

2 December 2013

The Executive Director  
Australian Law Reform Commission  
GPO BOX 3708  
Sydney NSW 2001  
C/-: [privacy@alrc.gov.au](mailto:privacy@alrc.gov.au)  
Attention: Professor Barbara McDonald

Dear Professor McDonald,

**Re: Serious Invasions of Privacy – Submission to Issues Paper: rapid takedown and child protection**

**I. Introduction**

The National Children's and Youth Law Centre (NCYLC) is a Community Legal Centre dedicated to working for and in support of Australia's children and young people, their rights and access to justice. We advance this mission by providing young Australians with sound legal advice and education; creating opportunities for their participation in decision making; promoting the implementation of the United Nations Convention on the Rights of the Child and advocating for changes to laws, policies and practices to advance their rights. We welcome this opportunity to comment on serious invasions of privacy in the digital era, particularly as they affect young people.

This submission will discuss Term of Reference 1: "Innovative ways in which law may reduce serious invasions of privacy in the digital era". More specifically, the submission sets out the Centre's proposal for a supported self-help and rapid take-down system to minimise harm and promote the best interests of young people experiencing invasions of privacy and other serious forms of cyber bullying.

While the Centre supports the creation of a statutory cause of action for serious invasions of privacy, we believe that a faster, easier and more accessible option for resolution is necessary to provide meaningful assistance to young people experiencing abuse online. We believe our proposal provides such an option.

**II. NCYLC's experience: how the law currently responds to serious invasions of young people's privacy**

NCYLC provides legal education, referral, advice and assistance to children, young people and their advocates across Australia through our legal information website, *Lawstuff* ([www.lawstuff.org.au](http://www.lawstuff.org.au)) and our email legal advice service, *Lawmail* ([www.lawstuff.org.au/lawmail](http://www.lawstuff.org.au/lawmail)). *Lawstuff* currently receives over half a million unique visitors a year, and *Lawmail* currently provides nearly 1,000 advices annually. *Lawstuff* and *Lawmail* provide information and advice on a wide range of legal issues confronting young Australians.

Increasingly, the young people who access our services come to us with questions about cyber bullying, sexting and fake social media accounts. The Centre notes that much work has been done in the *prevention* of cyber harms and serious invasions of privacy. However, little work has been done on developing a child-friendly framework to *respond* to serious invasions of privacy/cyber harms for young people. We have attempted to fill this gap by providing *response-focused* information and advice.

Our *Lawstuff* pages on cyber bullying have received upwards of 12,000 unique page hits since their creation in late 2010, and 7% of our *Lawmails* involve cyber bullying—many in the nature of serious invasions of privacy. A large

**National Children's and Youth Law Centre** ABN: 73 062 253 874

1<sup>st</sup> Floor, Law Building, UNSW SYDNEY NSW 2052 AUSTRALIA Tel: 61 02 9385 9588

Fax: 61 02 9385 9589 Email: [admin@ncylc.org.au](mailto:admin@ncylc.org.au)

Centre Website: [www.ncylc.org.au](http://www.ncylc.org.au)

Young People's Legal Information Website: [www.lawstuff.org.au](http://www.lawstuff.org.au)

proportion of these *Lawmails* are from young people who have exchanged nude or sexual images within the context of a relationship which has subsequently deteriorated, and who are now extremely distraught about the prospect of the images being circulated without their permission.

In our opinion, the current legal frameworks are inadequate to address this type of scenario, as they do not focus on a young person's best interests. The ineffectiveness of the current remedies available is perhaps best demonstrated by way of example through the Centre's own experience with clients who are young people or their advocates. All names and some other details have been changed to ensure client confidentiality.

### ***Case study***

We received a *Lawmail* from the parent of a 12 year old young person. A hate page on a service provider's website was created entitled 'GEORGIA HATERS'. The page referred to a young person with demeaning sexual language. The parent had contacted the police who said that there was nothing that they could do about the comments. With the Centre's support, the parent and the young person also reported the post to the service provider. The automated reporting system on the service provider's website responded within half an hour with a notice that the content had been reviewed and would not be taken down. Further reporting to the service provider by the Centre had the same result. It was only after the Centre was able to directly contact a staff member of the service provider that removal of the content occurred.

### ***The Centre's approach***

Depending on the circumstances of the case, NCYLC advises victims of cyber harms on a variety of legal and non-legal options. None of these options are specifically targeted at rapid take-down in the interests of protecting children from online abuse:

- Asking the individual to remove the content
- Blocking or 'unfriending' the individual who posted the content
- Reporting the content to the service provider for removal
- Speaking with a trusted adult and a counselling service such as Kids Helpline, Lifeline and Headspace
- Legal advice on criminal laws, including assault, harassment, unlawful stalking and intimidation, child exploitation material, menacing and intimidating use of a carriage service and reporting to police
- Reporting the incident to the school in the context of the school's anti-bullying policy
- Protection orders (commonly known as AVOs)
- Victims compensation for psychological harm
- The option of further legal advice on civil laws, including defamation and hate speech.

