covers obligations on ISPs and IAPs arising out of Parts 13, 14 and 15 of the Act. The term ISP is used to refer to both ISPs and IAPs.

What are the law enforcement and national security obligations of ISPs?
The law enforcement and national security obligations of ISPs are:

- to give officers and authorities of the Commonwealth, States and Territories reasonably necessary assistance in relation to the enforcement of criminal law and laws imposing a pecuniary penalty, protecting public revenue and safeguarding national security;

- to do their best to prevent their network and facilities being used in the commission of offences against the laws of the Commonwealth, or of the States and Territories; and

- to ensure their network or facility is able to intercept a communication passing over it, in accordance with a warrant issued under the *Telecommunications (Interception) Act 1979*.

For more information about interception requirements see the ACMA's Fact Sheet Internet service providers—interception obligations.

Supplementary Recommendation # 4A (cont)

Reference 04: (cont)

What are the privacy obligations of ISPs in relation to customer information?

Part 13 of the Act makes it an offence for an ISP and its employees to use or disclose any information or document which comes into its possession in the course of its ISP business, where the information relates to:

- the contents or substance of a communication carried by the ISP (delivered or not); or
- carriage services supplied, or intended to be supplied, by the ISP; or
- the affairs or personal particulars of another person.

In what circumstances is an ISP authorised to disclose customer information?
Exceptions to the prohibition on disclosure of customer information include:

- where the disclosure is reasonably necessary for the enforcement of the criminal law or the protection of the public revenue (see below);
- where the disclosure is made to ASIO for the performance of its functions;
- where the disclosure is required or is otherwise authorised under a warrant or under law.

What types of customer information will agencies be interested in?
For the purposes of simplification, the type of information agencies may be interested in can be categorised as;

1. the *Identity, Source, Path and Destination* of nominated internet services, and/or
2. the content of nominated communications.

ISP information needed to satisfy requests regarding the *identity, source, path* and destination of nominated services may come from various sources including :

- customer registration details;
- destination and origin email addresses for (user) target communications;
- calling line identification (for user access links);

Supplementary Recommendation # 4A (cont)

Reference 04: (cont)

- geographical location of a target service;
- network/traffic related data; and
- log files (for example, backup tapes showing details of a subscribers internet sessions, including files received).

Information categorised as content does not include network/traffic related data i.e. information required through transmission through networks.

Legislation does not specifically require ISPs (or other CSPs and carriers) to keep this type of information for law enforcement or national security purposes. However, an agency may request the holding of information pending further information or court order. Any costs associated with these requests would need to be agreed between the parties.

Agencies may request access to this information as part of the reasonably necessary assistance requirement, or they may make a specific request that an ISP keep certain information pertaining to a particular user.

How can agencies request customer information from ISPs?
The primary means by which agencies can request access to customer information held by ISPs are by:

- Part 13 Telecommunications Act requests;
- warrants (either interception or general search);
- notice authorised by, or under, law; or
- Court process

Access by agencies to the content of an internet communication in transit will amount to an interception and can only be authorised under the *Telecommunications (Interception) Act 1979* Cth.

Once a communication has been accessed by the user (or deemed to have been accessed, for instance, after it has left the network, or has been stored), it may be accessed by agencies acting under broader statutory or general law powers. These include a search warrant, a notice to produce, or an agency request for release of information derived from powers authorised by or under law [s.280 *Telecommunications Act (1997)* Cth]. This is a broad term which includes other statutory, judicial and quasi-judicial powers, such as court orders made during the discovery process, summons for witnesses to attend and produce records and subpoenas for documents.

Supplementary Recommendation # 4A (cont)

Reference 04: (cont)

Uncertified requests and certificates

Part 13 of the Act allows criminal law enforcement, public revenue and civil penalty enforcement agencies to make certified and uncertified requests for the disclosure of customer information.

For an uncertified request, the ISP must be satisfied that the disclosure of the information is reasonably necessary for the enforcement of criminal law, protection of public revenue or enforcement of a law imposing a pecuniary penalty.
Certified requests are those where a senior officer of a criminal law enforcement agency or a public revenue agency certifies in writing that the disclosure is reasonably necessary.

For certified requests, the ISP may rely on a certificate issued by an authorised officer that the disclosure is reasonably necessary. For uncertified requests, the ISP must make the judgment that the disclosure is reasonably necessary.
The requirement to provide reasonably necessary assistance does not apply to ASIO.

Disclosures may be made to an officer or employee of ASIO authorised in writing by the Director-General of Security to receive the disclosure, where it is made for the performance of ASIO functions, or where the officer or employee certifies that the disclosure is connected with those functions. ASIO requests will usually be in writing, but there may be instances where an urgent verbal inquiry may be necessary.

Warrants
A warrant may be used to access other customer information, including stored communications (see below). Agencies may choose not to use the warrant process if the information may be requested by other means.

Record keeping requirements
ISPs (and other CSPs and carriers) must keep records of all disclosures made under Part 13 (other than disclosures made to ASIO) for each financial year and lodge those reports with the ACMA within 2 months of the end of that financial year. The section 308 report form for reporting disclosures is on the ACMA website.

On what terms must reasonable help be given?
ISPs must give reasonable help to agencies on terms and conditions agreed by the agency and the ISP, and on the basis that the ISP neither benefits from, nor assumes the costs of, giving that help.

Supplementary Recommendation # 4A (cont)

Reference 04: (cont)

What about stored communications?
Access to the content of communications (for example, electronic mail) stored on an ISP's server is unlikely to fall within reasonably necessary assistance. An agency may use a general search or interception warrant or some other statutory provision to access stored communications.

Can an ISP be liable in civil proceedings for the disclosure of customer information?
Section 313 of the Act provides that a carrier or CSP is not liable for damages for an act done or omitted in good faith to give reasonably necessary assistance to officers and authorities of the Commonwealth, States and Territories.

Further information
For further information, please contact:
National and Community Interests Section
Australian Communications and Media Authority
PO Box 13112, Law Courts
Melbourne Vic 8010
Ph: (03) 9963 6800 (03) 9963 6800
Fax: (03) 9963 6961

Supplementary Recommendation # 4B

Appoint the Australian Communications and Media Authority (ACMA) responsible for establishing a Australian National Cyberbullying Reporting System

Supplementary Recommendation # 4B

Appoint the Australian Communications and Media Authority (ACMA) responsible for establishing a Australian National Cyberbullying Reporting System

Fifth, Recent discussions with **Kids Helpline Counsellors** have proven to strengthen my view that a practical element to my recommendation for a Australian National Reporting System – Data Base; would be to include the Helpline Counsellors to:

(vii) Continue to offer someone "**Friendly**" to "*talk to" a counsellor about cyberbullying or anything that has worried or upset you*"

(viii) Someone to give details regarding any **Cyberbullying incidents** during the phone conversation instead of trying to lodge a **"Scary" Web Page Complaint**; so the children are helped to feel empowered to "Do Something" about being Cyberbullied.

(ix) The Helpline Counsellors can also enter the relevant details into the **ACMA Data Base** with a **recommendation** as to the need to send a **1st Warning Notice** or to **refer the complaint to the AFP** for further investigation due to the seriousness of the Act or Comment of Discrimination and also to the **impact** this has had on the Victim and their Family.

Sixth, Depending on the success of this Cyberbullying "Online Program" it would be foreseeable to expand this service to another area of major concern for Cyberbullying, being on the "Mobile Phone" - Carriage Services..

ALL Complaints from the ACMA Help Line about **inappropriate Online Behaviour** will be investigated by ACMA Investigators and recorded on the National Cybersafety Reporting System – Data Base and classified as either:

(i) An **Invalid Complaint** of a critical, malicious, vengeful, spiteful or frivolous nature.

