Submission to the Inquiry into the Criminal Code (Non-consensual Sharing of Intimate Images) Amendment Bill 2018, Queensland Government by Associate Professor Terry Goldsworthy and Assistant Professor Matthew Raj and Senior Teaching Fellow Joe Crowley.

Currently, a range of criminal offences are perpetrated online. In addition to the commission of traditional offences, such as fraud, stalking, and domestic violence, new phenomena have emerged to warrant attention from the media, government, and communities. The phenomenon colloquially referred to as ‘revenge porn’ stands as one of the greater threats to public morality. To date, legislative responses to circumscribe revenge porn, both internationally and in Australia, have been sporadic and disjunctive. This article critically examines the impact and prevalence of revenge porn and provides a critical analysis of the civil and criminal responses to its commission. It concludes by arguing that addressing the challenges associated with investigating such offences, and educating about the dangers of revenge porn have to some extent been overlooked in the rush to legislate and create new offences. The article highlights that existing legislation may provide adequate protection.

INTRODUCTION
Our use of new technologies and the Internet is becoming more frequent and, indeed, pervasive. The global Internet population has grown from 2.1 billion in 2012 to 3.4 billion in 2016 (James, 2016). With this increase in the use of new technology comes the risk of greater opportunities for criminal behaviour. New technology is facilitating offences, both old and new. This

---

1 We make this submission with a view to examining the proposed legislation and considering potential problems. Specifically, we examine the proposed addition to the Criminal Code 1899 (Qld) of section 223 ‘Distributing Intimate Images’ and the amendments to its relevant section 207A. We stress that, throughout this submission, the views expressed are those of one or both authors; they do not necessarily reflect the opinions of our employer, Bond University.

2 Dr Terry Goldsworthy is an Associate Professor in the Faculty of Society and Design at Bond University.

3 Dr Matthew Raj is an Assistant Professor in the Faculty of Law at Bond University.

4 Joseph Crowley is a Senior Teaching Fellow at Bond University in the Faculty of Law at Bond University.
submission provides a summary of the growing trend in revenge porn type offences committed and, indeed, facilitated by new technology. It provides a critical analysis of the policy and legislative responses to such offences. It concludes by arguing that simply creating new specific offences may not be effective in dealing with this phenomenon and a wider response is needed. Such a response needs to focus on better law enforcement responses, and education and awareness in the community.

THE EMERGENCE OF REVENGE PORN
Revenge pornography atypically involves the following: an existing or previous relationship, an intent to cause harm, the unauthorised public release of an intimate image, and the act of releasing the intimate image is facilitated by technology. While this is neither a legal definition nor an exhaustive one, it captures the traditional concept and, indeed, wide-spread perception of revenge porn. In 2010 digital revenge porn came to prominent notice with the creation of the *Is Anyone Up* website that allowed for submission, and distribution of photos of ex-partners without consent (Salter & Croft, 2015).

The unauthorised public release of an intimate image following the breakdown of a relationship was not unknown in Australia prior to the Internet (Salter & Croft, 2015). Such acts, though not criminalised were actionable through the civil law of defamation. In 2001, the Supreme Court of Queensland adjudicated the matter of *Shepherd v Walsh*[^5], a dispute between a woman, Shepherd, and her ex-boyfriend and the publisher of “The Picture” magazine. Shepherd sought damages for defamation from her ex-Mr. Walsh (and others) after he had sent a nude photograph of her to *The Picture* magazine that featured in the Home Girls section and it was published. He had done this “as a revenge on his ex-girlfriend”. She received $50,000 in damages.

Media attention to revenge porn has increased dramatically in the last 5 years. A search of the Factiva[^6] media content provider for the term ‘revenge porn’ revealed that in 2012 there were eight stories about revenge porn, in 2017 there were 3214 stories.

![Factiva Media Engine search for stories using the term "Revenge Porn" 2012-2018](image)

[^6]: Factiva is a global news database featuring nearly 33,000 sources, including licensed publications, influential websites, blogs, images and videos. A search was conducted of all sources for the last 5 years for the term “revenge porn” either in the title or body of the article.
Recently, mainstream media has used the term to encompass almost any unauthorised release of intimate images, regardless of relationship status between the offender and the victim. The term has also been made synonymous with the mass dumping of images of multiple victims. Recent examples of this include the release of intimate images, in 2015, via the Internet of 400 women in Adelaide and some 700 from Brisbane (Branco, 2015a; Fewster, 2015).

In 2015, as part of a response to the growing concern in relation to what was summarily referred to as ‘revenge porn’, an Australian Senate Inquiry (hereafter referred to as the Senate Inquiry) was convened. The Senate Inquiry noted that revenge porn consisted of the non-consensual sharing of intimate images (Commonwealth of Australia, 2015, p. 2). Important considerations in applying the term seem to hinge on the nature of the image, the context or relationship in relation to the taking or obtaining of the image, and the harm inflicted (Commonwealth of Australia, 2015).

Arguably, revenge porn is one example of technology influencing criminal activity. Movement from the physical to the digital world, globalisation and society’s reliance on technology are some of the reasons why so many of our lifestyle activities are conducted in the digital world. Examples of this include technology driven communities such as Facebook, Twitter, and Instagram. Research by analytics software provider Domo shows that society’s use of such platforms has increased dramatically in recent years (James, 2016; Morrison, 2014).

These platforms and others allow people to capture their experiences, including intimate ones, and share them to a potentially global audience. The advent of the smartphone and other mobile technologies has, to some extent, revolutionised our ability to interact with technology daily. The above Factiva search revealed that social media, internet and media are the leading industries associated with media reports of revenge porn. In relation to social media, Facebook and Twitter were the most mentioned social media companies in stories concerning revenge porn.