There are limitations with each of these options. Some of these limitations include:

- Reporting the content to the service provider for removal

Reporting content to service providers can be incredibly complex<sup>1</sup> and does not give users flexibility in explaining the context in which bullying occurs. Reporting bullying on service providers is infuriating for some, 'it felt like putting a note in a bottle and throwing it in the ocean. There was no way to know if anyone was out there on the other end'.<sup>2</sup> It is possible, and common, for a request to be denied with no explanation given about why abusive content did not warrant removal.

<sup>1</sup> See, Facebook's reporting infographic: <[https://fbcdn-dragon-a.akamaihd.net/hphotos-ak-prn1/851563\\_293317947467769\\_1320502878\\_n.png](https://fbcdn-dragon-a.akamaihd.net/hphotos-ak-prn1/851563_293317947467769_1320502878_n.png)>

<sup>2</sup> Emily Bazelon, 'How to Stop the Bullies', The Atlantic, 20 February 2013, <<http://www.theatlantic.com/magazine/archive/2013/03/how-to-stop-bullies/309217/>>

- Legal advice on criminal laws, including assault, harassment, unlawful stalking and intimidation, child exploitation material, menacing and intimidating use of a carriage service and reporting to police

Recommending reporting harmful online content to law enforcement may be ineffective or risky in many cases, with young people often preferring to preserve their privacy. This is particularly the case in cases of 'sexting' content. The dynamics of a young person handing over information about their personal life to a law enforcement officer who is often of a different age, gender and generation is problematic.

There is also a real risk that a young person who reports to police that a naked picture of them has been published online may be charged with distribution of child pornography if they were the one that originally sent it (albeit privately to an individual such as a boyfriend or girlfriend). In non-sexting cases, even when young people do contact the police, it is the Centre's experience that police are very often not willing to charge for harmful online content. This is a result of complex issues involving resource efficiency as well as the technical expertise required to investigate these matters.

- Reporting the incident to the school in the context of the school's anti-bullying policy

While it is possible to report bullying behaviour to schools, school counsellors and principals may consider they have mandatory reporting obligations to police and child protection, for example if they have a suspicion that a child is being sexually exploited. Because of this risk, young people are less likely to inform the school of 'sexting' cases where the young person who is bullied is the original creator of a nude image. This is because the criminal law also makes it an offence to create a sexual image of a person under 18 (in addition to publishing such an image).

- The option of further legal advice on civil laws, including defamation and hate speech

It is also improbable that a young person will have the resources to commence legal proceedings for defamation. While anti-discrimination complaints do not carry the same resource limitations, they are unable to reduce the harm as it is occurring.

- Speaking with a trusted adult and a counselling service such as Kids Helpline, Lifeline and Headspace
- Victims compensation for psychological harm

The Centre recognises the tremendously beneficial work conducted by our partner organisations in providing mental health and counselling services. However these services are not targeted towards preventing future harm from occurring or deterring the perpetrator of cyber harms.

- Asking the individual to remove the content

In the Centre's wide experience, there is a very low possibility of a perpetrator of cyber-bullying removing harmful content if requested by the victim.

To assist with this, the Centre has trialled the use of warning notices that cyber bullying victims can send to the person who published the harmful content. The notice informs them of the crimes that could be committed and requests that they remove the content immediately. A sample notice of the kind the Centre prepares in cyber-bullying cases is set out at **Appendix B**. The notice approach allows the Centre, and the client, to leverage the seriousness of criminal laws without having to report to the police. The Centre believes that notices are an effective method of promoting individual resolution of disputes involving harmful content. However, the Centre has limited resources and employs only 3 full time staff. This provides constraints on the number of clients we can assist.

Under the proposed scheme, the Commissioner would issue notices with its letterhead carrying the authority of a governmental body. This would be effective in demonstrating the seriousness of the conduct alleged in the notice.

### III. The need for innovative ways to reduce serious invasions of privacy to young people in the digital era

Given that the current legal frameworks are inadequate to promote the best interests of young people and to minimise the harm they experience when they are victimised through serious invasions of privacy, the Centre has developed a proposal for an innovative mechanism to address this gap.

The proposal outlined below seeks to address extremely harmful forms of cyber bullying, including—but not limited to—serious invasions of privacy such as the distribution of private images or the creation of webpages intended to spread humiliating rumours (whether true or false) about a young person. These kinds of cyber harms are particularly traumatic for young people in small communities and school environments where such material is likely to be made widely available. Examples of this behaviour include ‘Bender’s root rate’ where a man in Bendingo, Victoria, set up a page on a service provider’s service to rate the sexual performance of the residents of that town; the page featured sexually degrading comments about children people as young as 13.<sup>3</sup>

Courts in Australia have previously recognised that images, especially nude images, can cause extensive harm to their subjects, and are capable of grounding an action in defamation.<sup>4</sup> The criminal law recognises the prohibition on information or images which are bullying, harassing, threatening or sexually exploitative. This includes laws on harassment and stalking, child exploitation material and laws prohibiting the recording or publication of private acts. Current federal legislation also recognises offensive, menacing and harassing conduct over the internet.<sup>5</sup> However, these provisions have not been used to the extent possible, given the high rate of abusive material about Australian children online. More importantly, they are quite possibly not the most appropriate laws to apply at first instance where the perpetrator of the online abuse is himself or herself a minor.