(ii) A **Valid Complaint** of a Inappropriate Online Behaviour, with and Act or Comment of Discrimination; Classified as a **Minor Offence Case** with a **Maximum Penalty** of **3 Years Imprisonmen**t.

(iii) A Valid Complaint of Inappropriate Online Behaviour, with an Act or Comment of Discrimination; Classified as a **Serious Offence Case** with a **Minimum Penalty** of **5 Year Imprisonment.**

Supplementary Recommendation # 4B (cont)

All Valid Complaints of a **Serious Offence Case** will be automatically referred from ACMA to the Australian Federal Police for further investigations with a possible Charge / Caution to be recorded against the Sender or User on the Data Base.

The AFP should be encouraged to investigate ALL **Minor Complaint Cases** and take some proactive Police Intervention to Charge children as young as 10 -14 Years Old ONLY if they understand the severity of their Actions or Comments of Discrimination and their "**Intention**" was to deliberately cause harm to their intended "Victim" and not just as a "**Reckless**" Act or Comment.

The AFP should be encouraged to charge young Offenders with a "Base Line" Offence against the

The Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill (No. 2) 2004 No.2.2004

Being,

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

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

(b) 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.

Consideration for the ACMA and AFP staff in assessing Classification of Acts or Comments of Discrimination with Online Content or Material as:

3. **Prohibited Online Content and / or**

4. **Prohibited Online Behaviour**

Supplementary Recommendation # 4B (cont)

The Guidelines for the Telecommunication Offences contains the following:

473.4 Determining whether material is offensive

The matters to be taken into account in deciding for the purposes of this Part whether reasonable persons would regard particular material, or a particular use of a carriage service, as being, in all the circumstances, offensive, include:

(c) the standards of morality, decency and propriety generally accepted by reasonable adults; and

(b) the literary, artistic or educational merit (if any) of the material; and

(d) the general character of the material (including whether it is of a medical, legal or scientific character).

After **Charging** and **Caution**, the AFP should assess the parties involved for their suitability for a Restorative Justice Pathway. This assessment requires both an "**Eligible Victim**" and an "**Eligible Offender**".

The three advantage of the Restorative Justice Pathway approach is that it ensures:

1. **Professional counselling** help for Victim through Victims of Crime Support.

2. Professional counselling help for Offender with a One Day Training Course **challenging** the **Offenders beliefs** and **understanding** of the negative impacts that Bullying and Cyberbullying create.

3. The Restorative Justice "**face to face**" meeting and apology has proven a very powerful medium for help in restoring confidence and respect for the Victim and equally restoring forgiveness and respect to the Offender and their Family and support persons.

Supplementary Recommendation # 4B (cont)

The Australian Communication and Media Authority (ACMA)

The proposed National Cybersafety Reporting System - Data Base

All complaints to the ACMA Help Line about inappropriate Online Behaviour will be investigated by ACMA Investigators and recorded on the National Cybersafety Reporting System – Data Base and classified as either:

1. A Invalid Complaint of a malicious, vengeful or frivolous nature

2. A Valid Complaint of a Minor Case of Inappropriate Online Behaviour

3. A Valid Complaint of a Serious Case of Inappropriate Online Behaviour i.e. A Case with a Serious Offence and a Penalty of 5 Year Imprisonment

Explanation:

1. A Invalid Complaint of a malicious, vengeful or frivolous nature

- Use of language that is **critical** of the Recipient and or others of a particular Group i.e. As an Act or Comment of Discrimination; e.g. Gender, Ethnicity; Nationality, Age, Disability, Social Status, Religious Beliefs, Scientific Opinion, Political View, etc.

ACMA Investigators action for this case will include the following procedures:

1. **Classify** the Complaint as a Valid Complaint of a Serious Case of Inappropriate Online Behaviour

2. **Record** the Complaint details on the National Cybersafety Reporting System Data Base

3. **Report** the Complaint Immediately to the Australian Federal Police for further Investigation and possible Charging / Caution of Sender

Supplementary Recommendation # 4B (cont)

The proposed National Cybersafety Reporting System - Data Base (cont)

2. A Valid Complaint of Inappropriate Online Behaviour with an Act or Comment of Discrimination - Classified as a Minor Offence Case with a maximum penalty of 3 years imprisonment

- **Use of Offensive, Degrading, Obscene or Offensive Language**
- **Use of Offensive, Degrading, Obscene or Offensive Images**
- **The 3rd Complaint from the one Recipient** or
- **A Further Complaint from the Recipient after the 1st and 2nd Warning Notices** have been sent to the Sender.
- **The 3rd Complaint from Three (3) Different Recipients** or
- **A Further Complaint from the Recipient after the 1st and 2nd Warning Notices** have already been sent to the Sender.

ACMA Investigators action for this case will include the following procedures:

A. Classify the Complaint as a Valid Complaint of a Serious Case of Inappropriate Online Behaviour

B. Record the Complaint details on the National Cybersafety Reporting System Data Base

C. Report the Complaint Immediately to the Australian Federal Police for further Investigation and possible Charging / Caution of Sender

D. Issue a 1st Warning Notice or a 2nd Warning Notice whichever is applicable after checking Data Base for prior complaints

Supplementary Recommendation # 4B (cont)

The proposed National Cybersafety Reporting System - Data Base (cont)

2. . A Valid Complaint of a Minor Case of Inappropriate Online Behaviour

The 1st Warning Notice sent to offending e-mail, web site, chat room, Twitter, Facebook, users that have been the subject of an Online Behaviour Complaint to the ACMA Help Line

1st Warning Notice - ACMA

This Service has been used to send inappropriate material to another - using a Carriage Service.

This Behaviour is now a Criminal Offence in Australia and the Sender may be charged and imprisoned for up to 3 Years, under the:

Commonwealth Crimes Act 1995 Section 474.17 which states it is an offence to:

"Use a carriage service to menace, harass or cause offence"

This Service Account and Electronic Device Identification Number now have a 1st Warning Record on the National Cybersafety Reporting System - Data Base

The 2nd Warning Notice sent to offending e-mail, web site, chat room, Twitter, Facebook, users that have been the subject of an Online Behaviour Complaint to the ACMA Help Line.

2nd Warning Notice - ACMA

This Service has been used to send inappropriate material to another - using a Carriage Service.

This Behaviour is now a Criminal Offence in Australia and the Sender may be charged and imprisoned for up to 3 Years, under the:

Commonwealth Crimes Act 1995 Section 474.17 which states it is an offence to:

"Use a carriage service to menace, harass or cause offence"

This Service Account and Electronic Device Identification Number now have a 2nd Warning Record on the National Cybersafety Reporting System - Data Base

Supplementary Recommendation # 4B (cont)

The proposed National Cybersafety Reporting System - Data Base (cont)

3. A Valid Complaint of Inappropriate Online Behaviour with an Act or Comment of Discrimination - Classified as a Serious Offence Case with a minimum penalty of 5 years imprisonment

Examples of:

- **Threats to Harm, Hurt or Kill** the recipient or another named, directly or indirectly as stated or inferred in an electronic communication to the recipient
- **Threats to Harm, Damage or Destroy** property of the recipient or another, directly or indirectly as stated or inferred in an electronic communication to the recipient
- **Use of language that vilifies** the Recipient and or others of a particular Group i.e. As an Act or Comment of Discrimination; e.g. Gender, Ethnicity; Nationality, Age, Disability, Social Status, Religious Beliefs, Scientific Opinion, Political View, etc.
- **The 3rd Complaint from the one Recipient** or
- **A Further Complaint from the Recipient after the 1st and 2nd Warning Notices** have been sent to the Sender.
- **The 3rd Complaint from Three (3) Different Recipients** or
- **A Further Complaint from the Recipient after the 1st and 2nd Warning Notices** have already been sent to the Sender.

