# *Image-Based Abuse, Non-Consensual Pornography, Revenge Porn: A Study of Criminalization and Crime Prevention in Australia and England & Wales*

***Majid Yar***[1]
University of Hull, United Kingdom

***Jacqueline Drew***[2]
Griffith Criminology Institute, Australia

***Abstract***
*Distribution of nude, intimate and sexualized images of individuals without consent and against the wishes of those individuals whose image has been captured, is of growing concern across the world. Moving from the conceptualization of 'revenge porn' in the early 2000's, through to our more sophisticated understanding of the issues of "image-based abuse" and "non-consensual pornography" this paper considers the broad context of these crimes. The paper draws on the concepts of online misogyny, gender-based victimization, and "toxic masculinity". The progress towards criminalization of such online abuse, with reference to the recent introduction of new laws in England & Wales and Australia is examined. This shift from voluntary to statutory regulation, and from civil to criminal law remedies has been coupled with new crime prevention and control initiatives that seek to encourage reporting leading to prosecution and educate users and empower victims. As countries successively tackle image-based abuse through their own criminal justice systems and stakeholder engagement, there is a need to learn from and critique what has already been established. Summarizing the approaches undertaken in England & Wales and Australia we draw important conclusions that are based on the experiences of early responders, bringing together several best practices for the prevention and response to image-based abuse.*

Keywords: Image-Based Abuse, Revenge Pornography, Cybercrime.

[1] Professor of Sociology and Associate Director of the Centre for Criminology and Criminal Justice (School of Social Sciences), University of Hull, Cottingham Rd, Hull HU6 7RX, United Kingdom. Email: m.yar2@lancaster.ac.uk
[2] Senior Lecturer, Griffith Criminology Institute, Griffith University, Messines Ridge Road, Mt Gravatt, Queensland, Australia. Email: j.drew@griffith.edu.au

## Introduction

The dissemination of nude, intimate and sexualized images of individuals (overwhelmingly female), without the consent and against the wishes of those pictured, has become of late a high-profile internet-based problem. It was initially identified and discussed in the early 2000s under the rubric of 'revenge porn' and correspondingly associated with vengeful acts of humiliation perpetrated by disgruntled ex-intimates and former romantic partners. More recently, new terminology has emerged including that of "image-based abuse" and "non-consensual pornography", signaling a broader understanding of the problem, and the fact that it extends beyond revenge by ex-intimates to include also covertly produced images and video recordings (such as so-called "upskirting", "downblousing" and "creepshots") and material that has been hacked or otherwise stolen before being shared online via social networking platforms, blogs and dedicated websites (Stokes, 2014: 930). While early responses were oriented very much to self-regulation through content removal by web hosts, social media services and ISPs, the past few years have seen a decisive shift through the introduction of criminal statutes and corresponding sanctions in numerous countries, including the US, England & Wales and Australia. This shift from voluntary to statutory regulation, and from civil to criminal law remedies, is being matched by new crime prevention and control initiatives that seek to encourage reporting leading to prosecution, educate users and empower victims.

This paper pursues a number of inter-connected aims. Firstly, it charts briefly the rise of image-based abuse (henceforth IBA) as a social problem, and situates its emergence within the broader context of online misogyny, gender-based victimization, and an anti-feminist backlash that has licensed a "toxic masculinity" which embraces the use of sexual humiliation and abuse as an instrument of patriarchal control. Consequently, we argue that the heightened awareness of the problem in public and policy domains has to be seen in connection with a broader critique of entrenched socio-cultural sexism and discrimination, as championed for example by the #MeToo movement.

Secondly, this paper details the moves to criminalize such online abuse, looking in particular at the recent introduction of new laws in England & Wales and Australia[3]. It also draws upon formative developments in the United States and elsewhere.

Thirdly, it maps the kinds of user-oriented crime prevention initiatives aimed at curtailing the incidence of online IBA and bringing offenders to justice, with a comparative focus upon endeavors in Australia and England & Wales. The effectiveness of these legally-based crime control initiatives is assessed and potential or actual impediment to effective response are identified. Our choice of these two jurisdictions for analysis is driven a number of factors: both have introduced laws criminalizing IBA over the same recent period (2013-18); the laws define the problem of sexual IBA in broadly similar ways and make similar provisions in terms of sanctions and, in tandem with the innovations in criminal law, both have introduced concurrently measures aimed at crime reporting, user education and prevention, such as hotlines, public information campaigns

[3] We restrict our view to England & Wales rather than the UK, as the separate legal jurisdictions of Scotland and Northern Ireland have made their own separate provisions. In respect of Australia, we look at legal developments at both State and Federal levels, as revenge porn laws have been enacted at both.

and advisory materials. This concurrence of parallel measures enables us to assess the developments and their effectiveness in comparative terms (Bennett, 2004). However, as will be discussed later, they also diverge in a number of notable respects.

## *1. THE RISE OF REVENGE PORN, NON-CONSENSUAL PORNOGRAPHY AND IMAGE-BASED ABUSE*

While it is difficult to date with precision the emergence of IBA, its appearance appears to have been conterminous with the popular uptake of the internet and World Wide Web in the mid-1990s. Early discussion of the phenomenon was very much encapsulated within accounts of a wider problem associated with cyber-stalking and online harassment. In the context of such offences, former intimates distributed online nude and sexual photographs of their ex-partners, typically following the acrimonious breakdown of a relationship – what one commentator dubs "pornographic souvenirs from relationships gone sour" (Hill, 2011). The intent to humiliate, embarrass and hurt those photographed through these disclosures explains why the practice came to be quickly associated with "revenge", and was in many instances part of a more concerted and wide-ranging campaign of harassment, intimidation and vilification (through, for example, spreading lies and misinformation about the targeted individuals, or sending them abusive messages via email or other electronic communication channels) (Yar and Steinmetz, 2019). In many such cases, the identities and personal details of those depicted are also shared, thereby both exacerbating the distress experienced and giving licence to other internet users to abuse and stalk the victim.

