



Australian Government
Attorney-General's Department

15/01/2016

Submission of the Attorney-General's Department

Senate Legal and Constitutional Affairs References Committee

**“Inquiry into 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”**

Contents

1. SCOPE OF SUBMISSION	3
2. WHAT IS REVENGE PORN?	4
3. CRIMINAL AND CIVIL LAW REMEDIES	5
COMMONWEALTH CRIMINAL LEGISLATION	5
STATE AND TERRITORY CRIMINAL LEGISLATION	9
COMMONWEALTH CIVIL LEGISLATION	9
TORT LAW – BREACH OF CONFIDENCE	10
4. OTHER POLICY RESPONSES	11
TECHNOLOGY-FACILITATED ABUSE	11
EDUCATION CAMPAIGNS	11
WORKING WITH INDUSTRY	11
AUSTRALIAN CYBERCRIME ONLINE REPORTING NETWORK	12
5. COMPARABLE OVERSEAS JURISDICTIONS	13
UNITED KINGDOM	14
UNITED STATES	14
CANADA	16
NEW ZEALAND	16
6. CONCLUSION	17

1. Scope of submission

The Attorney-General's Department (the department) thanks the Senate Legal and Constitutional Affairs References Committee for the opportunity to make a submission to the Committee's inquiry into the phenomenon colloquially referred to as 'revenge porn'.

On 12 November 2015, the following matter was referred to the Legal and Constitutional Affairs References Committee for inquiry and report:

- a. 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;
- b. the impact this has on the targets of revenge porn, and in the Australian community more broadly;
- c. potential policy responses to this emerging problem, including civil and criminal remedies;
- d. the response to revenge porn taken by Parliaments in other Australian jurisdictions and comparable overseas jurisdictions; and
- e. any other related matters.

This submission focuses on paragraphs (c) and (d) of the inquiry's Terms of Reference, outlining the current civil and criminal remedies available to victims of revenge porn under Commonwealth legislation and some of the approaches taken by comparable overseas jurisdictions.

In preparing its submission, the department has consulted with the Australian Federal Police, the Commonwealth Director of Public Prosecutions, the Department of Communications and the Arts and the Office of the Children's eSafety Commissioner. The department understands that these agencies may provide separate submissions to the inquiry.

2. What is revenge porn?

The department understands the term 'revenge porn' to encompass a range of scenarios. The central issue is the non-consensual distribution of private sexual material. The material itself may have been obtained consensually or non-consensually. The relationship between victim and perpetrator, the motivation behind the distribution of the material, and the medium through which it is distributed may all vary but may still constitute the non-consensual distribution of private sexual material. Hosts of revenge porn websites also have a role in facilitating revenge porn, distinct from that of direct perpetrators.

Certain community groups have encouraged a broader understanding of revenge porn beyond images that are strictly of a 'sexual' nature; intimate, non-sexual images (for example, of a Muslim woman without her hijab) distributed without consent can be equally as damaging and traumatic for a victim and can be used in much the same way as a sexual image by a perpetrator of abuse.¹ In preparing this submission, the department has considered the non-consensual distribution of private non-sexual material to be outside the scope of the definition of 'revenge porn'.

The most common understanding of revenge porn involves an ex-partner of the victim using material previously provided consensually as leverage—in order to force the victim to return to the relationship—or as revenge following the end of a relationship. There is evidence to suggest that revenge porn in this context is increasing. A recent survey of domestic violence workers conducted by the Domestic Violence Resource Centre Victoria, Women's Legal Services New South Wales, and Women's Services Network reported that 35 per cent of respondents had clients who 'often' mentioned that their abusers had threatened to distribute or post private photos or videos of them.²

The department notes the concerning prevalence of revenge porn in the context of domestic violence. This appears to be linked to a broader phenomenon that has arisen from the take up of mobile technologies, higher rates of online connectivity and the risks to privacy this presents.

¹ See for example Submission from Women's Legal Services New South Wales to Mr Tim Watts MP, 1 October 2015, 3-4 <<http://www.wlsnsw.org.au/wp-content/uploads/WLS-NSW-Sub-to-Criminal-Code-Amendment-Private-Sexual-Material-Bill-2015-Exposure-Draft-fa1.pdf>>.