ACMA Investigators action for this case will include the following procedures:

1. **Classify** the Complaint as a Valid Complaint of a Serious Case of Inappropriate Online Behaviour
2. **Record** the Complaint details on the National Cybersafety Reporting System Data Base
3. **Report** the Complaint Immediately to the Australian Federal Police for further Investigation and possible Charging / Caution of Sender

Reference 01: The proposed National Cybersafety Reporting System - Data Base: Warning Notices (cont)

1st Warning Notice - ACMA

This Service has been used to send inappropriate material to another - using a Carriage Service.

This Behaviour is now a Criminal Offence in Australia and the Sender may be charged and imprisoned for up to 3 Years, under the:

Commonwealth Crimes Act 1995 Section 474.17 which states it is an offence to:

"Use a carriage service to menace, harass or cause offence"

This Service Account and Electronic Device Identification Number now have a 1st Warning Record on the National Cybersafety Reporting System - Data Base

2nd Warning Notice - ACMA

This Service has been used to send inappropriate material to another - using a Carriage Service.

This Behaviour is now a Criminal Offence in Australia and the Sender may be charged and imprisoned for up to 3 Years, under the:

Commonwealth Crimes Act 1995 Section 474.17 which states it is an offence to:

"Use a carriage service to menace, harass or cause offence"

This Service Account and Electronic Device Identification Number now have a 2nd Warning Record on the National Cybersafety Reporting System - Data Base

Original Recommendation # 6

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

Original 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:

Appendix 15 – Extract (original Submission)

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.

Supplementary Recommendation # 6A

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

Supplementary Recommendation # 6A

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

All Valid Complaints of a **Serious Offence Case** will be automatically referred from ACMA to the Australian Federal Police for further investigations with a possible Charge / Caution to be recorded against the Sender or User on the Data Base.

The AFP should be encouraged to investigate ALL **Minor Complaint Cases** and take some proactive Police Intervention to Charge children as young as 10 -14 Years Old ONLY if they understand the severity of their Actions or Comments of Discrimination and their "**Intention**" was to deliberately cause harm to their intended "Victim" and not just as a "**Reckless**" Act or Comment.

The AFP should be encouraged to charge young Offenders with a "Base Line" Offence against the

The Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill (No. 2) 2004 No.2.2004

Being,

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

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

(c) 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.

Consideration for the ACMA and AFP staff in assessing Classification of Acts or Comments of Discrimination with Online Content or Material as:

5. **Prohibited Online Content and / or**

6. **Prohibited Online Behaviour**

Supplementary Recommendation # 6A (cont)

The Guidelines for the Telecommunication Offences contains the following:

473.4 Determining whether material is offensive

The matters to be taken into account in deciding for the purposes of this Part whether reasonable persons would regard particular material, or a particular use of a carriage service, as being, in all the circumstances, offensive, include:

(e) the standards of morality, decency and propriety generally accepted by reasonable adults; and

(b) the literary, artistic or educational merit (if any) of the material; and

(f) the general character of the material (including whether it is of a medical, legal or scientific character).

After **Charging** and **Caution**, the AFP should assess the parties involved for their suitability for a Restorative Justice Pathway. This assessment requires both an "**Eligible Victim**" and an "**Eligible Offender**".

The three advantage of the Restorative Justice Pathway approach is that it ensures:

4. **Professional counselling** help for Victim through Victims of Crime Support.

5. Professional counselling help for Offender with a One Day Training Course **challenging** the **Offenders beliefs** and **understanding** of the negative impacts that Bullying and Cyberbullying create.

6. The Restorative Justice "**face to face**" meeting and apology has proven a very powerful medium for help in restoring confidence and respect for the Victim and equally restoring forgiveness and respect to the Offender and their Family and support persons.

Supplementary Recommendation # 6A (cont)

The Australian Communication and Media Authority (ACMA)

The proposed National Cybersafety Reporting System - Data Base

In Summary all complaints to the ACMA Help Line about inappropriate Online Behaviour will be investigated by ACMA Investigators and recorded on the National Cybersafety Reporting System – Data Base and classified as either:

4. A Invalid Complaint of a malicious, vengeful or frivolous nature

5. A Valid Complaint of a Minor Case of Inappropriate Online Behaviour

6. A Valid Complaint of a Serious Case of Inappropriate Online Behaviour i.e. A Case with a Serious Offence and a Penalty of 5 Year Imprisonment

Comment:

To fully comprehend the Legal situation we must refer back to some fundamental information within the following References:

Extract from:

1. **Criminal Code Act 1995 –** 4 March 2011

2. Crimes Legislation Amendment (**Telecommunications Offences** and Other Measures) Bill (No. 2) 2004 No.2.2004

3. **Explanatory Memorandum** – 2002-4Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill (No. 2) 2004 No.2.2004 -

4. **Classification (Publications, Films and Computer Games) Act 1995,** 31 December 2010

Supplementary Recommendation # 6A (cont)

This recommendation includes a focus on the following Offences:

Part 10.6 – Telecommunication Services

- **Division 474 Telecommunication Offences**

Part 10.7 – Computer Offences

- **Division 476, 477 & 478 Computer Offences**

However, the main Offence of this recommendation proposes that the "Base Line" Offence should focus on the following Telecommunications Offence being:

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

A background of the current situation can be obtained by a review of the following documents:

1. Reference 05 - AFP Web Site – Incidents of Harassment
2. Reference 06 - All Saints School News Letter – 25.05.2009
3. Reference 07 – Emonson V Trustees of the Christian Brothers
4. Reference 08 - Bullying and assault – Legal Cases & Compensation
5. Reference 09 Update – Cyber-bullying cases put heat on Google & Facebook
6. Reference 10 - Parents welcome Brodie's Law on Bullying
7. Reference 11 - Nevett Ford Memo - OH & S- Workplace Bullying - May 2010

8. Appendix 01 - Commonwealth Criminal Code Act 1995

9. Appendix 02 - Extract from the Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill (No. 2) 2004 No.2.2004

10. Appendix 00 – Crimes legislation Amendment (Telecommunications Offences and Other Measures) Bill (no.2) 2004 – Explanatory Memorandum

Supplementary Recommendation # 6A (cont)

Appoint the Australian Communications and Media Authority (ACMA) responsible for establishing a Australian National Cyberbullying Reporting System

Conclusion

The things we need to do are as follows:

Introduce "Social Rules" into children's world with realistic boundaries and encouragement to grow into "Good Citizens". These rules and roles need to be supported by Family, Friends, School Staff and Community.

Introduce "Behaviour Choices and Social Consequences" into children "Real World" experience with family, School and Community Rules.

Children need clear, consistent and supportive rules and processes applied to ALL, to help set realistic boundaries. Such as some behaviour choices will result in certain consequences from detention, suspension and even Police Charges for Assaulting another Student or Staff Member.

Introduce "Behaviour Choices and Social Consequences" into children "Cyber World" experience with family, School and Community Rules.

Again, children need clear, consistent and supportive rules and processes applied to ALL, to help set realistic boundaries. Such as some behaviour choices will result in certain consequences from being blocked as a "Friend"; excluded from "Social Groups"; to having false Web Site pictures and comments posted about you; being the subject of a "Hate Site" and the Server won't take it down after three days; Socially attacked by your "Cyber Friends" who 90% of them you don't even know; to being set-up to pay for unwanted items purchased with stolen financial details; to being the target of some sexual predator.