The creation of, and access to, new markets of victims — no longer constrained by physical location — assists potential offenders. A noteworthy dynamic to the use of technology is the ease with which one can attract an online audience. This is where the internet can act as a force multiplier (Salter & Croft, 2015). Technology has further impacted crime through the extension and facilitation of traditional offences, for example frauds, but in the realm of sex offences, the ability to stalk, meet victims on dating sites. The creation of new offences through technology, revenge porn, unauthorised surveillance, electronic stalking and the use of audience and distribution to magnify the offence are also examples of technology and its influence on criminal behaviour and our policy responses.

**THE SCOPE OF THE PROBLEM**

Several factors have driven the rise in incidences of revenge porn, these include: the ability to create content, the ability to distribute this content, and the assistance in many cases of facilitators to distribute to a much wider audience. To highlight the issue of exploitation, an online study of 1,519 consumers conducted by McAfee in 2014 known as ‘Love, Relationships and Technology’ reported that 98 percent of respondents used their mobile device to take photos, and 54 percent sent or received intimate content including video, photos, emails and messages (McAfee, 2014). Of those surveyed, 69 percent were securing their smartphone with
a password or passcode. Of those found to secure their phone, 42 percent used the same password across multiple devices, which increases the likelihood that the security of these mobile devices will become exploited (McAfee, 2014). In 2014, at least 3,000 pornography websites around the world were hosting the revenge genre, and the number was said to be increasing (The Economist, 2014). An Australian study showed that 9.3 percent of Australians had nude or semi-nude images posted online or sent onto others without permission (Powell & Henry, 2015).

The emergence and increase of revenge porn type offences is also reflected by the fact that governments are also reacting to the growing problem – the New South Wales government in 2015 announced a parliamentary inquiry into existing laws and whether there was any need for reform (New South Wales Parliament, 2016). In 2015 the Australian Senate also conducted an inquiry into the revenge porn phenomenon (Commonwealth of Australia, 2015).

The United Kingdom (UK) has also considered the issue of revenge porn and implemented laws to combat it. As noted at the Council of Australian Government meeting (COAG) 2015, strategies are needed to tackle the increased use of technology to facilitate abuse against women, and to ensure women have adequate legal protections against this form of abuse (Branco, 2015b).

Technology-facilitated abuse encompasses the non-consensual distribution of sexual images, as well as stalking, monitoring of location via car or mobile device GPS systems, harassment and abuse through social media, texts or email and monitoring and tracking of website history of computers or mobile devices. (Branco, 2015b).

Undoubtedly, we are witnessing a merge between the physical and digital world in terms of offending. Anecdotal information in an email dated 18 June 2015 from the Gold Coast Centre against Sexual Violence provides some understanding into the role technology plays in traditional physical sexual offences. The councillors of the service identified five main areas that technology played a role in sexual assaults; victim met offender online, online harassment of the victim by the offender, victim transmitted explicit material, offender transmitted explicit material, and assault filmed.

For reasons, such as this it could be argued that the act of revenge porn should be considered an extension of sexual assault type of offences given the potential impact on victims. Indeed the eSafety Commissioner’s office identified that “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” (Commonwealth of Australia, 2016b, p. 2). Such an approach is seen in the revenge porn laws adopted by Israel. In 2014, Israel made revenge porn a crime by drafting a new law that “stipulates that those found guilty of posting such content will be prosecuted as sexual offenders, while those who are targeted will be recognized as victims of sexual assault.” (Yaakov, 2014). It carries a sentence of up to five years imprisonment (Yaakov, 2014).

CIVIL RESPONSES TO REVENGE PORN

---

7 Note Associate Professor Terry Goldsworthy is on the Management Committee of the Gold Coast Centre against Sexual Violence.
In the public domain, there have been a number of responses to the revenge porn issue. In June 2015, Google Senior Vice President, Amit Singhal, announced that Google would remove links to revenge pornography on request (Grandoni, 2015; Singhal, 2015). Microsoft followed suit in July (Beauchere, 2015). From a civil prospective, Google is the latest in a series of high-profile internet companies to enact a removal policy. Reddit, Twitter and Facebook have already initiated such policies (Goel, 2015; Issac, 2015; Tsukayama, 2015).

Google will consider the removal of material only once users have submitted an online request. The final decision as to whether content should be removed remains a matter for Google (Singhal, 2015). Though Google has identified that the decision was motivated by its appreciation of the destructive nature such material has on (mostly female) victims, it is consistent with Google’s current policy of removing sensitive personal information such as bank account numbers and signatures (Singhal, 2015).

However, the announcement is not universally welcomed. The decision to remove revenge porn has been cited as a potential infringement of the right to free speech (Riley, 2015). But, the criticisms are not all centred on civil rights arguments. Legitimate concerns are raised as to how exactly the policy will be administered and how Google will deal with historic revenge porn images that have been freely available (Masnick, 2015).

The Digital Industry Group Incorporated (DIGI) made submissions to the Senate Inquiry. The Group comprises, Facebook, Google, Microsoft, Yahoo and Twitter. The group stated that under its policies.