² D Woodlock, 'Remote control' (2015) 1 (Autumn/Winter) *DVRCV Advocate* 37.

3. Criminal and civil law remedies

Criminal and civil remedies have distinct roles to play in responding to revenge porn. This submission comments on the relevant Commonwealth provisions, and does not consider the adequacy of state and territory legislation.

Constitutional limitations

Under the federal system of government established by the Australian Constitution, powers are distributed between the Commonwealth and the states and territories. The power of the Commonwealth Parliament to make laws is limited to particular subjects, most of which are listed in sections 51 and 52 of the Constitution. However, with only a few exceptions, a state parliament can make laws on any subject of relevance to that state. For this reason, criminal law is largely the responsibility of states and territories.

However, there are exceptions to this rule. In particular, where the Commonwealth has legislative power with respect to a subject matter, it can create criminal offences in respect of the subject matter. For example, section 51(xxix) of the Constitution—the external affairs power—allows the Commonwealth Parliament to make criminal legislation for the purposes of ensuring Australia's compliance with an international treaty. Also relevant, particularly with regard to a discussion of cyber offences, is section 51(v) of the Constitution, which provides the Commonwealth the power to make laws with respect to postal, telegraphic, telephonic, and other like services. This has been interpreted as giving the power to make laws with respect to 'carriage services', which includes telecommunications networks and the internet.

Commonwealth criminal legislation

A number of Commonwealth criminal offences may be relevant to revenge porn.

Criminal Code Act 1995 (Cth)

The *Criminal Code Act 1995* (Cth) (the Criminal Code) contains a range of offences criminalising the use of telecommunications and postal services to engage in inappropriate behaviour, as well as child pornography offences which may be relevant where revenge porn involves images depicting minors. Due to constitutional limitations, there is no Commonwealth offence that may apply where a perpetrator of revenge porn disseminates private sexual material in some other way—for instance, by leaving it on the doorstep of the victim's parents' house or in some other public place in order to shame/threaten the victim. The Commonwealth offences also do not cover threats to disseminate revenge porn.

Telecommunications

Section 474.17 of the Criminal Code makes it an offence to use a carriage service, including the internet, social media services or a telephone, in a way that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive.

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

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

(a) the person uses a carriage service; and

(b) the person does so in a way (whether by the method of use or the content of a communication, or both) that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive.

Penalty: Imprisonment for 3 years.

Consistent with the principles set out in Chapter 2 of the Criminal Code, the individual concerned must have intended to use the carriage service and have been reckless as to whether they were using a carriage service in a way that the reasonable person would regard in all the circumstances as menacing, harassing or offensive.³

The 'reasonable person' test in section 474.17 allows for community standards and common sense to be taken into account when determining whether certain conduct or content of a communication is in fact menacing, harassing or offensive.

Under section 473.4 of the Criminal Code, matters to be taken into account when deciding whether reasonable persons would regard particular material or use of a carriage service as being offensive include:

- the standards of morality, decency and propriety generally accepted by reasonable adults
- the literary, artistic or educational merit (if any) of the material, and
- the general character of the material (including whether it is of a medical, legal or scientific character).

As outlined in the explanatory memorandum for this provision, examples of the type of use of a carriage service the proposed offence may cover include use that would make a person apprehensive as to their safety or well-being or the safety of their property, use that encourages or incites violence, and use that vilifies persons on the basis of their race or religion.⁴

The Commonwealth Director of Public Prosecutions advises that there have been 691 charges proven against 397 defendants under section 474.17 of the Criminal Code since its introduction in 2004.⁵ Whilst it is difficult to generalise examples of conduct for offences against section 474.17, it regularly includes:

- repetitive unwanted calls/SMS to a victim's mobile telephone
- use of a telephone to call/SMS a victim and threaten them, and
- use of a telephone to transmit unwanted sexual material to a victim.

Postal services

Where the private sexual material has been distributed using a postal service, section 471.12 of the Criminal Code may apply.