The AFP should be encouraged to investigate ALL **Minor Complaint Cases** and take some proactive Police Intervention to Charge children as young as 10 -14 Years Old ONLY if they understand the severity of their Actions or Comments of Discrimination and their "**Intention**" was to deliberately cause harm to their intended "Victim" and not just as a "**Reckless**" Act or Comment.

The AFP should be encouraged to charge young Offenders with a "Base Line" Offence against the

Conclusion (cont)

The Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill (No. 2) 2004 No.2.2004

Being,

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

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

(d) 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.

Consideration for the ACMA and AFP staff in assessing Classification of Acts or Comments of Discrimination with Online Content or Material as:

7. **Prohibited Online Content and / or**

8. **Prohibited Online Behaviour**

The Guidelines for the Telecommunication Offences contains the following:

473.4 Determining whether material is offensive

The matters to be taken into account in deciding for the purposes of this Part whether reasonable persons would regard particular material, or a particular use of a carriage service, as being, in all the circumstances, offensive, include:

(a) the standards of morality, decency and propriety generally accepted by reasonable adults; and

(b) (b) the literary, artistic or educational merit (if any) of the material; and

(c) the general character of the material (including whether it is of a medical, legal or scientific character).

Conclusion (cont)

After **Charging** and **Caution**, the AFP should assess the parties involved for their suitability for a Restorative Justice Pathway. This assessment requires both an "**Eligible Victim**" and an "**Eligible Offender**".

The three advantage of the Restorative Justice Pathway approach is that it ensures:

1. **Professional counselling** help for Victim through Victims of Crime Support.

2. Professional counselling help for Offender with a One Day Training Course **challenging** the **Offenders beliefs** and **understanding** of the negative impacts that Bullying and Cyberbullying create.

3. The Restorative Justice "**face to face**" meeting and apology has proven a very powerful medium for help in restoring confidence and respect for the Victim and equally restoring forgiveness and respect to the Offender and their Family and support persons.

The process of introducing structured "**conflict resolution**" into the discussion around Bullying and Cyberbullying is an essential one.

Children will continue to push boundaries in all matters as part of learning the reality of Behaviour Choices verses Consequences and for some it is a direct challenge to others with an attitude of ***"well who's going to stop me then?"***

Unfortunately, the rules and boundaries regarding Bullying and Cyberbullying have not been clearly defined nor invoked to protect our vulnerable children.

While some experts warn us from longitudinal studies, that a child displaying Bully Behavior at **8 years** old will still be bullying at **age 14** and will probably have a criminal conviction by the age of **24 years**, there is a need to act now.

Regrettably, we have some people involved in this inquiry agreeing with some experts that it is all too hard and that you cannot legislate against "**mean behaviour**".

However I would strongly argue that while it is true to say it is hard and yes we cannot legislate against "mean behavior" …….

Conclusion (cont)

BUT we CAN and MUST ACT with our current Legislation on Cyberbullying with inappropriate Online Behavior when it is done as a clear **Act or Comment of Discrimination**, with a clear intent to harm another person with **Prohibited Online Content** and / or **Prohibited Online Behaviour** and when it involves:

"Using a carriage service to menace, harass or cause offence"

It is a clear "BREACH of the LAW", being

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

With a legal precedence, being used by the AFP on ONLY three occasions in the last 7 years, in 2004, 2006 and 2011 (see Reference 08)

My comment to this scenario is to encourage ALL involved in this Cybersafety Inquiry, is that "WE CAN DO BETTER?"

……

I think it is also a pertinent time to review the original notes contained in the Explanatory Memorandum regarding the Amendments to the Telecommunications Offences with specific attention to the purpose and spirit of such an Offence

Appendix 03 – Extract of Division 474 – Telecommunications offences

Proposed Subdivision C – Offences related to use of telecommunications

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

Proposed subsection 474.17(1)

Proposed section 474.17 will replace existing section 85ZE of the Crimes Act as the offence provision dealing with menacing, harassing or offensive use of carriage services. Proposed subsection 474.17(1) is drafted differently to existing subsection 85ZE(1) to ensure it is drafted consistently with the existing *Criminal Code* offence dealing with use of a postal or similar service to menace, harass or cause offence (section 471.12). The maximum penalty of the proposed offence will be increased from one to three years imprisonment to appropriately reflect the seriousness of such conduct. The maximum fine will be $19,800 for a natural person and $99,000 for a body corporate under the existing $110 value for a penalty unit in section 4AA of the Crimes Act, and the provisions for calculating maximum fines in section 4B of that Act.

Conclusion (cont)

The proposed offence is broader than existing subsection 85ZE(1) in relation to menacing or harassing use of a carriage service, because it removes the requirement that the recipient be in fact menaced or harassed and replaces it with an objective standard. The proposed offence provides that reasonable persons must regard the use of the carriage service, given all the circumstances, as menacing, harassing or offensive. This allows community standards and common sense to be imported into a decision on whether the conduct is in fact menacing, harassing or offensive.

The proposed offence also broadens the coverage of the existing offence in relation to use of a carriage service that is offensive. Existing subsection 85ZE(2) provides that the offence dealing with use of a carriage service in an offensive manner does not apply to 'Internet content', as defined in Schedule 5 to the *Broadcasting Services Act 1992* (Broadcasting Services Act). This exception has been removed under the proposed amendments, so that use of a carriage service, by way of the Internet, in an offensive manner will be covered by the offence.

The inclusion of 'whether by the method of use or the content of a communication, or both' is intended to clarify the type of use of a carriage service that the offence covers. 'The method of use' refers to the actual way the carriage service is used, rather than what is communicated during that use. The continual making of unwanted telephone calls to a particular person would fall into this category. 'The content of a communication' refers to what is communicated during the use of the carriage service, for example an email making threats may be considered menacing use of a carriage service. It is proposed to amend the parallel postal offence to clarify its coverage in the same way (see Item 7).

The existing offence in section 85ZE explicitly provides that the offending conduct, of using a carriage service, must be *intentional*. The reference to intention is not included in proposed section 474.17, because by application of the default fault elements of section 5.6 of the *Criminal Code* the fault element of intention will automatically apply to this physical element of conduct. This means that a person must intentionally use the carriage service to be found guilty of the offence.

The fact that the use of the carriage service occurs in a way that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive constitutes a circumstance in which the offending conduct must occur. By application of the default fault elements in section 5.6 of the *Criminal Code*, the fault element of *recklessness* will apply to a physical element of an offence that is a circumstance. 'Recklessness' as it applies to a circumstance is defined in section 5.4 of the *Criminal Code*.

Examples of the type of use of a carriage service the proposed offence may cover include use that would make a person apprehensive as to their safety or well-being or the safety of their property, use that encourages or incites violence, and use that vilifies persons on the basis of their race or religion.

Conclusion (cont)

Proposed subsection 474.17(2)

Proposed subsection 474.17(2) is to make it clear that use of a carriage service to menace, harass or cause offence to employees of the NRS provider, emergency call persons, employees of emergency service organisations and National Security Hotline call takers (see the explanations of the definitions of 'NRS provider', 'emergency call person' and 'emergency service organisation') is caught by the offence in proposed subsection 474.17(1). Abuse and harassment in these circumstances is particularly serious, because of the effect it may have on the people who provide these important services and the delays it creates in handling legitimate calls (see also the offence under proposed section 474.18).

