Australian Government
Office of the Children's eSafety Commissioner

Red Building
Benjamin Offices
Chan Street
Belconnen ACT

PO Box 78
Belconnen ACT 2616

www.esafety.gov.au

Senate Legal and Constitutional Affairs References Committee

Submission on the "Phenomenon colloquially referred to as 'revenge porn', which involves sharing private sexual images and recordings of a person without their consent, with the intention to cause that person harm".

January 2016

Introduction

The Office of the Children's eSafety Commissioner welcomes the opportunity to provide this submission to the Committee's inquiry into the *Phenomenon colloquially referred to as 'revenge porn', which involves sharing private sexual images and recordings of a person without their consent, with the intention to cause that person harm.*

The Office is well placed to assist the Committee on its deliberation on this important subject and welcomes opportunities to provide further information in particular to terms of reference b, c, and d.

Having regard to the Office's functions, this submission outlines the Office's current remit in relation to the non-consensual sharing of intimate and sexual images and outlines matters for consideration by the Committee. These relate to the emerging problem of non-consensual sharing of intimate images including criminal responses, education and awareness raising, and international approaches to victim support services and civil deterrence measures.

The Office of the Children's eSafety Commissioner

The Office of the Children's eSafety Commissioner takes a national leadership role in enhancing online safety for Australian children (and by default their families) and supporting educators and frontline service providers to build resilience and confidence in online environments.

The *Enhancing Online Safety for Children Act 2015* (the Act) came into effect on 1 July 2015 and created a new independent statutory office: the Office of the Children's eSafety Commissioner (the Office). The Office is empowered to:

- Administer an effective complaints system to get harmful cyberbullying material targeted at Australian children down quickly from large social media sites.
- Manage complaints about offensive or illegal online content under schedules 5 and 7 of the *Broadcasting Services Act 1992* through the eSafety Hotline.
- Promote, coordinate and lead online safety education for Australian children nationally.

More recently, a new legislative function to support and empower Australian women and their children at risk of technology-facilitated domestic or family violence has been added.

Matters for the Committee's consideration

The key matters outlined in this report have been summarised into five points for the Committee's consideration:

1. The non-consensual sharing of private sexual images can be a form of family violence or sexual abuse, and can also constitute cyberbullying material, and in the case of minors child sexual exploitation material.

2. Additional services can provide confidential help and support to victims including the establishment of a helpline that offers advice and assistance similar to that provided by the 'UK Revenge Porn Helpline' and in cooperation with the internet industry.

3. Further research into the effectiveness and use of existing criminal sanctions, and civil deterrent measures similar to those taken by some states in the United States of America.

4. Any legislative proposals relating to non-consensual sharing of images could be part of a broader policy approach which includes support for appropriate programs and community education to address perpetrator behavior and victim blaming. The approach could recognise that the ability to choose from a range of conflict resolution tools including civil, criminal and alternative options can provide a measure of control to victims and ensure they are treated with respect and dignity.

5. The colloquial term 'revenge porn' can imply fault or blame on behalf of the victim. The use of alternative terms and in this submission the terms 'non-consensual sharing of intimate images' or 'nonconsensual sharing of private sexual images' have been used. On occasion the use of terms such as 'online sexual violation' or 'online sexual abuse' can be appropriate.

Key functions of the Office

Key functions of the Office include:

- Investigation of complaints where cyberbullying material targeted at an Australian child includes the sharing of sexual images on social media services or relevant electronic services.

- Investigation of complaints about child sexual abuse material and other illegal online content; including sexual images and videos of Australian children. The Office works with the international community of Internet Hotlines, known as INHOPE, to have overseas-hosted online child sexual abuse images taken down. This network does not deal with other types of images.

- Provision of preventative education to Australians including technology-facilitated domestic violence of which sharing private sexual photos without consent is a component.

The Cyberbullying Complaints Scheme

The Office administers a complaints scheme for serious cyberbullying material affecting Australian children and works in partnership with social media services, schools and others to resolve complaints. The complaints scheme comprises:

- A two-tiered scheme for the rapid removal of cyberbullying material from social media services. The Office has nine social media services as partners to help remove serious cyberbullying material: *Facebook, Instagram, YouTube, Twitter, Google+, Ask.fm, Flickr, Yahoo!7 Answers, and Yahoo!7 Groups*

- An end-user notice scheme under which notices can be given to a person who posts cyberbullying material targeted at an Australian child via an electronic services such as chat services, websites, emails and photo sharing services. The Commissioner has the power to give written notices and formal warnings directing a person posting cyberbullying material to: remove the material; to apologise to complainant(s); and to refrain from posting cyberbullying material.