³ *Criminal Code Act 1995* (Cth) ss 5.6(2), 5.2, 5.4.

⁴ Explanatory Memorandum, *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill (No. 2) 2004*, 34.

⁵ This information was extracted from the Commonwealth Director of Public Prosecutions' database on 4 January 2015.

471.12 Using a postal or similar service to menace, harass or cause offence

A person is guilty of an offence if:

(a) the person uses a postal or similar service; and

(b) the person does so in a way (whether by the method of use or the content of a communication, or both) that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive.

Penalty: Imprisonment for 2 years.

This offence carries the same fault elements as section 474.17—the person must have intended to use a postal or similar service, and have been reckless as to whether they were doing so in a way that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive. It also relies on section 473.4 as to matters that may be taken into account in deciding whether particular material is offensive.

Child pornography

There are additional Commonwealth offences that may be relevant if a private sexual image/video is of a person under 18.

Section 473.1 of the Criminal Code defines child pornography to mean material that depicts a person who is, or appears to be, under 18 years of age and who is engaged in a sexual pose or sexual activity. Thus, the image(s) distributed as part of sexting or as revenge porn may constitute child pornography due to the age of the victim depicted.

Sections 474.19 and 474.20 of the Criminal Code criminalise the use of a carriage service for child pornography material, as well as possessing, controlling, producing, supplying or obtaining child pornography material for use through a carriage service.

474.19 Using a carriage service for child pornography material

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

(a) the person:

(i) accesses material; or

(ii) causes material to be transmitted to himself or herself; or

*(iii) transmits, makes available, publishes, distributes, advertises or promotes material;
or*

(iv) solicits material; and

(aa) the person does so using a carriage service; and

(b) the material is child pornography material.

Penalty: Imprisonment for 15 years.

474.20 Possessing, controlling, producing, supplying or obtaining child pornography material for use through a carriage service

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

(a) the person:

(i) has possession or control of material; or

(ii) produces, supplies or obtains material; and

(b) the material is child pornography material; and

(c) the person has that possession or control, or engages in that production, supply or obtaining, with the intention that the material be used:

(i) by that person; or

(ii) by another person;

in committing an offence against section 474.19 (using a carriage service for child pornography material).

Penalty: Imprisonment for 15 years.

Prosecuting minors under these Commonwealth offences requires the consent of the Attorney-General, who will give consideration to the serious nature and circumstances of the alleged offending, amongst other factors. The consent requirement is intended to act as a safeguard to prevent the unnecessary prosecution of young persons (for instance, in incidences of consensual 'sexting'). The Supplementary Explanatory Memorandum to the *Crimes Legislation Amendment (Sexual Offences Against Children) Bill 2010* envisages that consent be granted in cases where the conduct is malicious or exploitative and the practice to date has reflected this approach.

Section 474.25 of the Criminal Code establishes offences related to the obligations of internet service providers and internet content hosts with regard to child pornography and child abuse material.

474.25 Obligations of internet service providers and internet content hosts

A person commits an offence if the person:

(a) is an internet service provider or an internet content host; and

(b) is aware that the service provided by the person can be used to access particular material that the person has reasonable grounds to believe is:

(i) child pornography material; or

(ii) child abuse material; and

(c) does not refer details of the material to the Australian Federal Police within a reasonable time after becoming aware of the existence of the material.

Penalty: 100 penalty units.

No other provision in the Criminal Code creates an equivalent obligation for internet service providers or internet content hosts to notify law enforcement of potentially illegal online material.

State and territory criminal legislation

As revenge porn encompasses a broad range of conduct, a number of state and territory criminal offences may be applicable. For example, traditional criminal offences such as harassment, stalking, blackmail and indecency may be relevant. In addition, Victoria and South Australia have passed legislation specifically addressing revenge porn in their respective Summary Offences Acts.⁶ The New South Wales Parliament has also recently announced an inquiry into serious invasions of privacy that will consider the growing trend of revenge porn.⁷ States and territories also have their own child pornography offences as well as 'sexting' offences in certain jurisdictions.