……

Note: Further background information of the current situation can be obtained by a review of the following documents:

1. Reference 05 - AFP Web Site – Incidents of Harassment
2. Reference 06 - All Saints School News Letter – 25.05.2009
3. Reference 07 – Emonson V Trustees of the Christian Brothers
4. Reference 08 - Bullying and assault – Legal Cases & Compensation
5. Reference 09 - Update – Cyber-bullying cases put heat on Google & Facebook
6. Reference 10 - Parents welcome Brodie's Law on Bullying
7. Reference 11 - Nevett Ford Memo - OH & S- Workplace Bullying - May 2010

8. Appendix 01 - Commonwealth Criminal Code Act 1995

9. Appendix 02 - Extract from the Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill (No. 2) 2004 No.2.2004

10. Appendix 00 – Crimes legislation Amendment (Telecommunications Offences and Other Measures) Bill (no.2) 2004 – Explanatory Memorandum

Supplementary Recommendation # 6A (cont)

AFP Web Site – Incidents of Harassment

Reference 05:

The Australian Federal Police (AFP)

Use of Commonwealth Criminal Code Act 1995 for incidents of harassment

Timeframe: A Total of 7 Years (2004 – 2011)

Incident: A Total of Four (4) Incidents

Summary of Incidents:

The Australian Federal Police (AFP)

1. A **39-year-old** Glenroy **man**, will face four counts of allegations he harassed a federal member of parliament via phone and email.

2. A **45-year-old** Croydon Park **man** was interviewed and charged with seven counts of using a postal or similar service to menace, harass or cause offence

3. A **38-year-old** (Japanese national) **woman** making death threats against two Federal Court of Australia employees in Brisbane The AFP will also allege the woman harassed staff of the Federal Court with more than 150 phone calls

4. A **42-year-old** Gold Coast **man** arrested for allegations that he made a series of threatening telephone calls to Australian media organisations and the Australian High Commission in Singapore

Supplementary Recommendation # 6A (cont)

AFP Web Site – Incidents of Harassment (cont)

Reference 05: (cont)

AFP Web Site:- Media Centre

http://www.afp.gov.au/media-centre/news/afp/2011/march/warrant-executed-in-glenroy-victoria.aspx

Media Statement: Warrant executed in Glenroy, Victoria

Release Date: **Friday, March 11 2011, 04:41 PM**

The AFP can confirm it today executed a search warrant at a residential premises at Glenroy, Victoria. Police seized a computer and mobile telephone at the premises.

A **39-year-old** Glenroy man will be summonsed to appear in court at a later date, to face four counts of using a carriage service to menace, harass or cause offence, contrary to section 474.17 of the *Criminal Code Act 1995.*

He will face allegations he harassed a federal member of parliament via phone and email.

Supplementary Recommendation # 6A (cont)

AFP Web Site – Incidents of Harassment (cont)

Reference 05: (cont)

AFP Web Site:- Media Centre

http://www.afp.gov.au/media-centre/news/afp/2009/october/man-charged-for-sending-offensive-letters-to-family-members-of-soldiers.aspx

Man charged for sending offensive letters to family members of soldiers

Release Date: **Wednesday, October 21 2009, 08:30 AM**

A 45-year-old Croydon Park man has been charged in Sydney for sending offensive letters to family members of deceased Australian soldiers.

The man faces allegations that he sent harassing and offensive letters to family members of soldiers killed whilst serving in Afghanistan.

Search warrants were executed yesterday in the Sydney suburbs of Croydon Park, Campsie, and Green Valley by the Sydney Joint Counter Terrorism Team.

The man was interviewed and charged yesterday evening with seven counts of using a postal or similar service to menace, harass or cause offence, contrary to section 471.12 of the *Criminal Code Act 1995.*

He was granted conditional bail and will face Downing Centre Local Court on 10 November 2009.

The maximum penalty for these offences is two years imprisonment.

Supplementary Recommendation # 6A (cont)

AFP Web Site – Incidents of Harassment (cont)

Reference 05: (cont)

AFP Web Site:- Media Centre

http://www.afp.gov.au/media-centre/news/afp/2006/July/woman-charged-over-death-threats.aspx

Woman charged over death threats

Release Date: **Monday, July 31 2006, 12:00 AM**

Australian Federal Police (AFP) today charged a woman for making death threats against two Federal Court of Australia employees in Brisbane.

The AFP will allege the 38-year-old Japanese national, from the Brisbane suburb of St Lucia, made the death threats during phone calls.

The AFP will also allege the woman harassed staff of the Federal Court with more than 150 phone calls.

The woman was arrested in the Sydney CBD this morning.

She was charged with two counts of using a carriage service to make a threat to kill a person under Section 474.15 (1) of the *Criminal Code Act 1995* and one count of using a carriage service to menace or harass under Section 474.14(1).

The woman appeared before Sydney Central Local Court today and was refused bail. She will reappear in Sydney Central Local Court tomorrow morning, 1 August 2006.

Supplementary Recommendation # 6A (cont)

AFP Web Site – Incidents of Harassment (cont)

Reference 05: (cont)

AFP Web Site:- Media Centre

http://www.afp.gov.au/media-centre/news/afp/2004/September/man-arrested-for-threatening-phone-calls.aspx

Man arrested for threatening phone calls

Release Date: **Thursday, September 23 2004, 12:00 AM**

The Australian Federal Police (AFP) arrested a 42-year-old Gold Coast man last night following an investigation into allegations that he made a series of threatening telephone calls to Australian media organisations and the Australian High Commission in Singapore.

Police will allege that during September the man made calls threatening that terrorists attacks would occur against Australian interests in Malaysia and Singapore. It's alleged that the first call was made just days after the bombing of the Australian Embassy in Jakarta.

The matter was referred to the AFP following calls to the National Security Hotline.

The Brisbane man was arrested at his home in Labrador around 8pm following the execution of search warrants by Brisbane based Joint Counter Terrorism Team members. He has been charged with Intentionally Use a Carriage Service to Menace or Harass under the Commonwealth Crimes Act 1914. He was remanded in custody to appear in the Southport Magistrates Court today.

National Manager Counter Terrorism, Federal Agent Graham Ashton, said the arrest should serve as a warning that this type of activity will not be tolerated.

"We live in an environment where all threats of terrorist related activity are taken extremely seriously and police do not take lightly the risk of causing unnecessary public concern.

"The AFP's Joint Counter Terrorism team in Brisbane has acted swiftly in relation to this matter and the public can be assured that we will vigorously pursue all information potentially related to acts of terrorism," Federal Agent Ashton said.

Supplementary Recommendation # 6A (cont)

AFP Web Site – Incidents of Harassment (cont)

Reference 05: (cont)

AFP Web Site:- Media Centre

http://www.afp.gov.au/media-centre/facts-stats/online-child-sex-offences.aspx

Number of charges/arrests/offenders for online offences

Incident Type: Child Sex Offences – Online Child Sex Exploitation

Period: 1 January 2008 to 22 April 2010

Offence description	Charges	Arrests
ACT - possess child pornography	1	1
CTH - possess/control/produce/supply/obtain child pornography material	18	12
CTH - use carriage service to groom person under 16yo by person 18yo+	3	3
CTH - use carriage service to menace/harass/offend	**1**	**1**
CTH - use carriage service to procure person under 16yo by person 18yo+	2	1
CTH - using a carriage service for child abuse material	3	3
CTH - using a carriage service for child pornography material	210	160
CTH - using a carriage service to "groom" persons under 16 years of age	6	6
CTH - using a carriage service to procure persons under 16 years of age	2	2
NSW - have sexual intercourse with person aged 14 years or over & under 16 years	9	2
NSW - possess child pornography	39	22
NSW - produce, disseminate or possess child pornography	12	11
NT - possess indecent article/child pornography	2	2
QLD - knowingly possess child exploitation material	61	38
SA - possession of child pornography	5	5
SA - production or dissemination of child pornography	1	1
VIC - possess child pornography	32	32
	407	**302**

Supplementary Recommendation # 6A (cont)

School News Letter - Bullying & Cyberbullying Information

Reference 06: (cont)

All Saints Catholic Boys College – NSW - NEWSLETTER DATE - 25 May 2009

http://www.ascbc.nsw.edu.au/0-newsletters/2009/Term%202/090525.pdf

The following information is provided by Catholic Education Commission which was sources from The NSW Police and The Sydney Morning Herald 25 October 2007.