### IV. The proposal

In September 2013, the Coalition Government published a proposed Policy to Enhance Online Safety for Children.<sup>8</sup> This Policy included the establishment of a Children’s E-Safety Commissioner to be a single point of contact for online safety issues for industry, Australian children and those charged with their welfare. The Policy also included the establishment of ‘an effective complaints system, backed by legislation, to get harmful material down fast’.<sup>9</sup>

The Centre wholeheartedly supports the establishment of such a Commissioner. This submission outlines our proposal for a child-rights framework within which the Commissioner could operate. The framework is designed to encourage individual responsibility, personal resilience and self-help. Its primary consideration is the best interests of the child, and its primary goal is to minimise harm to young people.

#### *Who will the system protect?*

The Commissioner will operate in respect of persons under the age of 18 in Australia (“a young person”). It is the Centre’s view that harmful online behaviour outside of this context is best addressed by existing criminal law, which comprehensively covers serious forms of cyber bullying.<sup>10</sup>

Under the proposed model, the Commissioner will only be able to issue binding rapid take-down notices regarding content which, in all the circumstances, is likely to cause harm to a child’. This term is intended to capture a broad range of online content that could cause harm to a child. The proposed definition of harm is “serious emotional distress”.

<sup>3</sup> Elise Snashall-Woodhams, ‘Fail: Josh’s ‘Benders’ page backfires’, 1 August 2012,

<<http://www.smh.com.au/technology/technology-news/fail-josh-s-benders-page-backfires-20120801-23e1i.html>>.

<sup>4</sup> *Ettinghausen v Australian Consolidated Press Ltd* (1991) 23 NSWLR 443

<sup>5</sup> *Criminal Code Act 1995* (Cth), Sch 1, s 474.17.

<sup>8</sup> The Coalition, ‘The Coalition’s Policy to Enhance Online Safety for Children’, September 2013

<<http://pandora.nla.gov.au/pan/22107/20130906-0245/lpaweb-static.s3.amazonaws.com/Coalition%202013%20Election%20Policy%20-%20Enhance%20Online%20Safety%20for%20Children.pdf>>, p. 4.

<sup>9</sup> The Coalition, ‘The Coalition’s Policy to Enhance Online Safety for Children’, September 2013

<<http://pandora.nla.gov.au/pan/22107/20130906-0245/lpaweb-static.s3.amazonaws.com/Coalition%202013%20Election%20Policy%20-%20Enhance%20Online%20Safety%20for%20Children.pdf>>, p. 4.

<sup>10</sup> National Children’s and Youth Law Centre & Legal Aid NSW, ‘New Voices, New Laws’, November 2012,

<[http://www.lawstuff.org.au/\\_data/assets/pdf\\_file/0009/15030/New-Voices-Law-Reform-Report.pdf](http://www.lawstuff.org.au/_data/assets/pdf_file/0009/15030/New-Voices-Law-Reform-Report.pdf)>

### *Rapid takedown and child protection*

It is important at this point to clarify what is meant by ‘rapid takedown’. The Centre considers that the period of time between a young person becoming aware of harmful content and having that content removed should be as short as possible given the paramount goal of child protection. For young people, one of the best methods of remedying harm is by preventing additional harm. Harmful content creates more harm to young people the longer it is publicly accessible. The Centre considers that rapid takedown should be in the order of minutes and hours, not days. More specifically, in the case of an individual, the Centre argues that take down of content should occur within 12 hours of receiving a notice from the Commissioner. In the case of service providers, take down should occur within 2 hours of receipt of such a notice.

The inadequacy of this timeframe is well illustrated by one of our cases outlined above involving a hate page about a 12 year old girl from a rural town. Within 24-48 hours of its creation, the page had attracted 250 likes and dozens of defamatory comments. As the page was publicly accessible, it is impossible to know how many additional people had accessed the page without liking or commenting. This situation would be distressing for anyone in our client’s position, but for a 12 year old girl living in a small community, each additional minute that this content remained online—allowing more and more people to see what has been said and to contribute to her humiliation—was agonising for her.

In conclusion, the Centre would like to reinforce the core message that, in the context of harmful online content about children, rapid takedown is synonymous with child protection.