Commonwealth civil legislation

While criminal law provides one avenue for responding to revenge porn, areas of civil law may be of relevance, including privacy law, the take-down powers of the recently established Office of the Children's eSafety Commissioner, and tort law.

Privacy law

The Commonwealth's *Privacy Act 1988* (Privacy Act) is the principal piece of Australian legislation protecting the handling of personal information about individuals. Most states and territories, with the exception of South Australia and Western Australia, have equivalent legislation. The existing Commonwealth, state and territory legislation applies to major organisations that collect and store personal information, such as banks, large retailers, government departments and utilities providers.

Generally, the Privacy Act does not regulate the actions of individuals. Instead, it regulates the activities of government agencies and many private sector organisations (those with an annual turnover of \$3 million or more). To the extent individuals carry on a business that shares personal information, the small business exception may not apply and the business activities of the individual will thus fall under the Privacy Act.⁸ While it may be difficult to determine the geographic home of a website or company, the Privacy Act will regulate the actions of a website or company where there is an 'Australian link'.⁹ Websites or companies that host content or 'hold' personal information may be considered a small business if they 'disclos[e] personal information about another individual to anyone else for a benefit, service or advantage' or 'provid[e] a benefit, service or advantage to collect personal information about an individual from anyone else'.¹⁰

⁶ See *Summary Offences Act 1966* (Vic) ss 41DA, 41DB and *Summary Offences Act 1953* (SA) s 26C.

⁷ New South Wales Parliament Legislative Council, Standing Committee on Law and Justice, 'Serious invasions of privacy in New South Wales—how adequate are our remedies?' (Media Release, 6 July 2015).

⁸ *Privacy Act 1988* (Cth) ss 6C(1), 6D(4).

⁹ *Ibid* ss 5B(2)-(3).

¹⁰ *Ibid* ss 6D(4)(c)-(d).

Personal information (including sensitive information) may in some instances be relevant to revenge porn and thus the Privacy Act may have some remit regarding revenge porn website hosts. The department notes that the Office of the Information Commissioner (OAIC) does not have power in relation to criminal sanctions, but only has general regulatory powers and the ability to make determinations on privacy complaints to the OAIC.

The Australian Law Reform Commission 2014 report *Serious Invasions of Privacy in the Digital Era* also considered the issue of the reduction of and remedies for, serious invasions of privacy in the digital era, including the legal design of a statutory cause of action. The Australian Government does not support a tort of privacy.

The New South Wales Parliament has commenced an inquiry into remedies for the serious invasion of privacy that will consider, amongst other issues, the growing trend of revenge porn.

Office of the Children's eSafety Commissioner

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).

Among other functions, it administers a complaints system to get harmful cyber bullying material targeted at Australian children down quickly from large social media sites. Revenge porn involving young people under 18 years of age would likely constitute harmful material targeted at an Australian child and be the type of material for which the Office could issue takedown notices to large social media services (section 35 of the Act), and end user notices and formal warnings to end users for non-compliance with a notice (sections 42-44 of the Act). To date the Office has worked collaboratively with social media partners and not needed to use its formal powers to remove content. An extension of this type of cooperation with social media services to revenge porn matters may assist in getting images down quickly. Additionally civil penalties to end-users in these matters could act as a deterrent and assist rapid removal of material online.

The Office can also investigate complaints about child sexual abuse material and other illegal content that is hosted online, including the sharing of sexual images of Australian children. The Office has take-down powers for Australian-hosted online content, and applies criteria set out in the Classification Guidelines to determine if takedown thresholds are met. The Office also 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.

Tort law – breach of confidence

Breach of confidence is a common law remedy individuals can use to protect their personal information and recover compensation. Essential elements of an action in equity for breach of confidence are that the information was of a confidential nature, that it was communicated or obtained in circumstances importing an obligation of confidence, and that there was an unauthorised use of the information.¹¹ There have been two successful breach of confidence cases involving revenge porn scenarios—*Wilson v Ferguson* in the Supreme Court of Western Australia (2015) and *Giller v Procopets* in the Supreme Court of Victoria (2008). Tort law is a matter for states and territories.