*The non-consensual sharing of intimate images expressly violate our policies and will be removed when we become aware of them. This type of non-consensual sharing typically violates our policies in several respects, firstly, because the content is shared with the intention to bully or harass the victim; secondly, because this type of content invades privacy; and thirdly, because such images frequently contain nudity.* (The Digital Industry Group Incorporated, 2016, p. 2)

A recent ruling in Germany has meant a small victory for German citizens as requests for the deletion of intimate images shared as part of a relationship have been held to be enforceable (Oltermann, 2014). It has been reported that couples are drafting pre-nuptial agreements that include social-media clauses (Thompson, 2014). Recent events have aided in limiting the damaging consequences of ‘revenge porn’, such as the European Union Ruling on 13 May 2014 by the European Court of Justice that a person has the ‘right to be forgotten’ (Travis & Arthur, 2014). Individuals are able to request that search engines remove information, including images, if it is ‘inadequate, inaccurate, irrelevant or excessive’ (European Commission, 2014, p. 2). These measures have, in part, confirmed that there is a significant issue with the distribution of non-consensual images on the internet, the availability of those images globally, and the harm that it causes to victims.

One example of a policy response to online harassment is the creation in 2015 by the Australian government of the Office of the Children’s eSafety Commissioner, which provides a facility for children under the age of 18 years to report a sexual image of themselves that is online and causing them concern (Commonwealth of Australia, 2016b). Since its inception it has conducted 5561 online content investigations and removed over 4000 URLs containing offensive material (Office of the Children's eSafety Commissioner, 2016).
INTERNATIONAL CRIMINAL RESPONSES TO REVENGE PORN

Criminal legislative responses both in Australia and internationally have some areas of commonality that are worth observing. It would seem responses can generally be categorised as specific and non-specific. Specific responses are those that have created niche offence for revenge porn. Non-specific responses are those that rely on more generalised offences (usually already in existence) to deal with instances of revenge porn and other offences. Various legislative acts in jurisdictions around the world provide for specific revenge porn offences. Examination of some highlight that most contain generic elements; lack of consent of the individual depicted, intent to cause harm, defined harm and specificity of image type. In many cases the legislation does not mention technology specifically as being necessary for the commission of the offence (i.e. commission of the offence through internet service providers etc.).

Intent is specified and described as acting intentionally or being knowingly reckless or acting with reckless disregard in relation to the acts concerning the images. Image type is described by terms such as private sexual image, nudity, exposure of genital organs, intimate body part, sexual acts or state of undress. While these descriptions are not definitive they do provide some general background to the framework of revenge porn specific legislation. The question as to whether terms like ‘deliberate’, ‘maliciously’ or indeed, what an ‘intimate image’ all mean will likely be left to the Courts to answer unless caution and care are liberally applied to the drafting of any legislation proscribing the commission of revenge porn.

In terms of harm it is defined by such terms as individual distress, emotional distress, coercion, harassment or intimidation. Underpinning this is the impact on such offences have on the victim. The impact on each victim depends on the resilience and nature of the victim. Further, the impact would also depend on the nature of the intimate image posted. When considering impact, there is also the issue of longevity of the offence. For instance, in a physical assault that offence is committed and then ceased. While the effects may be ongoing, the act causing the offence is, in most cases, finite from a temporal perspective. This may not be true for instances of revenge porn as the offence is sustained due to difficulties that may arise in removing the intimate images from the internet, or indeed, from preventing internet users from downloading the images for perpetuity. Moreover, although an image may be removed from one source, given the distribution networks in effect, it is highly likely that image may appear on another source site and thus the offence continues.

The UK introduced a specific offence in 2014, Section 33 of the Criminal Justice and Courts Act 2015 provided:

It is an offence for a person to disclose a private sexual photograph or film if the disclosure is made—

(a) without the consent of an individual who appears in the photograph or film, and
(b) with the intention of causing that individual distress.

Of note is that although the offence does not specifically mention technology-based offences, the clear intent of the legislation was to capture those offences. The UK Secretary of State for Justice, Christopher Grayling, outlined the purpose of the amendments.

The change will cover the sharing of images both online and offline. It will mean that images posted to social networking sites such as Facebook and Twitter will be caught by the offence, as well as those that are shared via text message. Images shared via email,
on a website or the distribution of physical copies will also be caught. Those convicted will face a maximum sentence of 2 years in prison. (Grayling, 2014).

The UK provisions contain several defences to the offence including if the image is released to prevent a crime, the publication of journalistic material in the public interest, and if the material had been previously disclosed. In September 2015 Paige Mitchell was convicted under the new laws for revenge porn for disclosing private sexual photographs of another woman with intent to cause distress (The Crown Prosecutor Service, 2015). Mitchell had posted explicit photos of the victim on to her Facebook profile and captioned the pictures with humiliating insults, she was sentenced to six weeks imprisonment (The Crown Prosecutor Service, 2015).

In 2015, New Zealand introduced the section 22 of the Harmful Digital Communications Act 2015 which created the offence of sending or posting material that would deliberately cause serious emotional distress. The act provides for both criminal and civil remedies and allowed for the creation of an approved complaints agency to investigate and resolve harmful digital complaints. The Japanese Government introduced the Revenge Porn Victimization Prevention Act in 2014 after only two days’ discussion (Matsui, 2015). The legislation was criticised as being ambiguous, too specific and lenient in sentencing outcomes; concerns were also raised about it impacting on freedom of speech (Matsui, 2015).

In the United States (US) some 40 states (as of September 2018) have specific laws that deal with the issue of revenge porn (Goldberg, 2016). In Virginia, the offence is the unlawful dissemination or sale of images of another person, under section 18.2-386.2, Code of Virginia. It is one of the few revenge porn offences that mentions technology.

...an internet service provider, an electronic mail service provider, or any other information service, system, or access software provider that provides or enables computer access by multiple users to a computer server in committing acts prohibited under this section.

It stipulates that the provider is not liable for the offence for content provided by another person. Idaho provided for revenge porn offences with the offence of video voyeurism, under section 18-6609 of the Idaho Code. The Idaho provision is interesting in that it also addresses the issue of intent to cause pleasure for others by “...arousing, appealing to or gratifying the lust or passions or sexual desires of such person or another person, or for his own or another person's lascivious entertainment or satisfaction of prurient interest”.

