ACCC Digital Inquiry

Submission: dated 15th February 2019
Submitter: Rod Harris, Company Director.

Topic

Preventing and Policing Cybercrime (Cyberbullying) in Australia

This submission is focused specifically on Cyberbullying, yet the subject matter aligns with other types of cybercrime

Contents

1. Problems to be rectified — Page 2
2. Cyberbullying case study (business & personal victims) — Page 5
3. Considerations re Resolution Options (Paragraph A&B is essential reading) — Page 8
4. Submitter introduction and preamble — Page 10
5. Resolution Submissions
   - (a) Submitter introduction — Page 10
   - (b) Establish a Primary Cybercrime Agency — Page 11
   - (c) Establish an Australian Cyber Digital Registry — Page 12
   - (d) Review and Implement/Upgrade Federal Cyber Legislation — Page 13
   - (e) Set new rules of engagement with Cyber Providers & Review Sites — Page 13
   - (f) Youth education — Page 14

Dictionary

ACORN	**Australian Cybercrime Online Reporting Network**
ASBFEO	**Australian Small Business & Family Enterprise Ombudsman**
Cyberbullying	**For sake of narrative ease, include Cyberstalking with Cyberbullying.**
Govt Authorities	**State or Federal Government Agencies and Departments**

Preventing and Policing Cybercrime (cyberbullying) in Australia

1. Problems to be rectified (updated 15/02/19)

At present, Australia does not have efficient and effective policies, systems, or legislation, to adequately:

(a) Prevent Cybercrime (Cyberbullying) being committed in Australia or by Australian Residents.

(b) Assist Australians to report on Cybercrime (Cyberbullying).

(c) Identify Cybercrime (Cyberbullying) Offenders and therefore share details with law practitioners.

(d) Apprehend and Charge Cybercrime (Cyberbullying) Offenders.

There is extensive evidence available from multiple credible sources within Australia and internationally, which demonstrates:

(a) An increasing number of Cyberbullying recipients committing suicide per annum, across all ages.

(b) An upsurge of Cyberbullying recipients suffering extreme financial hardship & health issues (ongoing).

(c) A skyrocketing upsurge in adults and businesses being negatively affected as Cyberbully victims.

(d) Unabated Cyberbullying is increasingly burdening the well-being of all Australian communities.

(e) Excessive costs are being incurred to operate Govt. Agencies that are widely unsuccessful in preventing and combating the rise in Cyberbullying because of the chronic lack of contemporary laws, policies and rules of engagement with online social platforms and interactive public apps and websites.

(f) Agency personnel stressed from being unable to curb Cyberbullying under current laws, policies/rules.

(g) Numerous requests by experts for the introduction of contemporary Cyberbullying laws, policies, and rules of engagement are being irresponsibly declined and/or deflected.

(h) When considering the many years of obvious upward trends of unabated cyberbullying in Australia, the Government could be accused of <u>inadvertently condoning</u> Cyberbullying for the sole benefits of the offenders. This is because there is no evidence to consumers or businesses to demonstrate the Government has made any material effort over many years to proactively implement better measures to prevent or apprehend Cyberbullies or to improve the support to victims!

Cyberbullying effects on Adults and Businesses

This author has been unable to locate "official" research findings into the damage caused by cyberbullying upon Australian businesses as victims, yet all the cyber experts recently interviewed concur:

- Cyberbullying against businesses is already significant and rising unabated, in line with the increased take-up and use of general cyber applications and e-commerce marketing/social platforms. <u>The current collective cost to Australian businesses in attempting to mitigate Cyberbullying attacks (unsuccessfully counter-defending) and the associated losses in productivity is estimated to be in the region of **A$10 billion per annum and rising.**</u>
- The rising severity of Cyberbullying will force more legitimate businesses to downsize and collapse.
- Cyberbullying upon adults and business managers has resulted in adult suicides, increased physical assaults and probably murders, in addition to inflicting significant hardship for all other associated stakeholders.
- There is some legislation to protect youth from Cyberbullying but not for adults or businesses.
- The Australian Govt is running 7-10 years behind in making any headway towards resolving the issues.

Preventing and Policing Cybercrime (cyberbullying) in Australia

Here are two pages with extracts from a combination of various Cyberbullying articles and online reports supplied by co-contributors to this submission. The content relates mostly to youth statistics, but the fundamental principles of "bullying" (cause and effect involving offender/recipient) does not necessarily change with age, demographics or gender. If this writer has inadvertently breached any copyright laws by sharing this information, a sincere apology is given along with an invitation for those concerned to make contact. Otherwise, it is suggested that readers should please be respectful if intending to re-distribute this information.

(i) While better connecting the world and democratizing information, **the internet has also allowed individuals to hide behind masks of anonymity.** The "faceless evil" of the internet is a growing threat when it comes cyberbullying. Despite a more recent ramping up of awareness campaigns, cyberbullying facts and statistics indicate the problem is not going away anytime soon.

(j) Cyberbullying has risen 32 % in last decade, and still rising.

(k) Cyberbullying is the cause of at least three suicides per week in Australia for youth, and highest cause of death for Australian youth between 5-17 years old.