### *Public interest, free speech*

It is important to recognise that the kinds of speech that the proposal intends to target are not the kinds that are currently afforded legal protection. For example, referring to a young person as a ‘slut’, ‘bitch’ or ‘whore’ is not speech which is made for genuine debate, artistic purpose or in the public interest. Furthermore, such speech is often already a breach of the law. For example, the above language could ground a complaint for sexual harassment under anti-discrimination legislation as could abusive comments directed towards a person on the basis of their race, sexual orientation, gender identity, HIV-AIDS status or disability. Repeated behaviour of this kind may constitute stalking or intimidation while threats to kill or injure are criminal offences in every jurisdiction. Furthermore, the national law criminalises incitement to suicide over the internet. In short, we do not consider that arguments about freedom of speech or public interest have any significant role to play where the serious invasion of privacy or harm is that of a child.

### *Children’s rights*

There is no defence of truth, privilege or public interest in child protection discourse. The paramount consideration for policymakers is acting to prevent harm to the child.

Existing legislation recognises the paramount goal of preventing harm. This includes child protection statutes, which provide:<sup>11</sup>

(a) that children and young persons receive such care and protection as is necessary for their safety, welfare and well-being, having regard to the capacity of their parents or other persons responsible for them, and

(b) that all institutions, services and facilities responsible for the care and protection of children and young persons provide an environment for them that is free of violence and exploitation and provide services that foster their health, developmental needs, spirituality, self-respect and dignity, and

(c) that appropriate assistance is rendered to parents and other persons responsible for children and young persons in the performance of their child-rearing responsibilities in order to promote a safe and nurturing environment.

<sup>11</sup> *Children And Young Persons (Care And Protection) Act 1998* (NSW), s 8.

The Centre considers that the Commonwealth has sufficient power under the Constitution to make laws in this area through its power to regulate “postal, telegraphic, telephonic, and other like services” under s51(v) of the *Commonwealth Constitution*.

However, the Centre believes that it is critical to the effectiveness of the scheme that the primary head of power relied upon for this framework is the external affairs power under s51(xxix) of the *Commonwealth Constitution*. The external affairs power is relevant because of Australia’s obligations under international law, particularly under the *Convention of the Rights of the Child*.<sup>12</sup>

## V. Functions of the Commissioner

Given the plethora of pre-existing programs providing information and education about cyber harms for young people targeting *prevention*, we have a strong view that the Commissioner’s primary function should be in *responding* to individual incidents involving cyber harm to young people.

The Commissioner’s functions would include:

- 1) developing memoranda of understanding with education departments, police and social networks that focus on the rapid takedown of material that is harmful to an Australian child;
- 2) creating tools for the use of child victims of cyber harms, their advocates and bystanders to take a more participatory approach to responding to cyber harms of an Australian child, encouraging self-help and fostering resilience in young people;
- 3) providing information, advice and referral to child victims of cyber harms, their advocates and bystanders;
- 4) facilitating the issue of rapid take-down notices of harmful content, for electronic service by a child or a person acting in their interests or the Commissioner itself;
- 5) liaising with children, parents, schools, education departments, principals, advocates and police about what are best practice approaches to responding to incidents of harmful content;
- 6) intervening in court matters relating to child bullying in a manner similar to the powers of the Australian Human Rights Commission;<sup>13</sup> and
- 7) generating publicity and making an example of successful litigation and recovery of money from infringement notices.

The Commissioner’s ongoing educative function in responding to incidents and assisting in self-help cannot be overstated. In the online space, ‘self-help’ mechanisms such as user reporting tools are often ineffective, despite the best intentions of service providers. They can be difficult to use, restrictive and do not allow for feedback or appeal processes.

The proposed scheme differs from existing approaches by creating a civil penalty for individuals and service providers who publish harmful content about a child. The Centre considers a civil penalty in the form of a fine will act as a sufficient deterrent for those who wish to publish harmful content. The proposed civil penalty must be high enough to dissuade and attract parental attention, but not so high that it leads people to contest the matter in court as a more preferable option.

One of the Commissioner’s core responsibilities would be to keep abreast of reporting processes across major service providers to ensure that it can advise young people of the best method of reporting harmful content. It is the Centre’s experience that young people and their advocates have encountered significant difficulties with automated

<sup>12</sup> Convention on the Rights of the Child, opened for signature 20 November 1989, 1577 UNTS 3 (entered into force 2 September 1990).

<sup>13</sup> Australian Human Rights Commission Act 1986 - Sect 11(1)(o).

reporting systems. For example, in the case mentioned above, upon reporting the hate page to the relevant website, we received a determination from the website that the content was not deemed to be abusive and therefore would not be removed. The client's mother had also reported the page, and had received the same determination. The inability to draw attention to harmful content amplifies the additional harm already caused to the young person. In our client's case, she was not only victimised by the page itself, but by a reporting system that refused to acknowledge the abusive nature of the page.

The Centre also recognises the need for the Commissioner to have access to relevant technological expertise to assist in its day-to-day operations. This expertise would enable the Commissioner to more accurately assess the availability, source and location of harmful content, and the most effective method of ensuring rapid-take down.