Colorado has the offence of posting a private image for harassment section18-7-107 and posting a private image for pecuniary gain section 18-7-108, under the Colorado Revised Statutes. The sections talk of posting or distributing through social media or any website an intimate image. Intimate image is held to include external genitalia or the perineum or the anus or the pubes of any person or the breast of a female. The section also expressly provides for civil remedies to be brought against an offender.

Canada in 2014 introduced the Protecting Canadians from Online Crime Act. It amended the Criminal Code section 162.1 by adding the offence of publication etc., of an intimate image without consent. It talks about an offender who knowingly publishes, distributes, transmits, sells, makes available or advertises an intimate image of a person without consent or being reckless as to whether that person gave their consent commits the offence. It does not have a harm element. In 2016, a 29-year-old man was sentenced to 90 days jail for posting three nude photographs of his ex-girlfriend to her Facebook account after their relationship came to an
acrimonious end (Khandaker, 2016). The man was also banned from using the internet for three years as part of his supervised probation (Khandaker, 2016).

AUSTRALIA – MOVING TOWARDS A SPECIFIC CRIMINAL RESPONSE

Despite there being an ability to capture revenge porn behaviour with existing offences there have been policy moves towards the creation of specific offences. There have been criticisms of the existing laws as being inconsistent and out of date with current technological advances (Henry & Powell, 2016). In 2016, the New South Wales (NSW) Parliament held an inquiry into “Remedies for the serious invasion of privacy in New South Wales” with a specific focus on revenge porn type offences. The inquiry noted

...the evidence that the available offences fail to cover some key types of privacy invasions, particularly the ‘revenge pornography’ type scenarios. The committee acknowledges the support...for a new criminal offence of taking and disseminating intimate images without consent, or threatening to do so.” (New South Wales Parliament, 2016, p. 39).

Regardless of this acknowledgement the inquiry did not recommend new criminal offences as the committee’s remit was to consider the adequacy of existing remedies for serious invasions of privacy, not consideration of the introduction of new criminal offences (New South Wales Parliament, 2016, p. 39). Accordingly it made recommendations that the government introduce new civil proceedings facilitating a statutory cause of action for serious invasions of privacy (New South Wales Parliament, 2016).

In 2015, the Australian Labor Party introduced a bill to amend the Criminal Code Act 1995(Cth). The amendments proposed to create “new offences that will prescribe appropriate penalties for persons involved in image-based sexual exploitation, also known as ‘revenge porn’. The offences reflect the community’s increased use of telecommunications to engage in harmful and abusive behaviour of a sexual nature and the harm that can be caused.” (Australian Labor Party, 2015). The bill is yet to be passed.

The Senate Inquiry called for the creation of a range of offences to deal with revenge porn scenarios. These included knowingly or recklessly recording an intimate image without consent; knowingly or recklessly sharing intimate images without consent; and threatening to take and/or share intimate images without consent, irrespective of whether or not those images exist (Commonwealth of Australia, 2015). In submissions to the Senate Inquiry the NSW Director of Public Prosecutions stated that “the ultimate position of this Office is that a specifically targeted criminal offence would fill a gap within the existing law and go some way to addressing what is a growing- and highly damaging concern within society” (New South Wales Director of Public Prosecutions, 2016, p. 1).

An example of a specific legislative response is the Victorian response to revenge porn. Victoria created a specific offence under the Summary Offences Act 1966 - sect 41DA - Distribution of intimate image, the section in brief outlines the offence as below.

Distribution of intimate image
(1) A person (A) commits an offence if—
(a) A intentionally distributes an intimate image of another person
(B) to a person other than B; and
(b) the distribution of the image is contrary to community standards of acceptable conduct.
The act then provides the below example of the prescribed offence.

A intentionally distributes an intimate image of another person (B) to a person other than B; and the distribution of the image is contrary to community standards of acceptable conduct.

The maximum penalty for the offence is two years’ imprisonment. This offence references the use of social media and it has an additional offence that covers threats to distribute. An intimate image is defined as either a person engaged in sexual activity, a person in a manner or context that is sexual, or the genital or anal region of a person or, in the case of a female, the breasts. The second type of intimate image, ‘a person in a manner or context that is sexual’ is arguably too broad. The legislation also fails to consider instances where real images may be doctored or fabricated to appear ‘intimate’, despite their lack of authenticity.

The Victorian provision also has exclusion clauses, which include if the offence is committed by a minor and if the act is committed with consent:

B had expressly or impliedly consented, or could reasonably be considered to have expressly or impliedly consented, to—

(i) the distribution of the intimate image; and
(ii) the manner in which the intimate image was distributed.

A key aspect of the offence is the community standard as to what is acceptable conduct. This has been described by the Victorian Attorney General as follows:

The bill provides guidance to courts to determine the application of community standards of acceptable conduct in a particular case. The court is directed to consider the context in which the image was captured and distributed, the personal circumstances of the person depicted, and the degree to which their privacy is affected by the distribution. The purpose of the community standards test is to ensure that the offences do not unjustifiably interfere with individual privacy and freedom of expression, while at the same time targeting exploitative, harmful and non-consensual behaviour. (Parliament of Victoria, 2014, p. 3188).

South Australian Laws are similar to the Victorian laws, sections 26B and 26C of the Summary Offences Act 1953 (SA), create the offence of distributing an invasive image. Sections 26B and 26 C of the act creates the offence of distributing an invasive image. There are also additional offences under this Act that also make it unlawful to film a person who is subjected to, or forced to, engage in a humiliating or degrading act, and/or distributing such a film.