(l) **According to Anadolu (?) news agency, every year around 750 Australian teens between 13-17 commit suicide because of cyber bullying.** Öztürk Yıldız, a former mayor of Turkish descent for Moreland in Melbourne stated **"Some of our children who are victims of cyber bullying have no idea how to handle and deal with the abuse. Sadly, a lot of them give way under the pressure and commit suicide. The rate of suicide is the highest here [in Australia],"** Yıldız also said the Internet's pervasiveness caused teens to be exposed to abuse at all times and that there was no barrier to protect them online.

(m) Possibly up to 10 suicide deaths per week in Australia across all ages due to Cyberbullying.

(n) Ginger Gorman is an award-winning social-justice journalist based in Canberra, "The nationally representative polling I commissioned from **the Australia Institute found the cost of cyberhate and online harassment to the Australian economy is $3.7 billion. That figure only counts lost income and medical expenses — so the real cost is far greater".** The survey found 44 per cent of women and 34 per cent of men have experienced one or more forms of online harassment. **This is equivalent to 8.8 million Australians experiencing harassment online.**

(o) In 2018, Rod Harris, a Company Director in Australia whose business was viciously attacked by a Cyberbully, (competitor) has calculated the overall cost to Australian businesses in counter defending cyberbullying and lost productivity is approximately $10 billion and will continue to rise by 10-20% per annum, if left unabated.

(p) A survey of 2,360 Australian parents conducted by the Office of the eSafety Commissioner in 2016 found that 29% of youth had been bullied online

(q) It appears bullying has effects beyond self-harm. Javelin Research finds that children who are bullied are 9 times more likely to be the victims of identity fraud as well.

(r) A 2007 Pew Research study found 32 percent of teens have been victims of cyberbullying. A decade later a study by the Cyberbullying Research Center found numbers were almost unchanged. By 2016, just under 34 percent of teens reported they were victims of cyberbullying. **Meanwhile, the USA National Crime Prevention Council puts that number much higher, at 43 percent.** According to the Cyberbullying Research Center, which has been collecting data since 2002, the extent of Cyberbullying has doubled since 2007, up from just 18 percent. **Disagreements in statistics and data gathering methods aside, the increase in cyberbullying is real.**

(s) Google Trends data indicates much more attention is focused on cyberbullying than ever before. The volume of searches for "cyberbullying" increased threefold since 2004: Source: Google Trends. **Research presented at the 2017 Paediatric Academic Societies Meeting revealed the number of children admitted to hospitals for attempted suicide or expressing suicidal thoughts doubled between 2008 and 2015. Much of the rise is linked to an increase in cyberbullying. (Source: CNN). More teen suicides are also now attributed in some way to cyberbullying than ever before.**

Continued next page…

(t) **Data from numerous studies indicate social media is now the favoured medium for cyberbullies.** Other formats are still in use, such as text messaging and internet forums such as Reddit. Recent stats include: 21% reported that they were affected by online rumours. (Source: Cyberbullying Research Centre). **7 percent of middle school and high school students had a mean or hurtful web page created about them.** (Source: Cyberbullying Research Centre) In a survey of parents and adults across Asia, 79 percent reported that either their child or a child they know had been threatened with physical harm while playing online games. (Source: Telenor)

(u) Cyberbullying often occurs on Facebook or through text messages. (Source: American Journal of Public Health)

(v) The long-lasting impacts of cyberbullying are difficult to ignore. Alongside the increasing number of suicides directly linked to cyberbullying, other consequences arise for bullying victims. One 2016 study discovered that bullying victims are more likely to engage in substance abuse and nonviolent delinquency. Other cyberbullying research indicates that cyberbullying carries over into how students feel about their physical safety at school. Additionally, cyberbullying can negatively impact a student's' overall success by cutting into their motivation.

(w) Key research on the impact of cyberbullying includes the following: As of August 2016, 16.9 percent of middle and high school students identified themselves as cyberbully victims. (Source: Cyberbullying Research Centre), Among adolescents, 36.7 percent of female respondents stated they'd be the victim of cyberbullying at some point in their lifetime, compared to 30.5 percent of boys. (Source: Cyberbullying Research Centre), Most online behaviours and threats to well-being are mirrored in the offline world (Source: Perspectives on Psychological Science), 34 percent of students claimed to have been bullied online at least once in their lifetime. (Source: Florida Atlantic University), 17 percent of students explained that they'd been bullied sometime within the past 30 days. (Source: Florida Atlantic University), Roughly 64 percent of students who claimed to have been cyberbullied explained that it negatively impacted both their feelings of safety and ability to learn at school. (Source: Florida Atlantic University),