1. Getting into someone's account and using it to send abusive emails

Offence: Unlawful access to protected data, section 308H Crime Act NSW
Maximum penalty: two years

Offence: Intimidation, s.545AB Crime Act NSW
Maximum penalty: five years and/or $5,500

2. Taking a photo of X in the shower and sending it to everyone

Offence: Indecent Filming S.21G Summary Offences Act NSW
Maximum penalty: two years and/or $11,000

Offence: Use of Carriage Service to Menace, Harass or Cause Offence Criminal Code (Cwth) s.474.17
Maximum penalty: three years

3. Teasing, making fun of or spreading rumours about someone online

Offence: Intimidation s.545B Crimes Act NSW
Maximum penalty: five years and/or $5,500

4. Flaming (ridiculing people in chatrooms)

May give the aggrieved person grounds to commence civil action for defamation

5. Harassing someone or making threats electronically

Offence: Intimidation s.545AB Crimes Act NSW
Maximum penalty: five years and/or $5,500

Offence: Criminal code (Cwth) s.474.15 - Use of Carriage Service to Make a Threat
Maximum penalty: 10 years (for death threat) or seven years (for threat of serious harm)

Supplementary Recommendation # 6A (cont)

The need to have a better system can also be illustrated by reviewing some past legal cases Involving compensation and responsibility in Bullying and Cyberbullying.

Three example are as follows:

Reference 07:

Emonson v Trustees of the Christian Brothers

http://www.caslon.com.au/cyberbullyingnote8.htm

In 2001 18 year old Aaron Emonson was awarded **$60,000** by a Victorian County Court after the jury heard that he had endured three years of bullying at his former school, St Patrick's College, Ballarat.

Emonson's solicitor noted that bullying was often a daily occurrence and violent. Emonson had been belted on the arm with a piece of wood in a woodwork class; there'd been another occasion where he'd been hosed down with a water hose, and had been required to remain at school for the balance of that day in saturated clothing; there'd been another incident where he had been choked with a length of material from carpet cord and throughout that period the parents had made various requests of the school to deal with it and the response was far less than adequate. ...

He had not progressed well at school and as a result he ceased his schooling at the end of Year 10.

One of the alleged bullies is reported as stating that Emonson's treatment was no different to what most St Patrick's students experienced. "Everyone was doing it to everyone ... We weren't singling Aaron out."

The court found that the school had breached its duty of care, having been recurrently alerted by Emonson's parents. Emonson sued the school for physical and mental injuries caused by the bullying.

The hearing featured an email by a St Patrick's teacher in 1998 detailing problems with bullying in the school and complaining of difficulties in addressing that abuse.

Supplementary Recommendation # 6A (cont)

Reference 08:

Bullying and assault – Legal Cases & Compensation

http://www.lawhandbook.org.au/handbook/ch06s03s03.php#

Reeta Verma, Lecturer in Law, La Trobe University, Melbourne

Bullying is described as a "repeated attack, physical, psychological, social or verbal in nature, by those in a position of power... with the intention of causing distress for their own gain or satisfaction". Bullying may involve direct physical or verbal abuse or indirect acts that are designed to harm the person's social reputation and/or cause humiliation and distress. It can be carried out with the aid of modern technologies such as the Internet (i.e. via "My Space") and mobile phones. This form of bullying is known as "cyber bullying").

Some of the acts of bullying involve:

- intentional injury or physical assault such as kicking, hitting, pushing, punching or damaging property;
- psychological assault such as teasing, name-calling, taunting, rumour spreading or ostracism;
- continued harassment of a student by other students through email, text messages or chat rooms with a aim of insulting and ridiculing others; or
- direct or indirect harassment such as sexual abuse, racial or homosexual vilification.

Unlawful discrimination may also amount to bullying (*see*: Chapter 17 Discrimination).

Schools and teachers have a legal responsibility to deal with bullying behaviour of pupils and to provide support both for the victim and the *perpetrator*. If they know or ought to know that a particular pupil is being bullied and fail to take reasonable steps to stop bullying behaviour, they may be liable in *negligence*. A pupil who suffers physical injuries due to the bullying of others may bring an action against the school or relevant education authority for compensation for his/her injuries. Christopher Tsakalos' case in New South Wales in April 1997 indicates that homophobic bullying in school may render the relevant education authority liable in negligence and/or for unlawful discrimination.

In *Gregory v State of New South Wales* [2009] NSWSC 559, the New South Wales Supreme Court awarded almost **$470,000** in *damages* to a victim of bullying. The victim was regularly called "sterile", "faggot", "paedophile" and "Nazi" by his peers and banned him from entering the Year 12 common room or sitting on the Year 12 lawn. The court accepted that the teachers did nothing to deal with the victim's complaints and had not intervened to protect him from being socially ostracised.

Supplementary Recommendation # 6A (cont)

Bullying and assault – Legal Cases & Compensation (cont)

Reference 08: (cont)

In *Warren v Haines* (1987) Aust Torts Reports 80-115, where a known bully picked up a 15-year-old girl and dropped her on her tail bone during morning recess in an unsupervised area in school, the *plaintiff* succeeded in her action against her school in the lower court. However, on *appeal*, the decision was overturned. While the court accepted that the school had a duty to provide adequate supervision to students, there was sufficient evidence to prove that the injury to the student occurred within a very short span of time where there was no opportunity for the teacher to intervene.

There is no legislation at either state or Commonwealth level that specifically prohibits bullying behaviour. However, the *Equal Opportunity Act 1995* (Vic), *Racial Discrimination Act 1975* (Cth), *Sex Discrimination Act 1984* (Cth), *Australian Human Rights Commission Act 1986* (Cth), *Disability Discrimination Act 1992* (Cth) and *Occupational Health and Safety Act 2004* (Vic) may each impose legal obligations on schools and teachers to deal with the problem of bullying.

Since January 2000, the Victorian government has urged all schools (particularly state schools) to develop programs to prevent school bullying. The school's code of conduct must include anti-harassment and anti-bullying strategies, and incidents of bullying must be responded to promptly. The *Framework for Student Support Services in Victorian Government Schools* suggests that all schools should develop and implement programs that focus on preventative and early intervention strategies to combat bullying and harassment

The *National Safe Schools Framework* (2003) and its Implementation Manual set out ways to deal with bullying, harassment and violent behaviour in schools. The Framework is a collaborative effort by Commonwealth, state and territory government and non-government school authorities in consultation with other key stakeholders in the safety and wellbeing of children in Australian schools. The Implementation Manual and a Resource Pack are available to download online from the Department of Education, Employment and Workplace Relations website at: www.deewr.gov.au.

All Victorian government schools have also adopted new strategies to prevent and address cyber bullying. Information about cyberbullying and help for young people is available from the Cybersmart Online Helpline service.

Since schools owe a direct (non-delegable) legal duty under the principles of negligence to protect the wellbeing of pupils in their care, school authorities may be liable to pay damages to pupils if they suffer injury through an act of bullying. Recent court decisions indicate that a victim of bullying who suffers emotional or psychological injury or long-term effects is able to recover damages from the relevant school authority (*see*: *Gregory v State of New South Wales* [2009] NSWSC 559, above).

Supplementary Recommendation # 6A (cont)

Bullying and assault – Legal Cases & Compensation (cont)

Reference 08: (cont)

Some out of court settlements and unreported cases (*see*: *Sharp's Case* in the UK: *Sharp v London Borough of Richmond-upon-Thames* (unreported, 1997)) also indicate that victims of considerably harsh bullying may be able to recover damages for the physical, psychological and enduring effects of bullying.