Western Australia has taken a different approach to combating revenge porn offences. Rather than create a standalone offence, in 2016 the West Australian government introduced Family Violence Restraining Orders (FVROs) with conditions including the banning cyber-stalking or distributing/threatening to distribute ‘intimate personal images of the person protected by the FVRO (Mischin, 2016). Those breach the conditions of the FVRO face two-year maximum sentence (Mischin, 2016).

CHALLENGES BEYOND CRIMINAL LEGISLATIVE RESPONSES

It has been noted that in some countries non-specific laws are already in existence that can deal with revenge porn situations (McGlynn & Rackley, 2015). Not all jurisdictions have rushed to
embrace specific legislative regimes. In June 2016 Governor Gina Raimondo, of Rhode Island State in the US, vetoed a specific revenge porn bill on the grounds that it would impede free speech and was too broad and vague (O’Brien, 2016). In 2016 Sweden refused to follow France in tightening its privacy regulations, arguing its laws provided enough protection and strengthening existing laws would not better protect victims of revenge porn (World Radio Switzerland, 2016). As has been noted:

*There already exists a range of offences which may cover cases of revenge porn raising the question of whether these offences are effectively enforced in relation to revenge porn and if they are whether a specific offence is necessary.* (Salter & Croft, 2015, p. 9)

The NSW inquiry noted that various sections of the *Crimes Act* create offences that may cover revenge porn scenarios and had been successfully used in *Usmanov v R*, a NSW case in which a former partner posted intimate images on Facebook without consent (New South Wales Parliament, 2016). These sections include 578C where it is an offence to publish an indecent article and various other sections that cover privacy issues. They also include the following; section 545B which prohibits annoying or intimidation of a person, and section 91 deals with a variety of voyeurism and filming offences, section 249K blackmail and section 308H unauthorised access or modification of restricted data on a computer. Currently, instances of the malicious distribution of intimate images in Queensland may, depending on the circumstances, be prosecuted as offences of extortion (section 415 *Criminal Code 1899*), unlawful stalking (s.359E *Criminal Code 1899*) and under the *Domestic Violence and Protection Act 2012*

Examples of non-specific legislation include the Federal offence of *Criminal Code Act 1995 (Commonwealth)* section 474.17, using a carriage service to menace, harass or cause offence. This section relies on the test of what a reasonable person would regard as being, in all the circumstances, menacing, harassing or offensive. There is no mention of revenge porn type offences since the section predates this phenomenon coming to notice.

The Commonwealth Director of Public Prosecutions (CDPP) has acknowledged that this section is “potentially capable of capturing parts of revenge porn conduct” (Commonwealth Director of Public Prosecutions, 2015, p. 2). The CDPP states that examples of using a carriage service include sending SMS, uploading material to social media websites and using the internet to “transmit data via e-mail or messaging applications” (Commonwealth Director of Public Prosecutions, 2015, p. 3). The CDPP stated that the most likely scenario that could be covered was “…where an individual disseminates, or threatens to disseminate, an image or recording brought into existence in intimate circumstances with a view to causing distress to the person depicted.” (Commonwealth Director of Public Prosecutions, 2015, p. 3). It is for this reason that DIGI recommended that the Senate Inquiry hearing ensure that current legislation was not sufficient to cover revenge porn type activity, before recommending new legislation (The Digital Industry Group Incorporated, 2016).

Great care must be taken when drafting legislation to combat an issue such as revenge pornography. For example, what does it mean to distribute? Does showing a friend or work colleague an image stored on an electronic device, such as a mobile phone constitute distribution? What about instances where the image is, instead of stored on a mobile phone, merely retrievable via an online ‘cloud’-like application? What if the image is not deliberately/intentionally distributed? It is submitted that any legislation that is drafted should
include both terrestrial and cyber forms of distribution to include, for example, the sharing or sending of a hard-copy photograph to another.

**ARE WE TARGETING THE RIGHT PEOPLE?**

Care must also be taken to ensure that the legislation will in fact be effective in targeting the appropriate offenders. Criticism has been levelled at the Victorian legislation with statistics revealing that almost 30 percent of offenders charged are aged between 10-17 years (Campbell, 2016). The Western Australian Attorney-General, Michael Mischin, argued the Victorian laws were targeting the wrong offenders:

*So it’s stupidity, naivety and immaturity rather than criminality and that’s not quite what we’re driving at,”* the Attorney-General said, adding that while the problem of “sexting” and “nude selfies” among young people was unacceptable and should not be ignored, criminalising children had to be a last resort. (Campbell, 2016)

In California, former Playboy model and radio host, Dani Mathers was charged under revenge porn laws for fat-shaming a 70-year-old woman by taking naked pictures of her in a gym locker room and posting them to her Snapchat account (Konstantinides & Wilkinson, 2016). The case highlights the unintended consequences that can result from revenge porn laws.

In Australia, the current Commonwealth law to deal with revenge porn covers using a carriage service to menace, harass or cause offence. It relies on the prosecution showing that the effect of releasing the image is that a reasonable person would regard it as being menacing, harassing or offensive. Women’s Minister Michaelia Cash has noted:

*Under this offence, there have been a number of successful prosecutions for revenge porn.*

One example is the Queensland woman who was in a relationship with a married man. The relationship ended and the man returned to his wife, after which he was instructed to destroy intimate images of the victim. The man did not, and his wife posted them on Facebook. The wife was charged under the Commonwealth legislation and convicted.

The authors obtained data from the Victorian Crime Statistics Agency for alleged offender incidents recorded for offence code 139 Intentionally distribute intimate image of another person, by sex and age - January 2015 to June 2017. The data shows that between January 2015 and June 2017, 23% of male offenders were aged between 10-19 years of age. Females made up 13% of offenders.