(x) Source: CDC: According to a decade-long Florida Atlantic University study of 20,000 middle and high school students, 70 percent of students said that someone spread rumours about them online. (Source: Florida Atlantic University), More than one in 10 students (12 percent) admitted to cyberbullying someone else at least once. (Source: Florida Atlantic University), Girls are more likely to be victims of cybercrime (except for those bullied within the last 30 days), while boys are more likely to be cyberbullies. (Source: Florida Atlantic University), There are significant cross-overs between in-person and online bullying. 83 percent of students who had been bullied online in the last 30 days had also been bullied at school. Meanwhile, 69 percent of students who admitted to bullying others online had also recently bullied others at school. (Source: Florida Atlantic University), Adolescents who engaged in cyberbullying were more likely to be perceived as "popular" by their peers. (Source: Journal of Early Adolescence), A need for broader-more reaching and open research

(y) Most teenagers (over 80 percent) now use a mobile device regularly, opening them up to new avenues for bullying. (Source: Bullying Statistics), Half of all young adults have experienced cyberbullying in some form. A further 10-20 percent reported experiencing it regularly. (Source: Bullying Statistics),

(z) Cyberbullying leads to more suicidal thoughts than traditional bullying. (Source JAMA Paediatrics)

Source: NoBullying.com: **Over half of all teens who use social media have witnessed cyberbullying. (),**

Source: NoBullying.com: The website Nobullying.com recorded over 9.3 million visits in 2016 from people seeking help with bullying, cyberbullying and online safety. **Almost 43 percent of kids have been cyberbullying victims. Around 25 percent have been victimized more than once.**

Source: DoSomething.org: A UK survey of more than 10,000 youths discovered that 69 percent reported doing something about abusive online behaviour directed toward another person. **The same U.K. survey also discovered that 71 percent of young adults believe social networks do not do enough to prevent cyberbullying.**

Source: DoSomething.org: **Over 50 percent of surveyed teens say they never confide in their parents after being victimized by cyberbullies. (Source: NoBullying.com)**

Continued next page…

2. Cyberbullying Case Study (Affecting Business & Personal victims) Dated 15/02/19

For confidentiality reasons, the real name of the business has been replaced by "XYZ".

XYZ is an established ICT Service Provider, based in QLD Australia. It is an employer of choice, with consistent net positive client port-in statistics and has never been the recipient of a demand from the likes of ACCC, Fair Trading, Fair work, or TIO etc, spanning decades. Readers can safely assume **XYZ** and its staff always act professionally in every aspect of their business activities.

In December 2018, an **XYZ** employee, by sheer chance, noticed that a person using multiple fake IDs had posted false and heinous information on multiple web sites and online social platforms (including the upload of bogus Facebook pages), with the intent to cause extreme damage and harm to the reputation of **XYZ**, its owner, and its employees. The goal of the Cyberbully was to force the company into liquidation.

XYZ noticed that the Cyberbully had commenced uploading the fake information in **October 2018**, yet not one site had contacted **XYZ** to inform or clarify the authenticity of the (fake and false) contents. The only semi-exception was Google Review, who took quite some time to notify **XYZ** of the negative reviews, which **XYZ** identified as also being fake/false, as uploaded by the cyberbully. Unfortunately, customers who witnessed the reviews would have assumed them to be legitimate, and it resulted in lost business for **XYZ**.

XYZ staff observed the Cyberbully uploading new bogus content online daily and was he stalking **XYZ** customers. Sites utilised by the Cyberbully included Facebook, Google and Business Directory web sites, and he also uploaded fake/false reviews on non-moderated employee review websites.

XYZ staff believe that the prime Cyberbully suspect was a former disruptive employee and would-be business competitor, who was employed by **XYZ** for a short period in 2018 and finished up just before the cyberbullying commenced. Prior to ceasing employment with **XYZ**, the suspect had mentioned to **XYZ** employees on several occasions that they wanted to "take over the company" and he told staff that "the company would go broke and that he would be willing to step in and takeover". **XYZ** staff ignored these comments at the time because they were aware that ordinarily **XYZ** was a solid and viable company, experiencing consistent and positive client growth, and that the **XYZ** owner had previously declined the suspects advances to take a shareholding in the company.

The offender's content was extremely distressing to **XYZ** employees and easily visible to the cyber public.

The offending content included the following definitions of cyberbullying as per the ACORN* website:

- Posting hurtful messages, images or videos online. Repeatedly sending unwanted messages online.
- Sending abusive texts, intimidating others online. Creating hurtful fake social networking pages.
- Nasty online gossip and chat, which is discriminatory, intimidating, intended to cause hurt and make people fear for their safety.

The Cyberbully's fake and false Facebook pages and other online posts included personal threats to **XYZ** personnel, misappropriated photos that identified **XYZ** employees and on multiple occasions included a doctored photo of an **XYZ** employee behind prison bars, which was extremely inappropriate because the employee had never had reason to set foot in a prison! **XYZ** is of the opinion that the bogus uploaded content also breached copyright, Trademark IP laws, the Privacy Act and Federal Telecommunications Act.

The offensive, disgusting and highly defamatory uploaded content by the Cyberbully had a terrible impact on the health and well-being of **XYZ** employees, giving rise to 50% of employees taking sick due to depression and anxiety.