The Act enables complaints to be made by the affected child, their parent or guardian, or a person authorised by the child to make a complaint on their behalf. In limited circumstances, complaints can also be made by a person up to the age of 18 years and six months. For material to be eligible it must be seriously threatening, seriously intimidating, seriously harassing or seriously humiliating the Australian child.

Material which is merely offensive or insulting is unlikely to fall within scope. Material which involves sharing of private sexual images is likely to fall within scope.

Where the material is posted on a social media service which is participating in the Tier scheme, the material first needs to be reported to the social media service. If the social media service does not remove the material within 48 hours of the report, the Office can then take action.

Complaints about cyberbullying can be made using the online complaint form on the Office's website www.esafety.gov.au. The website also has helpful information - videos, and step-by-step guides - about how to complain about cyberbullying.

Collaboration with social media services

To date, the Office has worked collaboratively with social media partners and has not needed to use its formal powers to remove content. The Office has experienced 100% compliance with requests to remove material and in its first six months of operation has:

- helped resolve 92 complaints of serious cyberbullying
- helped over 2500 young people in need of further support to access counselling through the Office's partnership with Kids Helpline
- worked quickly to resolve issues including impersonator accounts, threats of violence, hate pages, offensive images or videos, and unwanted contact and hacked accounts, with an average turnaround of 8 hours to resolve all matters.

In addition to resolving serious cyberbullying complaints, the Office has had:

- over 1.4 million website page views
- conducted 5561 online content investigations into child sexual abuse material and worked with 50 international partners to remove 4008 URLs of child sexual abuse material, with all items actioned within 2 days.

All social media partners in both tiers have been efficient in removing content and actively co-operating to help address the behaviour of cyberbullying demonstrating the effectiveness of a cooperative civil scheme for serious cyberbullying.

Feedback from both parents and schools about outcomes achieved by the Office has been strongly positive. As an example, parents have informed staff that they no longer felt alone in tackling cyberbullying, and expressed thanks for the 'speedy and efficient manner' in which the complaints were handled.

Education and awareness programs

The Office considers that education is critical in providing Australians with the ability to make appropriate choices about online safety education issues and to help them develop the knowledge and skills to operate as effective digital citizens.

Since 1 July 2015, the Office's trainers educated over 60,000 students, teachers and pre-service teachers face-to-face, and over 10,000 students across the nation have also learned about online safety via the Cybersmart Virtual Classrooms. The virtual classrooms include components for primary students on respectful relationships, and for secondary students on the law including sexting and unlawful publication of images online. Where there have been specific cyberbullying incidents, the Office will work directly with schools to address the issue in their school.

The Office is responsible for the Cybersmart education program. As a broad-ranging program covering online safety and digital citizenship Cybersmart includes internationally recognised and award winning resources, such as:

- the short film Tagged and its associated lesson plans which tackle issues such as cyberbullying, sexting and digital reputation management
- the audio visual Be Deadly Online resources and its associated lesson plans designed specifically for, and in consultation with, indigenous communities which address sexting and digital footprint management
- the audio visual #Gameon and its associated lesson plans, which target children between the ages of 10 to 14 and looks at the consequences of making poor decisions online, and
- the important sexting resource, So You Got Naked Online, developed in conjunction with Bravehearts, which seeks to move beyond blame to offering practical solutions to people experiencing problems and provides guidance to young people under the age of 18.

In addition, in 2016 schools will now be able to access 18 online safety education provider organisations that have been certified under the Office's voluntary certification scheme.

As the Office has a contractual relationship with Kids Helpline to refer complainants in need of counselling support, the Office has provided training to Kids Helpline and Parentline counsellors on cyberbullying including specific scenarios on social media platforms and the types of cyberbullying incidents that the Office can assist with resolving.

In November 2015, the Office trained over 55 South Australian police including investigators and management from the Electronic Crime Section, State Crime Prevention Officers, Special Crime Investigation Branch, Multi Agency Protection Section, and Training and Development Coordinators from the local areas, following a 'revenge porn' incident in 2015 involving a number of South Australian targets.

Technology-facilitated Domestic Violence

In September 2015, the Australian Government announced its Women's Safety Package to Stop the Violence.[1] The package comprises a wide range of measures to improve frontline support and

[1] http://www.malcolmturnbull.com.au/media/release-womens-safety-package-to-stoptheviolence

services, leverage innovative technologies to keep women safe, and provide education resources to help change community attitudes to violence and abuse.

The Office is developing a resource package to equip women to address abuse perpetrated through the use of technologies such as smartphones and social media services (including some resources on non-consensual sharing of intimate images).

The resource package will include resources for women and frontline professionals, and online safety training for frontline professionals. Information will include reporting mechanisms (to social media services and the police) and the places women can go for counselling support and legal advice.