<table>
<thead>
<tr>
<th>Sex</th>
<th>Age Group</th>
<th>Jan to Jun 2015</th>
<th>Jul 2015 to Jun 2016</th>
<th>Jul 2016 to Jun 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Male</td>
<td>10-19</td>
<td>≤ 3</td>
<td>6</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>20-29</td>
<td>≤ 3</td>
<td>12</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>30-39</td>
<td>≤ 3</td>
<td>5</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>40 years and over</td>
<td>≤ 3</td>
<td>10</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>Total¹</td>
<td>8</td>
<td>34</td>
<td>60</td>
</tr>
<tr>
<td>2 Female</td>
<td>Total</td>
<td>≤ 3</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>Grand Total</td>
<td></td>
<td>10</td>
<td>40</td>
<td>67</td>
</tr>
</tbody>
</table>
THE PROPOSED LEGISLATION

Great care must be taken when drafting legislation to combat the sharing of intimate images. Consideration ought to be given to the questions and comments below in relation to the proposed addition to the Criminal Code 1899 (Qld) of section 223 and amendment of section 207A.

In regards to policing, awareness, crime rates and trends it could expected that there will be an increase in criminal convictions among persons aged 18–24 years old, as they are more likely to be engaged in the sharing of intimate images. Given this ‘at-risk’ age group, it would be prudent for the Government to develop and maintain an effective educational campaign to clearly outline the effect of the proposed legislation. There will likely be a considerable burden on cyber-factions of the Queensland Police Service.

‘Distribute’ (Section 207A) - It is understood that the term ‘distribute’ will take its meaning from the existing definition in section 207A of the Criminal Code, namely:

*distribute* includes—communicate, exhibit, send, supply or transmit to someone, whether to a particular person or not; and (b) make available for access by someone, whether by a particular person or not; and (c) enter into an agreement or arrangement to do something in paragraph (a) or (b); and (d) attempt to distribute

The Criminal Code makes it clear that, to be criminally liable, a person must intend their actions, which in this case will include the act of distribution (section 23 Criminal Code 1899). However, to be criminally liable, must a person knowingly or intentionally distribute an intimate image? Consider the following examples:

Person A uses their mobile phone to show their friend, Person B, some recent holiday photographs, and in so doing (e.g., while scrolling/browsing the photographs), A unintentionally shows an intimate image (of A’s sexual partner) to person B. The dreaded scenario of pressing ‘reply all’ to a private, intimate e-mail exchange. Person A loses, sells or lends their electronic storage device (e.g., mobile phone, camera, laptop) to another person (‘B’), which contains intimate images and Person A has forgotten or is unaware of the intimate images. Person A’s electronic storage device system may be exploited (i.e., hacked) by another person and images stored on that device may be distributed. Person A uploads a group of images as an ‘album’ to a social media website. The ‘album’ may contain an intimate image that Person A has intentionally uploaded, but unknowingly.

These scenarios may not be too far-fetched.

‘A’ may not have deleted historic images from his or her electronic device prior to selling it. ‘A’, a teacher, could allow a student to borrow their USB storage pen and B, a student, could make the explicit, nude images stored and found on the USB pen, available to the public. This example, in fact, reportedly occurred in November 2015 at a college in Western Australia (Hedley & Hondros, 2015).

---

Doctored, Fabricated and/or Altered Images. The new offence includes ‘digitally obscured’ images and images that have been altered to appear to show sexual and/or intimate imaging (proposed section 207A). When considering the detection, avoidance and prosecution of ‘great harm’ within the community, should this legislation really create criminal liability for the doctoring or fabrication of an image? For example, imposing a naked body of an unknown other (e.g., an image downloaded from the Internet of an adult movie actor – which has been shared consensually) onto the image of the head of a complainant (which, incidentally, may also have been shared consensually)?

By comparison, the Criminal Justice and Courts Act 20159 (UK) combats the disclosure of ‘private sexual photographs and films’ but expressly provides that it is not private and sexual if it does not consist of or include an image that is private and sexual, or is only private or sexual by virtue of an alteration (section 35(5) of the Criminal Justice and Courts Act 2015). So, it would seem that pasting an image of Person A’s (the complainant’s) head onto an image of an adult film star’s naked body would not create criminal liability in the UK.

‘Intimate Sexual Activity’ (Proposed section 207A), ought ‘intimate sexual activity’ be defined? Would this include, for example, a picture of a female on the beach who is cupping their breasts? Or a picture of a person eating food suggestively? These acts may not be ‘ordinarily done in public’. Section 207A determines that female, but not male, breasts are ‘sexual’. Is there a cogent reason why the male breast is not protected (i.e., is there nothing sexual about a male bare breast)? For some males, the distribution of an image of their naked chest would cause ‘distress’. This seems disjunctive with the current progression of equality. What if a picture is taken of a male showing their breasts and this person later identifies as a female? Does the distribution of the earlier image constitute an offence?

Without Consent. We merely highlight that as the proposed section 223 adopts part of the definition of consent under section 348 of the Criminal Code, the Queensland Court of Appeal has determined that consent need not be given verbally, but it must be given. Indeed, the Court went so far as to state that ‘modern females will speak up and speak their minds’ (R v Winchester [2011] QCA 374 at [126] (Fryberg J)).

‘Distress’. Why is the term ‘distress’ used and not ‘detriment’, which includes ‘emotional harm’ (359A Qld Criminal Code 1899)? Is there a proposed definition of what amounts to ‘distress’? The other only times that this word appears in the Criminal Code 1899 (Qld) is in relation to vessels and vehicles (ss 469 Wilful Damage, 398 Stealing). The plain definition of ‘distress’ (Oxford Dictionary)10 is ‘extreme anxiety, sorry or pain’.