By Mid-February 2019, some four months after the cyberbullying commenced, **XYZ** calculated a loss of $200,000 revenue (increasing weekly), and the distraction of continuous uploaded bogus content was having a terrible effect on the business's productivity and business development plan. **XYZ** had to cancel strategic product launches, which caused further long-term loss of annuity income and created negativity with upline suppliers and other Stakeholders. Additionally, the Cyberbullying prevented **XYZ** from employing an additional four staff members because **XYZ** management were concerned that they too may become victims in what had become a very challenging working environment!

XYZ became aware of Customers who saw the Cyberbully's fake posts/reviews and purchased elsewhere, and became aware potential employees sought positions elsewhere after reading false employee reviews.

The Road to nowhere

This was the first time **XYZ** and its employees had been exposed to cyberbullying or any other form of cybercrime and were unsure of what to do about it, or which professional agency to contact for help. And it took **XYZ** several weeks to realise that the category name for the cyber harassment was "Cyberbullying".

Upon the day of discovering the Cyberbully fake and false posts (Dec 2018), the **XYZ** business owner commenced contacting numerous Govt. Agencies and Business Advocacy Support Groups for support and to date **(Feb 2019)**, nothing of consequence has eventuated. The agencies **XYZ** contacted did include: ACCC, ACORN, ASBFEO, ASIO, ASD, Qld & Federal Police, MP's, Solicitors and many other organisations, with the common advice being to "contact ACORN or a Solicitor".

A solicitor was of no value because, whilst the prime cyberbully suspect was known to **XYZ**, he was using multiple fake IDs, which meant that **XYZ** could not conclusively prove who the offender was. And if XYZ could conclusively identify the offender the cost to bring civil defamation charges would exceed $50,000!

The owner of **XYZ** spent two extremely frustrating months being "bounced from pillar to post" between various agencies, with both ACORN and QLD Police often referring **XYZ** back to the other party! During this period ACORN declined to assist **XYZ** on three occasions, stating that it was a civil matter, which prompted **XYZ** to write a stern letter of demand to ACORN via the Qld Police. This resulted in ACORN eventually registering **XYZ**'s complaint, issuing of a CRN and forwarding **XYZ**'s file to the Qld Police for investigation.

XYZ provided ACORN and the Police with the suspect's contact details and a 50% selection of photographic exhibits as evidence, as well as other miscellaneous information to help identify the Cyberbully. Within days, a QLD Police CIB Officer replied by email and informed **XYZ** that there was no Australian Agency that had the means or legislation to identify and/or apprehend the Cyberbully!

The email from Police stated: "the alleged conduct and information contained in the (Cyberbullying) posts does not amount to any criminal offence prosecutable by the Queensland Police Service. It does not satisfy the elements of the current stalking legislation under the Criminal Code. Queensland does not have any criminal cyber-bullying type of offences and critical reviews or Facebook posts do not amount to harassment or menace unless there are direct physical threats to harm any person or property. * In the absence of those threats, which would need to be explicit rather than inferred, there is no criminal offence. It does not satisfy any Commonwealth offences either with regards to misuse of a carriage service. It also does not amount to Criminal defamation and any prosecution for this offence requires the assent of the State Director of the Director of Public Prosecutions office before any proceedings are commenced. This would require the compilation of a comprehensive brief of evidence which in reviewing the posts provided, is not possible as there is no evidence of such conduct. After reviewing what you have provided it would be very unlikely that that permission would be given. Any other type of defamation proceedings would be civil in nature and would not involve the QPS. At this stage no further investigation will take place in relation to your complaint".

NB: ACORN does not list a phone number, email address or street address, and its reporting website has no means to upload exhibits etc. Accordingly, the inability to verbally communicate or share information with ACORN was extremely frustrating and seriously impeded **XYZ**'s necessity to resolve the cyberbullying promptly.

In effect, **XYZ** management had wasted a colossal two months of valuable time and resources in pursuing assistance from Australian Agencies that was never going to eventuate!

XYZ is not aware of the Police or any other Govt authority making so much as a simple phone call to the suspected Cyberbully for the purpose of a "discussion".

Four months after the Cyberbullying had commenced, **XYZ** discovered by pure chance, "The office of the eSafety Commissioner". The **XYZ** manager contacted them immediately for advice. But it was another dead end. Whilst the eSafety staff were very pleasant and certainly more sympathetic than any other Govt. Agency, they only have legislative powers to act for youth victims, not adults or businesses.

The owner of **XYZ** cannot understand why Government Agencies have legislative powers to protect youth from cyberbullying, but literally no effective cyberbullying prevention, legislative, or other support mechanisms to assist adult or business victims!

The wasteful expedition for help

XYZ reiterates that it had not received any material benefit from any Australian Government Cybercrime related Agency or any other non-Govt business support organisation, from the commencement of the Cyberbullying in October 2018 through to February 2019 (spanning five months) and the cyberbullying is ongoing. XYX also felt that the law enforcement authorities contacted were in somewhat disarray when it came to understanding the reporting procedures or giving advice in the matter of Cyberbullying.

Vigilant action is the only choice of resolution!