¹¹ *Wilson v Ferguson* [2015] WASC CIV:2514/2013 (16 January 2015) [46].

4. Other policy responses

Technology-facilitated abuse

On 17 April 2015, the Council of Australian Governments (COAG) agreed to take urgent collective action to address the unacceptable level of violence against women, including considering strategies 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.

As a result, the Law, Crime and Community Safety Council (LCCSC) tasked the National Cybercrime Working Group (NCWG) to report back on possible areas of action for all Australian jurisdictions to address technology-facilitated abuse of women. As Secretariat for the NCWG—a national cross-jurisdictional body of senior law enforcement and justice officials—the department led the development of this report for COAG. This process identified growing concerns across all jurisdictions that revenge porn is becoming a frequent tool for perpetrators of abuse against women. The NCWG's report considered actions for all jurisdictions to raise awareness of technology-facilitated abuse, to ensure the adequacy of the legal framework to address this type of abuse, and to support law enforcement and front line services in the collection of evidence of technology-facilitated abuse.

On 11 December 2015, COAG considered the report and agreed to actions to limit technology-facilitated abuse. The NCWG will continue to support LCCSC to deliver COAG's objectives.

Education campaigns

Consideration of the legal remedies available to victims of revenge porn should not outweigh the important role that education has to play in reducing and preventing such behaviours.

In partnership with Microsoft, the Commonwealth Bank of Australia, and Datacom, the Australian Federal Police manages and delivers the national ThinkUKnow cyber safety program. Cyber safety presentations are delivered face-to-face to parents, carers, teachers, and school children, by 500-plus trained and accredited industry volunteers (who are also police checked), as well as by state and territory police (youth liaison and crime prevention officers). Preventative messaging in relation to inappropriate online behaviour and 'sextortion' is included in ThinkUKnow cyber safety presentations, as well as online at www.thinkuknow.org.au. Topics covered include risks associated with online grooming, inappropriate content, cyber-bullying and scams, fraud and identity theft.

The department welcomes the recent addition to the functions of the Office of the Children's eSafety Commissioner, to support and empower Australian families and women at risk of technology-facilitated domestic or family violence. In particular, the Office of the Children's eSafety Commissioner will provide preventative education and materials to Australians in relation to respectful relationships and the prevention of technology-facilitated domestic violence of which the sharing of private sexual material without consent is a component.

Working with industry

Addressing revenge porn requires the continuing goodwill of the government's private sector partners. Service providers of online communities and social media networks have an important role to play by

responding promptly and effectively to reports of offensive online content, including where that applies to instances of revenge porn.

The department notes that many service providers have taken a proactive approach to combatting revenge porn online. Early in 2015, Reddit and Facebook made announcements banning nude or sexually explicit images posted without permission of the individuals depicted. Twitter's policy now includes intimate photos and videos on the list of private information that should not be published without consent, as does Periscope, the new live streaming application purchased by Twitter in March 2015. Google announced in June 2015 that it would begin treating sexually explicit images the same way it treats other sensitive personal information—that is, removing them from search results if they are published without consent. Microsoft made a similar announcement in July 2015, and established a new reporting page to make the process easier.

Australian Cybercrime Online Reporting Network

The Australian Cybercrime Online Reporting Network (ACORN) is an online reporting facility which allows members of the public, and small to medium businesses, to securely report cybercrime, such as hacking, denial of service attacks, scams, fraud, identity theft, and attacks on computer systems. The ACORN also accepts reports of online harassment, which may include revenge porn. When submitting a report through the ACORN, where the user has identified the initial report category of 'cyber bullying, sexting, online harassment or stalking', and the material or images involve a person over the age of 18, the ACORN will ask the user whether the incident involved the sharing of any inappropriate sexual images without permission.¹²

Importantly, the ACORN is not set up for urgent investigations and is not an appropriate reporting channel for life-threatening situations, including those involving domestic violence.