## VI. The Notice Process

The Centre's proposal provides a responsive environment to online bullying by fostering enhanced advocacy and self-help, supported by an enforceable penalty regime.

The process is as follows and is outlined at **Appendix A**.

- 1) Young person/advocate notifies the Commissioner of content harmful to a child (about the child).
- 2) The young person/advocate is told that the content will be assessed and triaged within 12 hours. In the meantime, the young person/advocate is encouraged to undertake self-help using tools developed by the Commissioner ("**Commission-assisted complaints and notices**"). These tools would include a complaint-facilitator for the most popular websites, as well as a notice-generator to inform the alleged offender of the potential illegality of their actions and to demand that they remove the problematic content.

A sample notice which could be automatically generated is set out at **Appendix C**.

- 3) If the content is not removed by the individual or the website and the Commission determines that it is harmful, the Commissioner can then issue an official notice to the individual requiring the content to be taken down within the **required time** and informing them that failure to do so will result in a civil penalty. ("**Commission-generated notice**").
- 4) If the individual does not comply with the notice within the **required time**, the Commissioner can:
  - i) issue an infringement notice to the individual AND
  - ii) issue a notice to the service provider, requiring that the content be removed within the **required time** and informing them that failure to do so will result in a civil penalty .
- 5) If the service provider does not comply with the notice within the **required time**, the Commissioner will issue an infringement notice to the service provider.

### *Notes on the process*

Memoranda of understanding with service providers will ideally support the framework for:

- the communication of notices to individuals' accounts/profiles
- the service provider's response to Commission-generated complaints and take-down notices, including an agreed manner of effecting service on the service provider.
- sanctions that the service provider can administer for repeat offenders and tools to identify pseudonym accounts of offenders

Where there is no relationship with a service provider, the statute would permit service by any form of electronic account (including email address, social media profiles).

The classification law provides a useful comparison to the proposed Commissioner model as it contemplates a statutory model for rapid take-down. Under the *Broadcasting Services Act 1992* (Cth), the Australian Communications and Media Authority has the power to issue take-down orders to Australian web hosts to remove content “as soon as practicable, and in any event by 6 pm on the next business day”.<sup>14</sup> Failure to comply with the notice is a criminal offence in addition to a civil penalty provision under the legislation.<sup>15</sup> The ACMA has indicated that the take-down notice scheme has significantly reduced the amount of prohibited content on Australian web hosts.<sup>16</sup> The Centre also notes the efficiency of systems used for the rapid take-down of child exploitation material and believes that this model can be duplicated in order to reduce the amount of cyber-bullying and online harms to young people.

Other legal frameworks which inform the notice and take down system contemplated by this proposal include:

- cease and desist notices in copyright, trademark and defamation law;
- stop orders issued by workplace safety inspectors where there is a serious risk to the health of a person;<sup>17</sup>
- the new bullying jurisdiction under the *Fair Work Act 2009* permitting the Fair Work Commission to make an order preventing an individual from being bullied at work;<sup>18</sup>
- personal/domestic violence intervention orders for those who fear for their safety; most jurisdictions also allow the issuing of interim orders issued by police prior to a formal court hearing.

The Centre also notes examples of Commonwealth statutory offices with administrative-law style powers, including the Privacy Commissioner, whose powers include the ability to investigate complaints.<sup>19</sup>

## VII. Risks

The Centre has identified the key risks to the effectiveness of the scheme and responses to address these risks.

### *Abuse of the user-generated notice system*

It is critical that the automatically-generated notice system is properly designed to prevent abuse, including the potential for the notices to be used themselves as tools to harm young people.

The Centre envisages that user-generated notices would be assigned a unique reference number. If an alleged offender receives a notice, they could verify the authenticity of the notice on the Commissioner’s website. This would reduce the likelihood of young people generating notices with abusive content. Also, the notice-generator would not permit free text responses. Young people or their advocates would select the nature of the harmful content, for example, bullying or harassment, and the notice would be prepared based on a prepared template. Furthermore, the notices generated from the automated system would be anonymous and do not contain the name of the young person reporting the conduct or the alleged offender (the Centre’s current notices operate this way – please see **Appendix B**; for a proposed sample notice generated by the Commissioner, see **Appendix C**). This reduces the risk of unsubstantiated allegations affecting the reputations of offenders who are often themselves young people. Finally, the notice process does not involve an admission of liability, but instead only makes allegations that someone has posted harmful content online.

The Centre also recognises that the availability of the notices may mean that they become less effective in deterring instances of harmful content online. However the Centre believes that this risk is outweighed by the benefit to

<sup>14</sup> *Broadcasting Services Act 1992* (Cth) Schedule 7, s 53.

<sup>15</sup> *Broadcasting Services Act 1992* (Cth) Sch 7, ss 106-107.

<sup>16</sup> W. Wei, *Online Child Sexual Abuse Content: The Development of a Comprehensive, Transferable, International Internet Notice and Takedown System* (2011), 81.