The **XYZ** owner concluded (as advised by Police) that there are no laws in Australia to protect **XYZ** and its personnel from the Cyberbully's threats and actual ongoing harm. Therefore, the only option available for **XYZ** to stop the cyberbullying is to conclusively identity the perpetrator and for **XYZ** to take vigilant action, which of course is ridiculous. [redacted]

As at 15th February 2019 (presentation date for this case study), XYZ is still having to counter-defend the actions of the very clever Cyberbully on a daily-basis. That's five months of hell, with no end in sight.

……End of case Study……..

Continued next page

3. Considerations re Resolution Options

A. Multi-Party Approach (Do not underestimate the power in timing of this consideration)

At present, the angst and concerns of consumers and governments around the world are "peaking" towards the questionable performances of mainstream Cyber social platform providers, such as Facebook, Google and other interactive Apps/sites. With the prime issues including privacy breaches, false & misleading content, harbouring of criminal activities, hackers, spammers and tax evasion etc.

Equally, at present, these main stream cyber providers are suffering from recent adverse exposure and damage to their reputations. They are motivated to reverse both government and public confidence.

In consideration of the above, now is the perfect time for Governments and the mainstream Cyber Providers to proactively engage and improve the rules of engagement, particularly with the obvious need to improve authentication and integrity of subscribers for cyber safety and law enforcement.

The mutual benefits for all parties are massive and presents a quantum leap opportunity in global Cyber Safety, with a minimum 50% - 75% reduction is Cyber Safety breaches, maybe higher.

If Australia, and any co-joining nations do not engage with the Cyber Providers now (and vice versa), the opportunity may never rise again, and, if so, it would be unlikely be such a proactive mutually beneficial approach. *NB: Social media & App sites thrive on membership and they would prefer to accommodate Government demands to gain more business (maintain viability) than be blocked.*

B. Submission feasibilities

This author is not an IT software Engineer but works with plenty of them and believes that anything "IT" is possible. The suggestions this author makes in this submission are conceptual basic frameworks, requiring the appointment of expert teams to negotiate, design and implement interfacing technologies and security systems to manage registrations, reporting and enforcement, and with corresponding legal teams covering legislation etc.

Implementation of the submissions would provide a development base to significantly improve the prevention of many other types of Cybercrime, to further assist Agencies to promptly identify and apprehend offenders, e.g. false reporting, tax evasion, tracking criminals etc.

It would be very unlikely for the likes of Facebook and Google etc to decline adhering to new rules of engagement where the alternative is a risk of being blocked, as is the situation in China. If blocking was to occur, it would be no big loss to businesses because it is a level playing field loss for anyone utilising these platforms for business use and governments are already missing out on tax revenue from online social media sellers. Plus, other "more amenable" Cyber Providers would take over. It has even been suggested that the Australian Govt provide its own version of Social Networking Platform (Aussie FB).

This author doubts Politicians would entertain a decision to threaten social media bans, because it may cost too many votes, so it is up to the likes of the independent ACCC to take the hard-lead on this issue.

NB: This Author does not suggest the threat of banning Cyber social platforms lightly, but the increasing incidences and disturbing rise of unabated cybercrime and false propaganda far outweighs the comparable value of the entertainment or business features that these online social media sites provide.

C. Miscellaneous considerations

(a) The more one investigates Cyberbullying in Australia, (like this author certainly is doing), the more obvious it becomes in how ineffectual the relevant Government authorities have been in dealing with such an important and escalating risk to the welfare of our nation.

(b) The tail is wagging the dog in terms of Australia's ability to prevent, identify and apprehend offenders!

(c) There are no effective restraints to prevent cyberbullying from occurring at present.

(d) There is no centralised and effective Cyberbullying Agency (excluding eSafety Commissioner for Youth). Thought should be given to expanding the budget and role of the eSafety Commissioner Office to provide a better range of legislative powers and support for Adults and Business.

(e) An employee of ACORN admitted that its reporting system is flawed, (unable to upload docs or images as evidence etc), and that ACORN is closing its online reporting registry on the 30th June 2019 or thereabouts, to be replaced by an alternative Ministry of Defence Reporting System.

(f) There is an obvious and increasing need to urgently implement <u>better</u> Cyber breach reporting systems.

(g) Under the Telecommunications Act, it is illegal to transmit offensive or threatening information via phone calls and email, so why doesn't the same law apply to information transmitted over the internet? And if it does, why aren't Police using this law to identify and charge cyberbullying offenders?

(h) There is an obvious and increasing need to urgently implement better rules of engagement between the public and the internet interactive sites to improve integrity of authentication.

(i) There is an obvious and increasing need to urgently implement better rules of engagement between the Australian Authorities and internet interactive sites to access reliable information promptly.

(j) There is an obvious and increasing need to improve Public awareness of cyber support agencies.

(k) This writer is unsure why ACORN and the Qld Police suggest Cyberbully victims engage a Solicitor when the reporting entity ACORN or Police are unable to identity an offender.