The information submitted in an ACORN report may be forwarded to federal, state, local, or international law enforcement or regulatory agencies within the relevant jurisdictions. However, investigation and prosecution is at the discretion of the receiving state and territory agencies. Not all reports to the ACORN will be referred or investigated. However, all reports are treated seriously and help law enforcement and government agencies to develop a clearer picture of cybercrime trends.

¹² Where the material or images involve a person under the age of 18, the ACORN will refer the user to law enforcement as well as the Office of the Children's eSafety Commissioner. Given the seriousness of these offences and the need to act immediately, the ACORN does not accept reports on online offences against children.

5. Comparable overseas jurisdictions

The following table outlines the key features of the relevant laws in the United Kingdom, the United States, Canada and New Zealand. Illinois and California have been selected as two examples of state legislation from the United States, noting that many more domestic jurisdictions there have criminalised revenge porn.

	Conduct	Fault element	Applies to offline conduct	Maximum imprisonment
United Kingdom NB. Scotland's legislation introduced but not yet passed	<i>England & Wales</i> Disclosing a private sexual photo/film without consent	<i>England & Wales</i> Intent to cause distress	<i>England & Wales</i> ✓	<i>England & Wales</i> Two years
	<i>Scotland</i> Disclosing/threatening to disclose an intimate photo/film without consent	<i>Scotland</i> Intent to cause fear/alarm/distress or reckless as to whether the victim will be caused fear/alarm/distress	<i>Scotland</i> ✓	<i>Scotland</i> Five years
United States NB. Federal legislation drafted but not yet introduced	<i>Federal</i> Reproducing/distributing/exhibiting/publishing/transmitting/otherwise disseminating a nude/sexually explicit image without consent	<i>Federal</i> Knows/should have known that such conduct would likely cause emotional distress to a reasonable person if that person were so depicted	<i>Federal</i> ✓	<i>Federal</i> Five years
	<i>Illinois</i> Non-consensual dissemination of private sexual images	<i>Illinois</i> Knows/should have known that the person in the image has not consented to the dissemination	<i>Illinois</i> ✓	<i>Illinois</i> Three years
	<i>California</i> Distributing intimate/sexual images where the person depicted suffers serious emotional distress	<i>California</i> Knows/should know that distribution of the image will cause serious emotional distress	<i>California</i> ✓	<i>California</i> Six months
Canada	Publishing an intimate image without consent	Being reckless as to whether or not that person gave their consent	✓	Five years
New Zealand	Posting an intimate visual recording which causes serious emotional distress to the victim and would cause such harm to an ordinary reasonable person in the position of the victim	Intent to cause serious emotional distress	✗	Two years

United Kingdom

England and Wales have outlawed revenge porn with the *Criminal Justice and Courts Act 2015*, which specifically states that it is an offence for a person to disclose a private sexual photograph or film if the disclosure is made without the consent of the individual who appears in the photograph or film, and with the intention of causing that individual distress.¹³ The law includes the sharing of these images without consent both on and offline and includes the physical distribution of images. Offenders face up to two years in prison. Revenge porn is defined as photographs or films which show something not of a kind ordinarily seen in public, depicting either an individual's exposed genitals or pubic area, or something that a reasonable person would consider to be sexual because of its nature, or content, taken as a whole.

Scotland's Parliament introduced the *Abusive Behaviour and Sexual Harm Bill* on 8 October 2015, criminalising the disclosure of, or threat to disclose, a photograph or film of a victim in an intimate situation where the perpetrator intends to cause the victim fear, alarm or distress (or is reckless as to whether the victim will be caused fear, alarm or distress).¹⁴ The offence carries a maximum penalty of five years' imprisonment. The offence is aggravated where it involves an intention to cause physical or psychological harm to a partner or ex-partner, including fear, alarm or distress. A person is defined as being in an 'intimate situation' if engaging in an act which a reasonable person would consider to be a sexual act, and is not of a kind ordinarily done in public, or the person's genitals, buttocks or breasts are exposed or covered only by underwear.