<sup>17</sup> See, generally *Work Health and Safety Act 2011* (NSW) Part 10 Div 2; *Work Health and Safety Act 2011* (ACT) Pt 10, Div 2

*Occupational Health and Safety Act 2004* (Vic) Pt 9, Div 8, s 112; *Work Health and Safety Act 2012* (Tas) Pt 10, Div 2; *Work Health and Safety Act 2012* (SA) Pt 10, Div 2; *Occupational Safety and Health Act 1984* (WA) Pt 6, Div 1, s 49; *Work Health and Safety (National Uniform Legislation) Act 2011* (NT) Pt 10, Div 2; *Work Health and Safety Act 2011* (QLD) Pt 10, Div 2

<sup>18</sup> *Fair Work Act 2009* (Cth) s 789FF.

<sup>19</sup> *Privacy Act 1988* (Cth), s 36.



young people in educating themselves and engaging in self-help to resolve disputes. Furthermore, the automatically generated notice is not the only deterrent in the proposed scheme. The primary deterrent is a Commission notice requiring rapid take-down of content. If an individual fails to comply with such a notice, they can be issued with an infringement notice.

### *A new criminal offence on the statute books*

The Centre also acknowledges that the scheme in essence creates a new criminal offence for failing to comply with a Commissioner's notice to take down content. However, it is important to note that those engaged in online bullying are already subject to the criminal law, for example through stalking and intimidation offences in every state and territory<sup>20</sup> and the national law of menacing, harassing or offending someone over a carriage service.<sup>21</sup> The maximum penalties for stalking and intimidation offences in all states and territories is at least 2 years imprisonment and up to 10 years in some cases;<sup>23</sup> and the maximum penalty under the national law is 3 years imprisonment.<sup>24</sup>

We propose that the penalty for failing to comply with a notice would be \$100 in the case of an individual (or higher in the case of repeated conduct after warnings). This falls far short of the penalties applicable if the matter were to proceed to adjudication in a criminal court. The proposed system also avoids the stigma of involvement in the criminal justice system and the resource burden on law enforcement to investigate common but harmful instances of cyber bullying.

This is not to say that law enforcement does not have an appropriate role to play in instances of harmful content published online. The Centre has noted experiences where the only appropriate response to the conduct is a report to police. As part of the proposed scheme, the Commissioner would maintain cooperative relationships with law enforcement and use its discretion to refer serious matters for investigation. The Commissioner would maintain its discretion not to issue an infringement notice for failure to comply with a take-down notice where the matter had been referred to law enforcement.

Our proposal is based on five well-recognised children's rights principles regarding criminal liability:

- Criminal proceedings are not to be instituted against a child if there is an alternative and appropriate means of dealing with the matter;
- Arrest and detention of children should only be used as a measure of last resort;
- The least restrictive sanction is to be applied against a child who is alleged to have committed a crime;
- Children convicted of offences must be treated in a way that is appropriate for their age; and
- Children have the right to express their views—and to have their views taken into account—in all matters affecting them.

### *Unnecessary regulatory burden on service providers and enforceability of sanctions*

The Centre is also aware that service providers may perceive the proposal as an unnecessary regulatory burden. However the Centre sees the proposal as acting to reduce the burden on service providers by specifically identifying and drawing attention to instances of harmful content. This would allow service providers to spend more time reviewing *proven* reports of harmful content than monitoring extensive report queues. Furthermore, the memoranda of understandings to be developed between the Commissioner and service providers will enable flexibility in responding to incidents while reinforcing the coercive power of the Commissioner should the service provider fail to comply with take-down notices.

While the Centre also acknowledges the jurisdictional challenges of enforcing criminal penalties on service providers located outside of Australian territory, this is not a sufficient reason to avoid criminalising conduct which is harmful to children. Australian law already recognises that foreign entities can be subject to Australian jurisdiction. For

<sup>20</sup> *Crimes (Domestic and Personal Violence) Act 2007* (NSW) No 80 s 13; *Criminal Code Act 1899* (Qld) s 359B; *Criminal Code Act 1983 No 47* (NT) s 189; *Criminal Law Consolidation Act 1935 No 2252* (SA) s 19AA; *Criminal Code Act 1924 No 69* (TAS) s 192; *Crimes Act 1958* (Vic) s 21A; *Criminal Code Complication Act 1913* (WA) s 338E; *Crimes Act 1900 No 40* (ACT) s 35.

<sup>21</sup> *Criminal Code Act 1995* (Cth) s 474.17.

<sup>23</sup> *Crimes Act 1958* (Vic) s 21A(1).

<sup>24</sup> *Criminal Code Act 1995* (Cth) s 474.17.

example, the High Court of Australia has previously recognised a foreign online publisher’s liability for defamatory content posted on servers located in the USA.<sup>25</sup>

Other jurisdictions have previously found offshore service providers liable for breaches of domestic law. New Zealand has recently introduced draft legislation to enable the rapid take down of harmful material,<sup>26</sup> while the German government has previously fined Google for breaches of Privacy Law, and ordered to pay 145,000 euros (equivalent to \$189,000).<sup>27</sup> While there are certainly difficulties in enforcing penalties against offshore providers, the above examples demonstrate that large online service providers are amenable to domestic regulation.