Victims of bullying may also bring an action against the perpetrator for battery and assault.

Assault consists in intentionally creating in another person an apprehension of immediate harmful or offensive contact. If the threat is carried out, the whole incident is... described as an 'assault and battery'." (J.G.Flemings, 1998, *The Law of Torts*, 9th edn., LBC Information Services, Sydney, p. 31.)

Offensive and insulting behaviour such as spitting in another person's face, pulling someone's hair, planting a kiss on someone without that person's *consent*, seizing something from another person's hand, pouring water on someone, or pulling a chair from under a person so that he or she falls on the ground, may amount to bullying as well as battery. In *Lisa Eskinazi v State of Victoria* (unreported, VCC, 20 June 2003), the Victorian County Court awarded **$76,000** to a victim of bullying who was frequently called names (such as "hooker", "whore", or "fat pig") and beaten up by her fellow students at the school.

Assault and battery are civil wrongs as well as crimes under Australian law. Pupils above the age of 10 may face criminal proceedings in the Magistrates' Court for assault. Upon conviction, the Magistrate may direct that the perpetrator pay compensation to the victim or person aggrieved for injury or loss.

Kids Help Line in Australia provides telephone counselling for the victims of bullying and is available 24 hours a day, seven days a week.

Kids Help Line
Counselling line: 1800 551 800 1800 551 800 (24 hours, 7 days, toll free)
Web: www.kidshelp.com.au
Web counselling times (Victoria): 3 pm–9 pm Mon-Fri; 10 am–8 pm Sat-Sun

Supplementary Recommendation # 6A (cont)

Reference 09: (cont)

UPDATE 1-Cyber-bullying cases put heat on Google, Facebook

http://www.reuters.com/article/2010/03/09/internet-bullying-idUSN0820019920100309

Mon Mar 8, 2010 7:13pm EST

* Google in Italy, Facebook in Australia see cyber-bullies

* Legal issues may not be a concern for Web businesses

* Social pressures may force more accountability though (

By Dan Whitcomb

LOS ANGELES, March 9 (Reuters) - The Internet was built on freedom of expression. Society wants someone held accountable when that freedom is abused. And major Internet companies like Google and Facebook are finding themselves caught between those ideals.

Although Google, Facebook and their rivals have enjoyed a relatively "safe harbor" from prosecution over user-generated content in the United States and Europe, they face a public that increasingly is more inclined to blame them for cyber-bullying and other online transgressions.

Such may have been the case when three Google (GOOG.O) executives were convicted in Milan, Italy on Feb. 24 over a bullying video posted on the site -- a verdict greeted with horror by online activists, who fear it could open the gates to such prosecutions and ultimately destroy the Internet itself.

Journalist Jeff Jarvis suggested on his influential BuzzMachine blog that the Italian court, which found Google executives guilty of violating the privacy of an autistic boy who was taunted in the video, was essentially requiring websites to review everything posted on them.

"The practical implication of that, of course, is that no one will let anyone put anything online because the risk is too great," Jarvis wrote. "I wouldn't let you post anything here. My ISP (Internet Service Provider) wouldn't let me post anything on its services. And that kills the Internet."

A seemingly stunned Chris Thompson, writing for Slate, said simply: "The mind reels at this medieval verdict."

UPDATE 1-Cyber-bullying cases put heat on Google, Facebook (cont)

Reference 09: (cont)

'POLICEMEN OF THE INTERNET'

And Matt Sucherman, a Google vice president and general counsel, wrote in a blog post that the company was "deeply troubled" by the case, saying it "attacks the very principles of freedom on which the Internet is built."

Legal experts have been more sanguine, saying the verdict in Milan will most likely end up an outlier -- unable to stand the scrutiny even of the Italian appeals courts, never mind setting legal precedents elsewhere.

But in sentencing the executives to six-month suspended jail terms, the court may have seized on a growing desire to hold Internet companies responsible for the content posted by users.

"I actually think that this is probably not a watershed moment because the Google convictions violate European law and ultimately they will be overturned," said John Morris, general counsel for the Washington, D.C.-based Center for Democracy and Technology.

"Having said that, yes we are quite worried about the trend in other countries to suggest Internet service providers and Web sites should be the policemen of the Internet," Morris said.

If the trend takes hold, it could put the companies on the defensive, forcing them to spend more time defending such cases or fending off calls to restrict content in some way.

China polices the web and demands cooperation from web companies, while the United States has stuck up for Internet freedom in the face of censorship by more repressive governments.

But social pressure often comes from the ground up, as Facebook recently found out in Australia.

In that case Facebook pages set up in tribute to two children murdered in February, 8-year-old Trinity Bates and 12-year-old Elliott Fletcher, were quickly covered with obscenities and pornography, prompting calls for the social network to be more accountable for its content.

To have these things happen to Facebook pages set up for the sole purpose of helping these communities pay tribute to young lives lost in the most horrible ways

UPDATE 1-Cyber-bullying cases put heat on Google, Facebook (cont)

Reference 09: (cont)

adds to the grief already being experienced," Queensland Premier Ann Bligh wrote to Facebook founder and CEO Mark Zuckerberg in a letter released to the Australian media.

THE 'MYSPACE SUICIDE'

"I seek your advice about whether Facebook can do anything to prevent a recurrence of these types of sickening incidents," Bligh said in the letter.

A Facebook spokeswoman responded that the popular social network, which has more than 400 million users worldwide, had rules to check content and that any reports of hate or threats would be quickly removed.

"Facebook is highly self-regulating and users can and do report content that they find questionable or offensive," the spokeswoman, Debbie Frost, said.

Calls for prosecution of cyber-bullying first reached a peak with the case of a suburban mother accused of driving a love-lorn 13-year-old girl, Megan Meier, to suicide in 2006 by tormenting her with a fake MySpace persona.

Lori Drew, the mother of a girl with whom Meir had quarreled, was found guilty of misdemeanor federal charges in a case dubbed the "MySpace Suicide" in the U.S. media, but a judge later dismissed her conviction on the grounds that the prosecution was selective the law unconstitutionally vague.

But Meier's death and a series of child exploitation cases linked to News Corp's (NWSA.O) MySpace brought pressure on the site to increase its security measures and may have cost it in its apparently losing rivalry with Facebook for social network dominance.

Such issues point to the business risks for the likes of Google and Facebook as they seek to reconcile demands for accountability with the impossibility of monitoring everything posted on their sites.

"We are a society that expects companies and people of authority to take responsibility, not only for their own actions but for the actions of those beneath them," said Karen North, director of the Annenberg Program on Online Communities at the University of Southern California.

"The difficulty is, we've created an Internet culture where people are invited to put up content, but the responsibility falls in both directions," North said. "(On the Internet) we all share the responsibility to monitor the content that we find and for our societal standards to be maintained." (Editing by Peter Henderson and Cynthia Osterman)

Supplementary Recommendation # 6A (cont)

Reference 10: - Extract – 7 News – Workplace Bullying

http://au.news.yahoo.com/latest/a/-/latest/9137870/new-laws-to-curb-bullying/

Parents welcome 'Brodie's Law' on bullying

By Xavier La Canna, AAP

April 5, 2011, 4:35 pm

The parents of a teenager who killed herself after being bullied by workmates have backed plans for tough new anti-bullying laws, but say authorities still need to do more.

Damian and Rae Panlock's daughter Brodie was taunted incessantly by workmates while a waitress at a Melbourne cafe before she jumped to her death in 2006, aged 19.