United States

For several years now, there has been a growing debate in the United States about the adequacy of existing legal frameworks to address revenge porn. Although American privacy and copyright laws appear to provide avenues for redress in certain cases, critics have dismissed the suitability of these civil law remedies to address revenge porn, citing the cost of civil litigation and the conceptual diminishing of a revenge porn matter to one of property law as key challenges to this approach.¹⁵

The draft *Intimate Privacy Protection Act*—yet to be introduced—proposes to make it a federal crime, by providing that it is unlawful to reproduce, distribute, exhibit, publish, transmit, or otherwise disseminate a visual depiction of a person who is nude or partially nude or engaged in sexually explicit conduct, regardless of whether the depicted person consented to the capture of the image.¹⁶ The perpetrator must have known, or should have known, that such an act would likely cause emotional distress to a reasonable person if that reasonable person were so depicted. The offence carries a maximum five year penalty. Notably, the offence can also apply to telecommunications and internet service providers who fail to remove the content in question within 48 hours of receiving a notice of such content from the victim, the victim's legal representative, or a law enforcement officer.

¹³ *Criminal Justice and Courts Act 2015* (UK) s 33 <<http://www.legislation.gov.uk/ukpga/2015/2/section/33/enacted>>.

¹⁴ *Abusive Behaviour and Sexual Harm Bill* (Scot) s 2 <[http://www.scottish.parliament.uk/S4_Bills/Abusive%20Behaviour%20and%20Sexual%20Harm%20\(Scotland\)%20Bill/S4SPBil81S042015.pdf](http://www.scottish.parliament.uk/S4_Bills/Abusive%20Behaviour%20and%20Sexual%20Harm%20(Scotland)%20Bill/S4SPBil81S042015.pdf)>.

¹⁵ DK Citron and MA Franks, 'Criminalizing revenge porn' (2014) 49 *Wake Forest Law Review* 345.

¹⁶ Rep. Jackie Speier, 'Intimate Privacy Protection Act of 2015 Discussion Draft' (2015) *Historical and Topical Legal Documents*, Paper 1003 <<http://digitalcommons.law.scu.edu/historical/1003>>.

26 states have outlawed revenge porn. The criminal offences of two states in particular—Illinois and California—are worth considering. Notably, neither state requires intent to cause emotional distress, however, California requires that the person depicted suffers serious emotional distress, while Illinois' legislation does not.

Illinois

Illinois' revenge porn legislation criminalising the non-consensual dissemination of private sexual images came into effect from 1 June 2015.¹⁷ The law does not require that the offender have the intent to cause emotional distress to the victim, unlike other states' laws. In addition to establishing a three year maximum sentence, it includes an additional provision requiring forfeiture of any profits derived from the distribution of the material. Furthermore, it considers whether a reasonable person would know or understand that the image was to remain private and that the person depicted has not consented to the dissemination, deterring secondary recipients from forwarding and redistributing the images. Importantly, the images do not necessarily have to be spread by the internet to qualify as an offence. Finally, the Illinois law applies when a victim is identifiable from his or her face as well or when other identifying information is displayed in connection with the image ('doxxing').

California

As of September 2015, the *California Penal Code* sections 647(j)(4)(A) and 647(j)(4)(B) expressly prohibit what the Californian Attorney General Kamala Harris refers to as 'cyber exploitation'—the non-consensual distribution and publication of intimate photos or videos.¹⁸ It is illegal for any person to intentionally distribute an image of an intimate body part or parts of another identifiable person, or an image of the person depicted engaged in an act of sexual intercourse, sodomy, oral copulation, sexual penetration, or an image of masturbation by the person depicted or in which the person depicted participates, when the persons agree or understand that the image shall remain private. The person distributing the image is criminally responsible when he/she knows or should know that the distribution of the image will cause serious emotional distress, and the person depicted suffers that distress.

In addition to the offences above, victims of cyber exploitation also have a private right of action against their perpetrators under California law. *Assembly Bill No. 2643* codified a private right of action against any person who intentionally distributes a photograph or recorded image of another without consent, if: (1) the person knew that the other person had a reasonable expectation that the material would remain private, (2) the distributed material exposes an intimate body part or shows an act of intercourse, oral copulation, sodomy, or other act of sexual penetration, and (3) the other person suffers general or special damages as described in Civil Code section 48(a). A victim may also be able to bring a tort claim for the public disclosure of private fact and/or the intentional infliction of emotional distress depending on the circumstances of the case.