## VIII. Conclusion

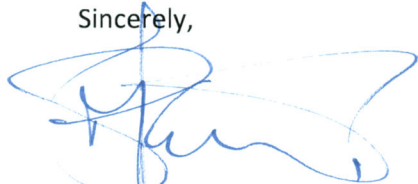
Children and young people have a right to grow up in surroundings that are safe and free from physical, sexual and emotional violence. This applies both online and off. However, childhood and adolescence are invariably about trial and error, and young people cannot be shielded from all harm. Thus, the task of those concerned with youth online safety is not to eliminate the risks of online exploration altogether, but to educate children and young people to make good and informed decisions, and to address and mitigate the harm to young people where this exploration goes awry.

The Centre’s proposal seeks to do this in a targeted and resource-efficient manner by promoting resilience and self-help buttressed by an enforceable penalty regime. Ultimately, the proposal recognises that in the online world, rapid take-down is synonymous with child protection.

Thank you for this opportunity to make a submission.

Please do not hesitate to contact us with any questions.

Sincerely,



Matthew Keeley  
Director & Principal Solicitor



Kelly Tallon  
Cyber Project Coordinator



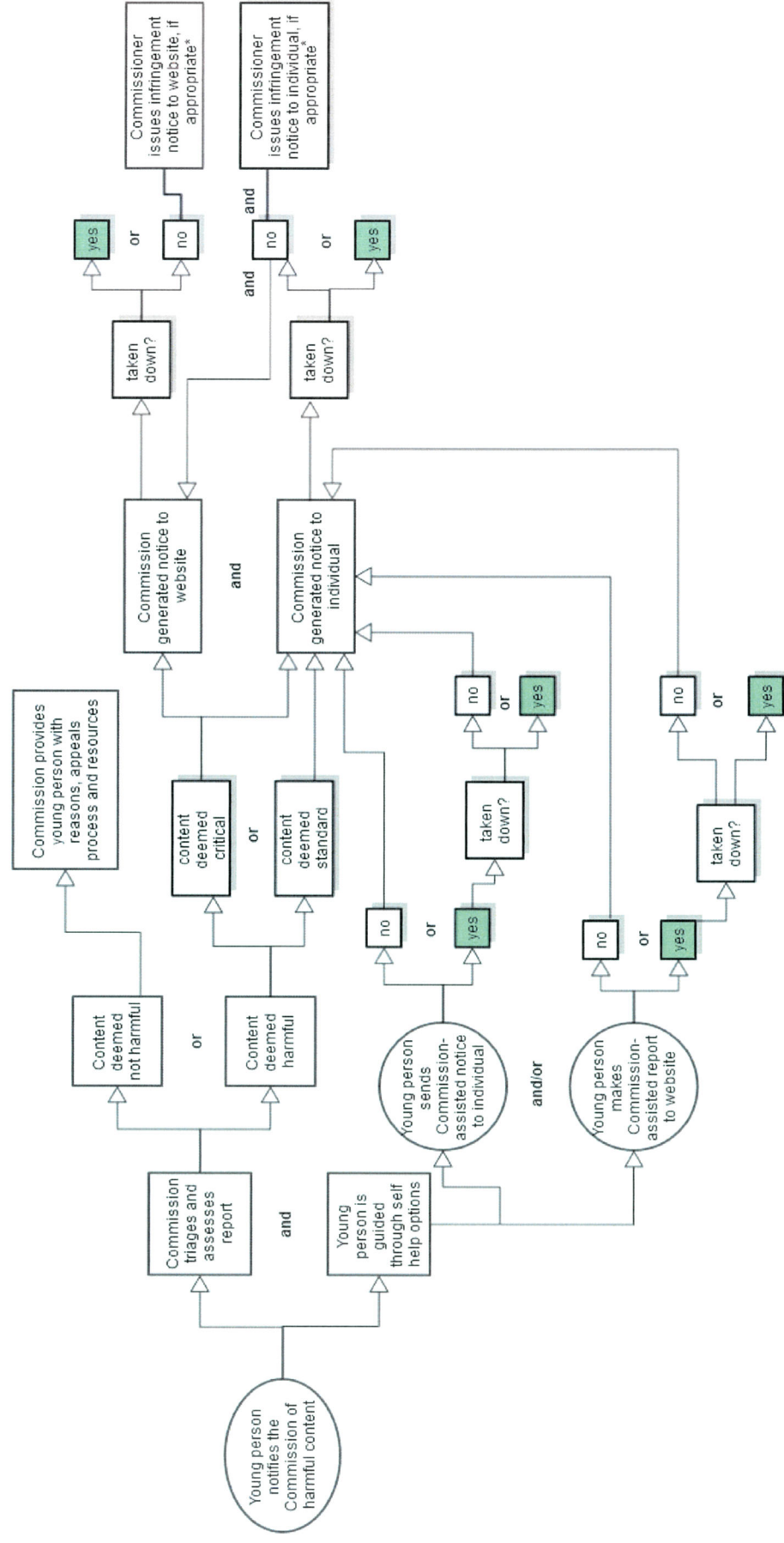
Jax Arnold  
Solicitor

<sup>25</sup> Dow Jones & Co Inc v Gutnick (2002) 210 CLR 575

<sup>26</sup> New Zealand Government, *Harmful Digital Communications Bill 168-1, Cl 20*, <<http://www.legislation.govt.nz/bill/government/2013/0168/latest/096be8ed80c76cca.pdf>>

<sup>27</sup> Kevin J. Obrien, ‘Germany Fines Google Over Data Collection’, *New York Times*, 22 April 2013, <<http://www.nytimes.com/2013/04/23/technology/germany-fines-google-over-data-collection.html? r=0>>

**Appendix A – the notice process under the proposed model**



**NB Neither the Commissioner nor the child victim of the serious breach of privacy is precluded from taking other action, including pursuing civil redress or criminal prosecution.**

## Appendix B – sample notice currently produced by NCYLC

*Personal and Confidential*

---

### NOTICE OF INTENTION TO REPORT TO POLICE

---

It has been alleged that a person acted inappropriately by:

- repeatedly contacting someone under the age of 16 on Skype and requesting nude photos; and
- continuing to pressure them for nude photos after their carer demanded that this stop.

If these allegations are true and this is person you, you may have committed the following crimes:

- using an internet service for child pornography material (sexual images of a person under 18)  
Criminal Code 1995 (Cth) section 474.19
- using an internet service to threaten, harass or cause offence  
Criminal Code 1995 (Cth) section 474.17
- stalking (messaging someone repeatedly in a way that causes them serious emotional harm)  
Criminal Code Act 1899 (Qld) section 359B
- unlawfully procuring a child under the age of 16 years to commit an indecent act  
Criminal Code Act 1899 (Qld) section 210