Ought the Committee consider making it a requirement that the accused intended to cause distress? (This is the case in the UK: section 33 (1)(b) of the Criminal Justice and Courts Act 2015).11 The application of s 223(1)(b) will be interesting in the light of social media accounts where the audience to an uploaded image (i.e., consensual sharing) can be controlled (e.g., Person A allows four people to access the images uploaded to their Instagram account). Consider a situation where an intimate image is shared with several others, but subsequently non-consensually shared with another (i.e., a fifth person).

---

9 http://www.legislation.gov.uk/ukpga/2015/2/contents/enacted
10 https://en.oxforddictionaries.com/definition/distress
11 http://www.legislation.gov.uk/ukpga/2015/2/part/1/crossheading/offences-involving-intent-to-causdistress-etc/enacted
Other Legislation. Ought there be a ‘community standards’ test when prosecuting this offence, as in Victoria (s 41DA of the Summary Offences Act 1966 (Vic) (see below))? This has been described by the Victorian Attorney General in the reading of the bill into Parliament as follows:

“The bill provides guidance to courts to determine the application of community standards of acceptable conduct in a particular case. The court is directed to consider the context in which the image was captured and distributed, the personal circumstances of the person depicted, and the degree to which their privacy is affected by the distribution. The purpose of the community standards test is to ensure that the offences do not unjustifiably interfere with individual privacy and freedom of expression, while at the same time targeting exploitative, harmful and non-consensual behaviour.”

The committee should consider following the UK model in excluding criminal liability for the distribution of an intimate image to the sender (section 33(2) of the Criminal Justice and Courts Act 2015)? Ought the committee consider following the UK model in creating a defence for the distribution of an intimate image in the course of, or with a view to, the publication of journalistic material (section 33(7) of the Criminal Justice and Courts Act 2015)? Might there be aggravating circumstances: for example, the intimate image is obtained by means of the non-consensual access of the image?

**CRIME PREVENTION AS A SOLUTION**

As with any crime, solutions are much more than just circumscribing behaviours through legislation. Crime prevention strategies such as education and awareness campaigns both from government and private sectors stakeholders should also be considered as part of any response. The Senate Inquiry recommended that:

...that the Commonwealth government implement a public education and awareness campaign about non-consensual sharing of intimate images for adults by empowering and resourcing the Office of the Children’s eSafety Commissioner and the Australian Federal Police to build on their existing work with children in relation to cybersafety. (Commonwealth of Australia, 2015, p. 8).

Part of this education strategy should be ensuring that there is acceptance in the community that harm minimization and risk mitigation strategies are part of a rational response to a crime problem. DIGI recommended that the Senate Inquiry consider:

...that addressing this issue cannot be done by legislation alone and that there must be a co-ordinated initiative across government, industry and the community to promote awareness of a sense of responsibility that should dissuade people from undertaking the non-consensual sharing of images and that there are serious consequences for doing so. (The Digital Industry Group Incorporated, 2016, p. 7)

---


This issue was highlighted in a recent case in Australia where some 70 Australian schools were targeted by an international online pornography ring which saw images of female students being exchanged and posted online (Torpey, 2016). The Queensland Police Service (QPS) issued advice for parents to “…talk with their children openly about these matters and discuss the consequences of posting too much personal information, including your school, your age and your suburb online. Once this information is matched with a photo of you, then the possibilities are concerning” (Queensland Police Service, 2016). In response to this the QPS was criticised for engaging in victim blaming (Torpey, 2016).

It is not victim blaming to engage in a valid discussion of crime prevention measures. To take the above approach of victim blaming for example, advice would not be provided to tell people to secure their cars because there is an increase in stolen vehicles. This approach was highlighted in the evidence of Australian Federal Police Assistant Commissioner, Shane Connelly, when giving evidence to the Senate Inquiry. Connelly stated “people just have to grow up in terms of what they’re taking and loading on to the computer because the risk is so high,” (Merhab & Yosufzai, 2016). The Assistant Commissioner was then asked if he was victim blaming.

*Mr Connelly said he was not implying that but "wicked" people would always take advantage of the naive, and the case was the same for revenge porn, cyber-crime or online child abuse. (They say) if you go out in the snow without clothes on you’ll catch a cold - if you go on to the computer without your clothes on, you’ll catch a virus,". "It’s a wicked analogy but it’s pretty realistic." (Merhab & Yosufzai, 2016)*

It is reasonable to suggest to people steps they can take to avoid becoming a victim of crime. It is also reasonable to direct your advice to the targeted victim group. It has been noted that perhaps the best way to prevent offences of this nature from occurring is to “…discourage people from sharing such sexually explicit images without thinking about how those images might be used in the future.” (Matsui, 2015, p. 317). Identifying and educating at risk groups is also an important crime prevention strategy. For instance, young people are more likely to engage in sexting behaviour when unaware of the potential consequences (Strohmaier, Murphy, & DeMatteo, 2014).

**INVESTIGATIVE CHALLENGES**

In attempt to streamline reporting of online harassment the Australian government created an Australian Online Reporting Network (ACORN), which is a national policing initiative to facilitate the reporting of cybercrime (Commonwealth of Australia, 2016a). Crimes dealt with by ACORN include online harassment which may be inclusive of revenge porn type scenarios (Commonwealth of Australia, 2016a). There remain however, two main challenges for law enforcement.