(l) This writer has contacted several social media specialists and discovered that there is an alarming annual increase in the number of businesses having to continually fund expensive online marketing strategies purely to counteract the negative impacts of the rising number of false posts and reviews, as typically posted by an increasing amount of unidentifiable (fake) authors! The cost of funding is a constant drain on businesses and no matter how much a business spends to improve its image on line, it can all come crashing down within minutes, and with long term devastating results, simply by the posting of fake and false reviews by perpetrators that cannot be identified or apprehended.

(m) Such is the prevalence of fake reviews and posts, it is almost impossible for cyber viewers to decipher which reviews are genuine and which are not. Unfortunately, most cyber viewers don't realise they are witnessing false and misleading information and are being misled to make wrong purchasing decisions.

(n) Cyber extortion is a big problem, e.g. Guest to Motelier "give me free accommodation or I'll trash your trip advisor rating" and the severity gets much worse. Nothing material is stopping Cyber extortion!

(o) The costs of cyberbullying (when comparing the costs of other Cybercrime activities) is costing Australian Businesses $10 billion dollars per annum and rising, with nothing but negative returns!

(p) eSafety Commissioner has legislative powers for youth but not Adults or Businesses.

4. Submitter Introduction

This Submitter is a multi-stream certified Engineer, with qualifications in corporate governance and own a "technology business". I make no claim to be an expert on managing Cybercrime.

The following submissions are based upon my recent experiences, observations and interviews with experts associated with Cybercrime, particularly Cyberbullying and Cyberstalking. My young son was a victim of bullying that necessitated a change of school, plus I have many friends and business colleagues who have, suffered significantly (including suicide) from being victims of Cyberbullying, Cyberstalking and many other forms of Cybercrime.

Youth and Adults go through life safest when there are protective guidelines in place to follow. When guidelines don't work, there is a need to implement laws and when laws don't work it leads to wars.

No matter which Australian or global Cybercrime statistics you chose to follow, all demonstrate that cybercrime is increasing at an alarmingly rate and that Cyber Provider "guidelines" and support policies have failed miserably, with the negative results badly affecting all communities that touch the internet.

It is time for us to urgently implement better methods of Cybercrime management and stricter legislative powers (laws). I draw your attention to the preamble located on page 8, Sub title "Considerations re Resolution Options", Paragraph A & B (Multi-Party Approach). This content explains why the perfect timing to engage proactively with mainstream Cyber Providers, in order to improve the rules of engagement, has never been better than right now!

And equally, its high time we stop the tail wagging the dog! That is, we need Cybercrime agencies to take a dominant lead to enforce Cyber Providers to engage and act more responsibly, as opposed to us subscribers and victims continuing to endure or risk perpetual hardship as is the current the situation, as brought about by irresponsible Cyber Providers.

My submissions, if implemented, won't stop all cybercrime and I know there many other very talented people who are far more IT qualified than me to deliver equally superior IT technically based submissions in order to help manage and tackle the more complex issues, e.g. combating invisible and hardened repeat criminal offenders operating offshore etc.

But, I'm very confident my submissions would reduce localised* minor cyber offending by 90% and reduce localised* serious cyberbullying and cyberstalking by at least 50%, plus greatly assist our Australian Cybercrime Agencies to better manage and minimise other areas of general cybercrime.

All my submissions are basic concepts for more experienced experts in the relevant fields of the subject matter to assess and hopefully pursue and I welcome any feedback.

Thank you, Rod Harris. [redacted]

*Australia subscribers globally or actions that occur within Australian Cyber Coverage.

Continued next page…

5. Resolution Submissions (a) to (e)

(a) Establish a Primary Cybercrime Agency. *(Preventing, Reporting and Enforcement)*

This author has not had adequate time nor has the presumed security clearances to investigate in full the mandates and extents of effectiveness of Ministerial Government Departments and Agencies in respect to managing the reporting, prevention and policing of Cybercrime (Cyberbullying), but what is clearly apparent upon scratching the surface of this topic, is that there are a multitude of Govt Departments and Agencies involved in Cybercrime who appear somewhat in disarray when it comes to their staff having a precise understanding of their designated charters and responsibilities, along with inconsistencies in policies and procedures. Nor do the employees appear to have a strong handle on what duties and responsibilities are designated to other Cybercrime Departments and Agencies.

Cybercrime is a dynamic mine-field of issues changing daily and therefore many policies and procedures cannot be implemented on "a set & forget" basis. The roles for all Ministers, Executives, Front line Management and employees in this sector of security is very challenging with never ending tasks. Furthermore, Cybercrime agencies have been severely disadvantaged in recent years by an extraordinarily high turnover of Prime Ministers and corresponding Cabinet reshuffling, which has a negative effect on future planning, budgeting and ultimately performance levels.

One thing is for certain, Cyber usage will be forever steadily rising with ever-changing cybercrime attacks! At present, our Australian Cybercrime Agencies are simply not coping for a multitude of reasons and indeed going backwards in stemming the increase of Cybercrime incidences. *If you keep doing what you have always done, you will get the same results. So, we must continually change our approach to minimising and managing Cybercrime.*

It is imperative to ensure there is well organised central point of Cybercrime executive management and support teams; not satellite silos, as appears to be the situation now, whereby consumers, businesses (and indeed Govt personnel) are unsure of who to approach for prompt and effective cyber-related assistance. Nor are satellite offices conducive in a mission critical sector whereby urgent and collaborative executive forward planning regarding Cybercrime needs to occur on a daily basis.