- involving a child in making child exploitation material  
Criminal Code Act 1899 (Qld) section 228A

To avoid a report to the police, please STOP this behaviour immediately and DO NOT CONTACT the other person again.

You should get confidential advice about this notice:

- for free legal advice, you can contact Legal Aid on 1300 65 1188 or at [www.legalaid.qld.gov.au](http://www.legalaid.qld.gov.au)
- for general advice, you can contact Kids Helpline on 1800 55 1800 or at [www.kidshelp.com.au](http://www.kidshelp.com.au)

Thank you for your cooperation.

Dated: 1 November 2013

*This Notice was drafted by the National Children's and Youth Law Centre*

## Appendix C – Proposed automatically-generated notice of allegations

---

NATIONAL CHILDREN'S E-SAFETY COMMISSIONER

---

### ALLEGATION OF HARMFUL CONTENT

---

To whom it may concern,

An Australian child under 18 has notified the National Children's E-Safety Commissioner that another person has acted inappropriately by:

- creating a social network page for the purpose of bullying, harassing and abusing that child;
- posting offensive comments about that child and encouraging others to do the same; and
- refusing to remove the content after repeated requests.

If these allegations are true and this person is you, you may have broken the following criminal laws:

- using an internet service to threaten, harass or cause offence—Criminal Code 1995 (Cth) section 474.17
- stalking (continuously posting offensive material about a person in a way that causes them serious emotional harm)—Criminal Code Act 1899 (Qld) section 359B
- defamation (posting false material about a person with the intention to cause them serious harm)—Criminal Code Act 1899 (Qld) section 365
- sexual harassment (making sexual remarks about a person with the intention of humiliating them)—Anti-Discrimination Act 1991 sections 118 and 119

#### WHAT SHOULD I DO NEXT?

If you have done the things listed above, you should:

1. stop this behaviour immediately; and
2. delete the material within 12 hours of receiving this notice.

#### WHAT HAPPENS IF I DON'T ACT?

If you do not do these things within 12 hours, the National Children's e-Safety Commissioner may:

- issue you with a notice requiring you to remove the material;
- fine you \$100 if you fail to remove the material after further notice; and
- report your conduct to the police.

#### WHERE TO GET HELP

You should get confidential advice about this notice:

- for free legal advice, you can contact Legal Aid on 1300 65 1188 or at [www.legalaid.qld.gov.au](http://www.legalaid.qld.gov.au)
- for general advice, you can contact Kids Helpline on 1800 55 1800 or at [www.kidshelp.com.au](http://www.kidshelp.com.au)

Sincerely,

The Office of the Children's E-Safety Commissioner

Dated: 1 November 2013

*This Notice was generated from the National Children's E-Safety Commissioner  
# 1234567*