¹⁷ *Criminal Code of 2012*, 720 ILCS 5/ s 5/11-23.5 (2014)

<<http://www.ilga.gov/legislation/ilcs/ilcs4.asp?DocName=072000050HArt%2E+11&ActID=1876&ChapterID=53&SeqStart=14300000&SeqEnd=20800000>>.

¹⁸ Cal Penal Code, s 647 (2015) <<http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=639-653.2>>; the department also notes that s 653.2(a) criminalises behaviour that encompasses 'puppeting' revenge porn, i.e. where a perpetrator might post a provocative image of the victim with personally identifiable details 'for the purpose of imminently causing that other person unwanted physical contact, injury or harassment, by a third party.'

In January 2015, Californian Attorney General Kamala Harris convened a task force of 50 major technology companies (including Microsoft, Google, Facebook, Yahoo, and Twitter), victims' advocates, and legislative and law enforcement leaders to fight cyber exploitation. A result of this work has been an online resource hub launched in October 2015, with tools for victims, the technology industry and law enforcement agencies to combat cyber exploitation.¹⁹

Canada

Canada's 2014 *Protecting Canadians from Online Crime Act* was introduced primarily to address cyber bullying concerns and amends the Canadian *Criminal Code* to provide for a new offence of non-consensual distribution of intimate images.²⁰ It also makes complementary amendments to authorise the removal of such images from the internet and the recovery of expenses incurred to obtain the removal of such images, the forfeiture of property used in the commission of the offence, a recognisance order to be issued to prevent the distribution of such images and the restriction of the use of a computer or the internet by a convicted offender. The offence is punishable by up to five years' imprisonment.

'Intimate image' means a visual recording of a person made by any means including a photographic, film or video recording, in which the person is nude, is exposing his or her genital organs or anal region or her breasts or is engaged in explicit sexual activity; in respect of which, at the time of the recording, there were circumstances that gave rise to a reasonable expectation of privacy; and where the person depicted retains a reasonable expectation of privacy at the time the offence is committed.

New Zealand

New Zealand's 2015 legislation—the *Harmful Digital Communications Act 2015*—makes it an offence to post a digital communication with the intention to cause harm, with a sentence of up to two years' imprisonment (including an offence of refusing to remove the offending material).²¹ Digital communication includes an intimate visual recording of another individual, who is in a place which, in the circumstances, would reasonably be expected to provide privacy, and the individual is either naked or has his or her genitals, pubic area, buttocks, or female breasts exposed, partially exposed, or clad solely in undergarments; or engaged in an intimate sexual activity; or engaged in showering, toileting, or other personal bodily activity that involves dressing or undressing. Harm means serious emotional distress.

The Act also 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 and gives the District Court the power to issue orders such as take-down notices and impose penalties on people who do not comply with court orders (punishable by up to six months' imprisonment or a fine).

¹⁹ See <<https://oag.ca.gov/cyberexploitation>>.

²⁰ *Criminal Code*, RSC 1985, c C-46, ss 162.1-162.2 <<http://laws-lois.justice.gc.ca/eng/acts/C-46/page-85.html#docCont>>.

²¹ *Harmful Digital Communications Act 2015* (NZ) s 22

<<http://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html#DLM5711856>>.

6. Conclusion

This submission has outlined the existing Commonwealth offences potentially applicable to revenge porn—namely, provisions pertaining to the use of a carriage or postal service to menace, harass or cause offence, as well as online child pornography offences. The submission also provides an overview of comparable overseas jurisdictions' approaches to criminalising revenge porn. The department acknowledges the importance of criminal offences to address acts of revenge porn, but also notes the potential for civil law approaches to address the needs of revenge porn victims.

Ultimately, while the law plays an important role in deterring individual behaviour, the department notes that enforcement, education and community support services are also all essential features of a holistic government response to revenge porn.