Maybe there already is a well organised central point of Cybercrime Management, but if so, it certainly is not producing the desired or required results that this author/submitter would like to witness.

The crux of submission (d) is the recommendation to establish an <u>independent</u> expert panel to:

i. Confidentially conduct a 360-degree review of Australia's future management of Cybercrime.

ii. The review to include an assessment of current competencies/deficiencies as compared to what will be required in future, and include input from all stakeholders, e.g. consumer and business advocacy groups (ACCC, BCA, ASBFEO etc).

iii. The expert panel utilise the information gathered in the review, for the basis of a report listing recommendations to improve the over-arching operational framework of a future singularly managed all-encompassing Primary Cybercrime Agency. The report be delivered in a joint sitting with the Prime Minister and leader of the Opposition.

iv. This writer anticipates the review will uncover significant deficiencies in many areas and warns against any party eliciting political blame games! Therefore, terms of reference must ensure (a) the expert panel members are clearly unbiased and (b) includes a political bipartisanship agreement, to guarantee the confidentiality of the findings, reporting processes and outcomes.

(b) Establish an Australian Cyber Digital Registry

Attention Readers: Before viewing submissions (b), (c), & (d), please read the preamble located on page 8, Sub title Considerations re Resolution Options, Paragraph A & B (Multi-Party Approach). The content explains why the timing to engage proactively with mainstream Cyber Providers, in order to improve the rules of engagement, has never been better than right now! Equally, its high time we stop the tail wagging the dog!

The Australian Government (possibly in conjunction with My Gov) to establish a mandatory* registration system for all current and future Australian cyber subscribers, whereby applicant cyber subscribers must pass the equivalent of a 100-point identification checklist (including photo ID) in order to be granted a personal electronic authentication ID tag. The ID Tag will be required to subscribe or renew registrations with mainstream Cyber Providers.

Main stream Cyber Providers will be required to include a symbol next to the subscriber's cyber name to confirm if the subscriber has a current ID tag and therefore can be assumed is a legitimate (authenticated) consumer or business subscriber.

The purpose, benefits and ability to expand upon the features of the ID Registration system are infinite:

i. Sends a clear message globally that demonstrates the Australian Government is serious about managing CyberSafety professionally and reducing Cybercrime on home soil and abroad.
ii. Significantly reduce Australian Cybercrime, particularly Cyberbullying and Cyberstalking
iii. Assist law enforcement agencies to identify and police unacceptable behaviour.
iv. Adds significant credibility to the integrity of online reviews, whereby viewers can identify if reviews are genuine or not, as Digital ID authentication would minimise fake/false reviews.
v. Assist to save Australian businesses from wasting $10 billion per annum.
vi. An aid to prevent and demonstrate that offenders can be identified and apprehended.
vii. A system that Australia could replicate for other nations.
viii. Ability for Governments to track and block an electronic ID if compromised.
ix. A platform that allows for future applications to deter other types of cybercrime.
x. Ability to acknowledge and reward Cyber Providers who proactively assist in the formation and maintenance of such an ID authentication system
xi. Ability to penalise or block those Cyber Providers who don't comply or object to the formation and maintenance of such ID authentication systems.
xii. It is undeniably in the Communities best interest to implement the above and Australia is in the perfect position to make it happen. This is because our nation is globally credible and large enough to persuade or force Cyber Providers to engage proactively in implementing the ID authentication system, and yet statistically, in global terms, Australia is small enough to successfully run a "Beta or Pilot Program" to iron out any bugs, before (possibly) replicating the authentication system with co-joining Countries.
xiii. As a first to market solution, Australia is on the front foot to set the rules of engagement with any potential co-joining countries.
xiv. Establishing and maintaining the ID Registry would not be an expensive (comparatively), with minimal operating risks (excluding privacy breaches).
xv. When all factors considered, there is so much to gain and very little to lose.

Author considered **Voluntarily, which could be an introductory option, but ultimately self- defeating for voluntary subscribers, unless they have questionable alibis or genuine reasons to remain. Due consideration is required with appropriate rules set and enforced.*

(c) Review and implement/update Federal Cyber legislation, retrospectively by 2-3 years.

Attention Readers: Before viewing submissions (b), (c), & (d), please read the preamble located on page 8, Sub title Considerations re Resolution Options, Paragraph A & B (Multi-Party Approach). The content explains why the timing to engage proactively with mainstream Cyber Providers, in order to improve the rules of engagement, has never been better than right now! Equally, its high time we stop the tail wagging the dog!

At present there are grossly insufficient laws to enable Australian Enforcement Agencies to be able to promptly identify, apprehend or charge Cybercrime offenders (presumably this includes civilly also*).

This submission recommends introducing Federal criminal legislation to enable Australian Federal Cybercrime Law Enforcement Agencies to promptly identify, apprehend and charge Cybercrime offenders, particularly to protect adults and businesses (already legislation in place to protect youth).