The Office considers the non-consensual sharing of private and intimate photos can be a form of technology-facilitated domestic violence. Research demonstrates that the threat of sharing intimate images is being used in domestic violence and sexual assault situations to blackmail victims, or to discourage them from seeking help from the police. It's not just 'revenge' towards an ex-lover that motivates perpetrators of these harms. In many cases, it is part of a pattern of abuse against and control over women.[2]

The threat of an abusive partner distributing private sexual photos or videos perpetuates intimate partner violence. Threats of violence and intimidation are among the most favoured weapons of domestic abusers, and the rise of social media has only made those tactics more commonplace.[3]

An RMIT survey titled *Digital Harassment and Abuse of Adult Australians*, found that women were more likely than men to report experiencing sexual harassment online and '1 in 10 Australians reported that someone had posted online or sent on to others a nude or semi-nude image of them without their permission'.[4]

Potential criminal responses

At present, there are a number of Federal, State and Territory laws that appear to prohibit the sharing of intimate images without consent or prohibit a broader category of offences that encompass this type of conduct. As well there is a general power for Government agencies to seek help from the Telecommunications Industry to enforce the criminal law nationally.[5] For example:

- Section 474.17 of the *Criminal Code Act 1995* (*Cth*) prohibits the use of carriage services to menace, harass or cause offence to another person. The offence carries a maximum penalty of 3 years imprisonment and may apply to instances of 'revenge porn'.

- In South Australia, Section 19AA of the *Criminal Consolidation Act 1935* prohibits unlawful stalking, including by publishing or transmitting offensive material by means of the internet. South Australian legislation also prohibits the distribution of 'invasive images' of another person without that person's consent.[6]

[2] Woodlock, Delanie (2015), *Technology-facilitated Stalking: Finding and Recommendations from the SmartSafe Project,* Domestic Violence Resource Center Victoria Collingwood.
[3] Ibid
[4] Powell, Anastasia and Henry, Nicola, (2015) *Digital Harassment and Abuse of Adult Australians,* REPORT_AustraliansExperiencesofDigitalHarassmentandAbuse
[5] Telecommunications Act 1979 (Cth), Section 313,
[6] Summary Offences (Filming Offences) Amendment Act 2013 (SA)

- Victoria has explicit criminal offences that prohibit the distribution of an 'intimate image' without consent including threats to distribute such an image. The offence carries a maximum penalty of 2 years imprisonment.[7]

- In NSW, section 578(c) of the *Crimes Act 1900* was used successfully to prosecute in the case of Usmanov, where the former partner of Mr Usmanov posted six intimate images of the complainant on his Facebook page without permission.[8]

While the above is not an exhaustive list, the range of existing laws available to law enforcement agencies have not been widely used, to take action against individuals who share intimate images without consent, due to the lack of clear precedent on how these laws can apply.

Further exploratory research to assess the application of existing legislation to this issue could be beneficial prior to the introduction of any new criminal offences.

Careful consideration should be given to the impact of any new criminal sanctions on young people under the age of 18, as well as consideration of diversions or alternatives which can impose immediate consequences for offending behavior while avoiding the social cost associated with the criminal justice system.

The nature of a criminal investigation can leave a victim vulnerable and they can find the process confusing and overwhelming.[9] Victims can be, for the very first time, involved in the criminal justice system and may have to speak to police officers, lawyers and judges and ultimately go to court.[10] The process may lead to further 'shaming' as images are shared with more people, exacerbating trauma, while original images can take long periods of time to be taken down and may never be completely removed.

Overseas approaches

Several common law jurisdictions recently enacted legislation in an attempt to address the harm caused by non-consensual sharing of intimate images including New Zealand, the United States of America, the United Kingdom and Canada. The various penalties range from civil and criminal approaches alongside provision of vital education resources and support services.

The UK 'Revenge Porn Helpline'

The UK enacted criminal legislation under Section 33 of the *Criminal Justice and Court Act 2015*. Alongside this legislation the Government provided funding for a victim support service that facilitates cooperation with social media services to assist the removal of images from social media sites and minimise the proliferation of such images across the internet.

[7] Summary Offences Act 1966 (Vic), section 41DA
[8] Police v Ravshan Usmanov [2011] NSWLC 40.
[9] European Commissioner Victim Rights http://ec.europa.eu/justice/criminal/victims/index_en.htm
[10] Ibid

The Revenge Porn Helpline, a service launched by the South West Grid for Learning, provides advice and information to individuals on how to get images and recordings off social media and other websites.[11] The Revenge Porn Helpline offers free, confidential advice and support, and states that

> 'While we cannot guarantee removal of all images online, exceptional partnerships with the internet industry allows us to minimise the reach, and some of the harm caused by revenge porn'.[12]

The Helpline utilises its good will and relationships to facilitate cooperation from the Internet industry. The service, whose tagline is 'Don't suffer in silence' provides victims with immediate and tangible support in 'real time'. The Helpline can offer victims some measure of control to manage a potentially escalating incident.