The first challenge is anonymity of both the victim and offender. Anonymity applies to the offender committing the offence in such a way as to deliberately preserve their anonymity. Anonymity of the victim was highlighted in the above school example where the QPS noted the issue of non-reporting, “…while we have not received any formal complaints, we are working with our interstate colleagues, the AFP and the eSafety Commissioner and have conducted an initial investigation into the origin of the site” (Queensland Police Service, 2016). The concept of anonymity goes to the heart of the nature of revenge porn in that you need a complainant to come forward to act. This contrasts with child exploitation matters where the state effectively becomes the complainant in a criminal matter. In adult revenge porn cases,
there is a reliance on the complainant to firstly become aware of the matter, and then secondly report it to authorities. It has been suggested that the apparent lack of action by authorities has been taken to indicate “…that women who take and share intimate images of themselves have fallen outside the bounds of appropriate femininity and have become legitimate objects of public ridicule and disgust.” (Salter & Croft, 2015, p. 1). Henry and Powell (2016) also noted the poor enforcement in relation to revenge porn offences. It may well be reasonable to assume that revenge porn matters would suffer from similar under-reporting rates as domestic violence and sexual assault matters for similar reasons.

Secondly, offences of this kind are often transnational in nature – they occur in multiple countries and multiple legal jurisdictions. This poses investigative challenges in securing the evidence needed to prosecute. Given the online nature of revenge porn scenarios it is inevitable that cross jurisdictional boundaries will provide difficulties that police will need to be trained to overcome and have the appropriate tools to do so. This was the case in the aforementioned school case with the site being hosted overseas. The Northern Territory police noted the difficulties in relation to revenge porn complaints they had dealt with:

_In all instances the individuals posting the material have used a variety of platforms and methods to obfuscate their involvement, often using platforms that are based outside of Australia creating significant delays and difficulties in obtaining evidentiary material. In addition, it is difficult to identify the identity of the individual that actually posted the material and to identify in which jurisdiction the offence occurred._

(Northern Territory Police Force, 2016, p. 3)

The NSW inquiry recognised the difficulty in investigating revenge porn matters. Accordingly it made recommendations for better training of Police in regards to technology facilitated stalking, abuse and harassment offences (New South Wales Parliament, 2016). This lack of training was also recognised by the Senate Inquiry which recommended that Australian police undertake basic training in relation to the revenge porn scenarios and offences related to them (Commonwealth of Australia, 2015).

The submission from the Northern Territory Police was the only publicly listed submission for law enforcement in either the NSW or Australian Senate inquiries (Commonwealth of Australia, 2015; New South Wales Parliament, 2016). This could perhaps be indicative of law enforcement agencies not seeing this issue as a core policing function. In submissions to the Senate Inquiry the Northern Territory Police noted that since July 2015 they had received only six complaints to their High Tech Crime Squad referred from ACORN (Northern Territory Police Force, 2016). The police noted no matters had proceeded to trial “due to the difficulty in identifying the suspect and establishing their level of involvement, embarrassment of the victim and unwillingness to proceed with a formal complaint and be involved in the Court process” (Northern Territory Police Force, 2016, p. 2). DIGI recommended that the Senate Inquiry consider how “…existing remedies can be better promoted to victims, and enforced by the law enforcement community and the judiciary.” (The Digital Industry Group Incorporated, 2016, p. 5).

**CONCLUSION**

Although there are already offences that cover acts of revenge porn, it appears that prosecutions under these are rare. The creation of new offences may not the panacea it has been held out to be. A baseline of evidence would need to be presented to show that current legislative offences
present in Australian jurisdictions are ineffective in dealing with revenge porn related offences. The various State and Federal prosecution authorities are the custodians of this information. Additionally, it must be shown that any proposed new offences would be effective in addressing any perceived failings of the current scheme, and were simply not “window dressing” with the creation of a specific new offence.

Further to this, there needs to be more engagement from law enforcement agencies regarding this issue. In support of this better training of law enforcement personnel on how to respond and investigate offences of a revenge porn nature is required. In addition to this, crime prevention strategies in the form of community education and awareness need to be proactively undertaken with an emphasis on at risk victim populations.

There is insufficient evidence from the current laws’ success rates to justify a move to specific laws. There has also been a failure to show how these new offences are effective in tackling other deficiencies identified in responses to revenge porn offences. These issues include ensuring we have effective victim responses to revenge porn, such as strategies to increase ease of reporting and reduce under-reporting. A lack of specialisation in policing responses has also been identified in various government inquiries. Additional training for police is needed to deal with complex investigations that can involve cross-jurisdictional and transnational issues.

The role of social media platforms will also be crucial to an effective response. We must differentiate between legitimate crime prevention strategies and victim-blaming in what can be a highly emotive area. So, the upshot is that we need to give existing laws more time to see if they are effective before we implement new ones, and we must ensure any new laws are targeting the intended offenders.

Dr. Terry Goldsworthy  
Associate Professor  
Criminology Department  
Faculty of Society and Design  
Bond University  
Email - [redacted]

Dr. Matthew Raj  
Assistant Professor  
Faculty of Law  
Bond University  
Email - [redacted]

Joseph Crowley  
Senior Teaching Fellow  
Faculty of Law  
Bond University
REFERENCES

Reference List:


**LEGISLATION**

- Code of Virginia
- Colorado Revised Statutes
- Crimes Act (NSW)
- Criminal Code Act 1995 (Cth)
- Criminal Code 1899 (Qld)
- Criminal Code (Canada)
- Criminal Justice and Courts Act 2015 (UK)
- Domestic Violence and Protection Act 2012 (Qld)
- Idaho Code
- Protecting Canadians from Online Crime Act
- Revenge Porn Victimization Prevention Act 2014 (Japan)
- Summary Offences Act 1953 (SA)
- Summary Offences Act 1966 (Vic)