It maybe that new legislation will only aid in identifying or apprehending Australian subscribers or where offences occurred in Australian territory (or same with a co-joining country), but any improvement in legislation right now would be significant and result in an immediate reduction in cybercrime and less harm to people and communities within Australian and co-joining countries.

i. Introduce/Update federal Cyber-criminal laws to cover bribery, cyberbullying, cyberstalking, defamation, extortion, uploading harmful material using fake ID's, uploading of false or harassing or offensive posts, posting misleading information, misappropriating and misusing copyright and trademarks etc,

ii. Where possible, focus on Federal legislation over state/territory laws.

iii. Ensure the conclusive identification of an offender is made known to the respondent.

Civil litigation is too expensive for consumers or small business to fund; therefore, the onus is on introducing criminal legislation, whereby the Federal Police also have the power to issue "on the spot fines" for minor cyber offences, with the penalty based on a matrix of category/severity. Allocate the income to cybercrime prevention.** ***With the current rate of cyberbullying & false reviews etc, income from fines maybe comparable with traffic infringements!

(d) Set new rules of engagement with main stream Cyber Providers & Review Sites

Attention Readers: Before viewing submissions (b), (c), & (d), please read the preamble located on page 8, Sub title Considerations re Resolution Options, Paragraph A & B (Multi-Party Approach). The content explains why the timing to engage proactively with mainstream Cyber Providers, in order to improve the rules of engagement, has never been better than right now! Equally, its high time we stop the tail wagging the dog!

i. Legislate to ensure an approved Agency of the Australian Government (and possibly that of co-joined Governments of other countries) have the right to demand cyber user details within 24 hours of making such a request upon any mainstream Cyber Provider, in the event whereby:

   a. The Cyber Provider's foot print covers the Country of the applicant.

   b. The Agency confirms the person of interest is a citizen of that, or co-joined country.

ii. Such details to be made available upon demand (if known) are to include IP address, MAC Address, geolocation and any contact/identity details held by the Cyber Provider that may not be entered on the Australian Government or Co-Joined Governments Digital Registries.

iii. Legislation to include hefty fines and ability to block the Cyber Provider from coverage over Australia territory (and/or other co-joined counties in mutual agreement with Australian Agencies).

iv. Review Web Sites.

At present, literally anyone can upload a fake and/or false review on a review web site such as Google Reviews, Facebook Reviews, Business Review web sites, Employee Review web sites etc and get away with it without being identified or charged for misrepresentation etc.

Equally concerning, is that the respondent or their associated organisation is more often not made promptly aware that someone has posted a fake or false review, which is unfairly harmful to the respondent and therefore unacceptable. This is a significant problem costing Australian companies billions each year to counter defend. It is a problem that must be urgently rectified.

My submission is to introduce legislation to block and penalise "Review Web Sites" that decline to deploy "auto forwarding" features to promptly and effectively email a respondent that someone has posted a review about them or their associated organisation. And ideally, legislate so that review websites must not be permitted to make a review public for a minimum 72 hours after a right of reply notification has been emailed and receipted with the respondent. The person uploading the review usually knows the respondents email address and the likes of Google and Business Directory Websites such as True Local can easily implement such rules of engagement.

Such rules of engagement with Review sites will significantly:

(a) Reduce fake and false reviews, and acts of cyberbullying and acts of cyberstalking.

(b) Improve the legitimacy of reviews so viewers are not misled.

(c) Enable review respondents to be timely notified and afforded a reasonable right of reply.

In reference to Employee Review Websites (Glassdoor, seek etc), countries like Australia already have very good employee support organisations, e.g. Fairwork, whereby aggrieved employees can obtain quality redress advice and assistance etc. Therefore, poorly moderated employee review sites (unlike the well-moderated www.seek.com.au), are overall more of a hindrance than help and many are recruitment agencies in disguise, e.g. www.glassdoor.com is owned by the same company that owns global recruitment company "Indeed".

v. Ensure the new rules of engagement are enacted within a set time period, e.g. 3 months.

vi. Upon implementation, ensure review sites display the new terms of engagement, with the overarching message that offenders maybe identified and charged for false misrepresentations.

(e) Youth Education

Whilst it is clear there are determined efforts and multiple ongoing initiatives by various agencies, community groups and schools etc to minimise cyberbullying with youth, this author is concerned there may be some inconsistencies in ensuring the delivery of consistent contemporary CyberSafety education to all students nationally, with best practice monitoring and reporting systems included.

If not already in place, this author suggests implementing a Federally mandated and supplied CyberSafety educational program to be delivered to every child at the commencement of each school year being primary, middle, secondary and to possibly include mid-year refreshers.

This program would deliver CyberSafety education, including recognising and reporting offenders, and culminate with an exam and pass certificate, including the completion of an electronic on-line questionnaire to (a) identify if a child is at risk of cyberbullying (requiring investigation or assistance) and (b) Provide statistical information for the Governments eSafety Commissioner to help improve the quality and focus of forward educational material, policies and procedures.

----------End of Submissions----------