Additionally victims, who may find it difficult to talk about what has happened, are afforded the peace of mind that a dedicated service with specialised personnel familiar with the topic exists. Unlike criminal sanctions which can take weeks, months or even years to be effective, the Helpline may be able to quickly assist in removing offending material.

The service offers an anonymous reporting tool to assist victims to initiate contact (although they will likely need to confirm personal information once they feel comfortable doing so) and provides referrals to further counselling support where necessary.

New Zealand

New Zealand's *Harmful Digital Communications Act 2015* (the HDC Act) make it an offence to send messages and post material online that deliberately cause serious emotional distress (punishable by up to two years imprisonment or a maximum fine of $50,000 for individuals, and a fine of up to $200,000 for companies).

The HDC Act establishes a complaint mechanisms for victims of behaviour such as cyberbullying, harassment, and "revenge porn" and will provide new civil remedies and criminal offenses.[13] As well, the HDC Act establishes an agency to resolve complaints about harmful digital communications, providing a quick and efficient way for victims to seek help from an independent body.

The Agency will offer a range of support services and diverse resolution options to victims including resolving complaints through advice, mediation, negotiation and "persuasion"; and providing advice and education on policies related to online safety and conduct on the Internet.[14]

The United States of America (USA)

Many states across the USA have legislated to deter against 'revenge porn' behaviour. Penalties range from misdemeanours in some jurisdictions and felonies in others. Some states in the USA have also included a civil component, one example is the approach taken in Texas.

[11] Revenge Porn Helpline UK *http://www.revengepornhelpline.org.uk/*.
[12] *http://www.revengepornhelpline.org.uk/*.
[13] Press Release, Hon. Judith Collins, Collins Calls Time on Cyber Bullies
[14] Ibid

In 2015, Texas passed *Bill S.B.1135* subjecting those who post nude or sexually explicit images to harm another person, to civil and criminal liability.[15] Under the new laws, a defendant can be liable under both civil or criminal law and face a maximum financial penalty of $4000 or a jail term of up to one year. Claimants can also be awarded damages and injunctive relief restraining and preventing the disclosure or promotion of intimate visual material.

Civil measures, including financial incursions, have been found to be an effective, prompt and appropriate means of sanction and of creating a deterrent for a wide range of regulatory matters and offences.[16] They can be a flexible penalty that can be adjusted to reflect both the severity of the incident and avoid the social costs attached to additional criminal sanctions.

Offering a victim support service such as the UK Helpline alongside civil deterrent measures could provide a combined remedy that minimises the risk of re-victimising women. Unlike some criminal processes, this approach could offer a less stressful, faster and less expensive option that can bring peace of mind quickly.

Education and public awareness programs

Alongside civil and criminal sanctions, education programs and public campaigns are a sometimes overlooked component in creating behavioral change. Good awareness programs can be a first line of defence against sophisticated online attacks and there is growing evidence that individuals want messages that are 'just in time', action oriented and example rich. Cybersmart's Digital Citizenship research affirmed this.[17]

People are often confused and distressed about the lack of clear guidance about what to do should they find sexual images of themselves published online. Clear, targeted public awareness information and education programs that are strategically planned to communicate a key message can be effective.

In 2015, the United Kingdom's Ministry of Justice, in partnership with the UK Safer Internet Center, Woman's Aid and the Suzy Lampugh Trust, launched the *Be Aware B4 You Share* awareness program aimed at deterring potential offenders from sharing revenge porn. It also lets victims know the law is on their side and support is available.[18]

Be Aware B4 You Share discourages behaviour that constitutes an offence. Evidence suggests that awareness raising campaigns will be more effective where people believe there are repercussions for certain behaviour and where they are targeting a behaviour that is easy to understand and easy to detect.[19]

Ideally, any legislative considerations including criminal or civil sanctions would be part of a broader approach, resourced to provide appropriate programs, public awareness initiatives and community education to address non-consensual sharing of images and associated gender and victim blaming.

[15] S.B.1135, http://www.legis.state.tx.us/tlodocs/84R/billtext/pdf/SB01135F.pdf#navpanes=0
[16] The deterrent effect of higher fines on recidivism: driving Offences NSW 2007; http://www.bocsar.nsw.gov.au/Documents/CJB/cjb106.pdf
[17] Digital Citizens Guide Community and stakeholder research, Cybersmart programs 2014, https://www.esafety.gov.au/education-resources/classroom-resources/digital-citizenship
[18] https://www.gov.uk/government/publications/revenge-porn-be-aware-b4-you-share
[19] Not Just slick TV Ad, the Conversation 2015, http://theconversation.com/not-just-a-slick-tv-ad-what-makes-a-good-domestic-violence-awareness-campaign-45041