Her death came after she was abused by colleagues who poured beer and oil on her, spat on her and offered her rat poison after an earlier failed suicide attempt.

Brodie's three tormentors, Nicholas Smallwood, Rhys MacAlpine and Gabriel Toomey, were convicted under Occupational Health and Safety laws and fined a total of $85,000, while the cafe owner Marc Luis Da Cruz and his company were ordered to pay $250,000.

But, in accordance with the law at the time, none were jailed.

On the day they were fined last year, Mr Panlock said the law should be changed to allow a custodial sentence.

On Tuesday, he and his wife welcomed changes to stalking laws to be introduced into Victorian parliament this week under which bullies will face up to 10 years' jail.

Under the new laws, dubbed "Brodie's Law", people who engage in cyber bullying could also face criminal charges.

Mr Panlock said he looked forward to the amendments becoming law but unions and WorkSafe needed to do more.

"Just get the unions into it, with WorkSafe, and find out what they are doing, face to face, not an ad in the paper," Mr Panlock said.

"It is the only thing I can think of as a solution."

Rae Panlock said she hoped the new laws meant workplace bullying would be taken more seriously.

"If you think someone is a little bit down, maybe they just need someone to talk to, and that goes for all the corporate bosses out there listening," she told reporters.

Supplementary Recommendation # 6A (cont)

Victorian Attorney-General Robert Clark said the new laws would help protect workers from actions that would cause physical or mental harm.

Nevitt Ford Memo – Workplace Bullying – May 2010

Reference 11:

Extract:

Occupational Health and Safety in Victoria

- **Safe Working Environment**
- **Workplace Bullying**

Introduction

In Victoria, occupational health and safety in the workplace is principally regulated by the Occupational Health and Safety Act 2004 (Vic) ("the Act") and the Occupational Health and Safety Regulations 2007 (Vic).

The Act contains the key principles, duties and rights in relation to occupational health and safety. The general nature of the duties imposed by the Act means that they cover a very wide variety of circumstances.

The prevention arm of the Victorian WorkCover Authority, WorkSafe Victoria, is the regulatory agency which administers and enforces occupational health and safety legislation in Victorian workplaces. WorkSafe Victoria may prosecute organisations and individuals that breach the Act and the duties contained therein.

The Duties

The principal duty imposed on employers under the Act is to, so far as reasonably practicable, provide and maintain for employees of the employer a working environment that is safe and without risks to health.

'Employee' is defined to include independent contractors engaged by employers as well as the employees of any such contractors.

The definition of 'health' in the Act includes psychological health.

In discharging their principal duty towards employees, employers must be able to demonstrate that they have maintained the workplace in a safe manner; provided systems of work that are safe and without health risks; ensured the safe use, handling, storage and

transport of plant substances; and provided adequate facilities, information, instruction and training to enable employees to carry out tasks safely.

Further, employers must, so far as reasonably practicable, monitor the health of employees, and the conditions of their workplace, and keep records about employee health and safety.

The obligations and duties of employers encompass the need to have effective systems in place to eliminate, and deal with, workplace bullying and violence.

> The Court of Appeal described the content of duties under the Act in *DPP v Commercial Industrial Construction Group Pty Ltd* [2006] VSCA 181 at [48]-[49] as follows:
>
> … the formal adoption of a satisfactory safety management system will not have the beneficial effects intended unless it is accompanied by the employer's active implementation of the system in the workplace. The employer's duty will not be discharged by simply creating a safe system of work. The obligation requires the employer to ensure "that procedures and instructions are actively and positively complied with by employees". Not only must employees be appropriately trained but there must be ongoing supervision and compliance audits, to ensure that the system is being applied in practice. Employee compliance with the safe system of work must be constantly monitored by the employer.
>
> [49] An employer should recognise that it is common experience that human error will be encountered in the workplace. Error can range from inadvertence, inattention or haste through foolish disregard of personal safety to deliberate non-compliance with the prescribed safe system of work. In *R v Australian Char Pty Ltd* and *DPP v Amcor Packaging Pty Ltd*, this Court has referred with approval to the observations of Harper. J in *Holmes v R.E. Spence & Co Pty Ltd* that an employer's responsibility for the safety of its workers will not be discharged unless the employer takes "an active imaginative and flexible approach to potential dangers in the knowledge that human frailty is an ever present reality".

Under the Act an employee has a duty to take reasonable care for his or her own health and safety and for the health and safety of anyone else who may be affected by his or her acts or omissions at the workplace, and to cooperate with his or her employer with respect to any action taken by the employer to comply with any requirements imposed by the Act.

Supplementary Recommendation # 6A (cont)

Nevitt Ford Memo – Workplace Bullying – May 2010 (cont)

Reference 11: (con)

Workplace Bullying

Recent cases in Victoria clearly illustrate that workplace bullying can lead to prosecutions against employers, company officers and/or employees for conduct falling below the standard required and alleged breaches of the duties imposed under the Act.

While bullying currently has no legal definition, WorkSafe Victoria and other regulatory organisations have defined workplace bullying as “repeated unreasonable behaviour directed towards an employee or group of employees that creates a risk to health and safety”.

A broad range of behaviours can be bullying, and these behaviours can be direct or indirect.

Examples of direct forms of bullying include:
• verbal abuse.
• putting someone down.
• spreading rumours or innuendo about someone.
• interfering with someone’s personal property or work equipment

Examples of indirect bullying include:
• unjustified criticism or complaints.
• deliberately excluding someone from workplace activities.
• deliberately denying access to information or other resources.
• withholding information that is vital for effective work performance.
• setting tasks that are unreasonably above or below a worker’s ability.
• deliberately changing work arrangements, such as rosters and leave, to inconvenience a particular worker or workers.
• setting timelines that are very difficult to achieve.
• excessive scrutiny at work

Those employers, company officers and/or employees who are prosecuted may be liable for significant penalties and costs orders, as well as the resultant adverse publicity.

In addition employers can be liable to pay compensation to victims of bullying.

Recently the Melbourne Magistrates' Court imposed fines totaling $335,000.00 in relation to bullying conduct which was in breach of the Act.

Supplementary Recommendation # 6A (cont)

Nevitt Ford Memo – Workplace Bullying – May 2010 (cont)

Reference 11: (con)

The case focused on a café in Hawthorn and the bullying of a teenage waitress who allegedly committed suicide as a result of the harassment. The matter received unprecedented media attention for a bullying prosecution in Victoria.

Charges were brought against three individual employees, the company which owned the café, and also the sole director of the company.

An earlier coronial inquest into the death of the teenage waitress had implicated the individual employees in the physical and psychological bullying which occurred at the café.

The defendants pleaded guilty to the charges.

At the Plea Hearing the Court heard that between 1 June 2005 and 20 September 2006 the teenage waitress was subjected to a range of repeated direct and indirect physical and nonphysical bullying behaviour by the individual employees.

The bullying acts allegedly included verbal taunts, criticisms, name-calling, and physical Interference.

In sentencing the defendants, the Magistrate described the atmosphere at the café as almost “poisonous”, and found that the café was aware and had “tacitly approved” of the “persistent and vicious” bullying of the teenage waitress.

Also relevant was the fact that the employer provided no induction program/system for new employees and had no policies or procedures in place to educate employees in respect of appropriate workplace behaviour and workplace bullying.

The company was fined a total of **$220,000.00** for failing to provide and maintain a safe workplace and for failing to properly train and supervise employees. The company's director was fined a total of $30,000.00 and convicted of the same offences.

The three individual employees were fined **$45,000.00, $30,000.00** and **$10,000.00** for failing to take care for the health and safety of a fellow employee.

In addition to the fines, each of the defendants received costs orders of between $1,500.00 and $2,500.00.