Over time, as the practice of sharing (and viewing) such images expanded, a range of other motivations have also come to the fore, including a desire for notoriety, sexual gratification, and economic gain (the latter generated by advertising revenue on image-hosting sites or extorting victims by demanding a "take down fee" for removing the offending content) (Stroud, 2014; Fletcher, 2014; Franklin, 2014; BBC News, 2015). In other words, "revenge porn" in its strict sense is in fact part of a "continuum of image-based sexual abuse" (McGlynn, Rackley & Houghton, 2017).

Opportunities for offenders (those engaging in unauthorized online sharing of sexual images) have become more readily available in consequence of a number of communications-related developments, including: 1. the growth of "sexting" behavior, in which individuals voluntarily share nude and provocative images, videos or text with current or prospective intimates (Crofts, Lee, McGovern & Milivojevic, 2016; Lenhart, 2009; Mitchell, Finkelhor, Jones & Wolak, 2011), content which might subsequently be misused and shared with others; 2. the practice of creating self-images ("selfies") which are intended to be shared with a limited audience via social media platforms such as Facebook, which are subsequently co-opted, without permission, and repurposed for sexual gratification or voyeuristic enjoyment; 3. the use of cloud storage to host personal media content, including intimate images, which are subsequently accessed by others through hacks or data breaches, and shared online (as notably happened in 2014 when private and nude pictures of (predominantly female) celebrities were hacked from Apple's iCloud storage platform and shared on social networks such as Imgur and Reddit (McCormick, 2014); 4. the growing trend of using camera phones to covertly photograph individuals in public and/or private settings, then sharing these images online via sites dedicated to so-

called "creepshots", "upskirting" and "downblousing" (Powell, 2010); and 5. the ways that the internet affords users and abusers the ability to maintain their own anonymity (Stroud, 2014), while simultaneously identifying victims (including the practice of "doxing", "the intentional public release onto the Internet of personal information about an individual by a third party, often with the intent to humiliate, threaten, intimidate, or punish the identified individual" (Douglas, 2016, p.199)).

Beyond these media-specific factors, we must recognize (as alluded to in our introductory remarks) the broader socio-cultural context which has recently seen the articulation of a reactionary (white) masculinity that licenses and valorizes the denigration of women, alongside people of color, and sexual, ethnic and religious minorities (Nagle 2017; Salter & Blodgett, 2016). The pervasive air of intimidation, sexism, harassment and marginalization experienced by women has of late been highlighted by the #MeToo movement, in which victims of such conduct break their silence and share publicly the nature and extent of the abuse suffered (Frye, 2018). In its specific online manifestation, this "toxic masculinity" has been apparent on social networks and content-sharing platforms such as Reddit, 4Chan and 8Chan (Massanari, 2017), which have become repositories for gender-based abuse, including the circulation of "revenge porn" and other kinds of image-based offences (Marganski, 2018). Of those lodging complaints of IBA with the police in England in 2015, female victims outnumbered males by a factor of eight (Davies, 2015). The misogynistic character of these activities is further demonstrated by the vitriolic, sexually crude and demeaning viewer comments that typically accompany the posted images (Martinez, 2014). Thus, IBA has emerged and thrived by drawing support from an ideology that legitimizes gender-based and other forms of denigration as a form of masculine self-assertion or empowerment.

The precise extent of online IBA is difficult to gauge, for a number of reasons. Firstly, is the limited amount of systematic data collection through victimization studies. Further, IBA is often under-reported by victims (some of whom may be unaware that their pictures and details have been shared without permission) and due to the varying definitions and delimitations of the problem according to different actors and authorities (for example, whether the images concerned need to be sexually explicit, or the sharing of images needs to be motivated by an intent to annoy or harass the victim, in order to count as IBA). We can, however, garner some indicative sense of the extent of the problem. One of the first and most prominent "revenge porn" sites, IsAnyoneUp, launched in 2010 and remained live and active for 16 months. Its founder subsequently reported that he was receiving some 35,000 submissions every week, with an even split between images that had been "self-submitted…from those seeking quick Internet fame" and genuine instances of unauthorized and unwelcome sharing of images (Stroud 2014: 170). While such sites come and go, including the likes of Pinkmeth, Texxxan, Anon-IB, and IsAnybodyDown (Ibid.: 170-171; Calvert, 2013: 671; Gault & Cox, 2018). Interestingly, after being shut down, sites such as Pinkmeth subsequently resurfaced on the Dark Web (Cox, 2015).

When laws criminalizing IBA came into force in England & Wales in April 2015 (discussed further in the next section), the following 6 months saw 1,160 incidents reported across 31 police forces; while the average age of victims was 25, a significant minority were under the age of consent, with some younger than 11 years old; 68% of offences were committed using Facebook, and other popular social media platforms such

as Instagram and Snapchat also figured (Spratt 2016). The only UK-based victimization survey to date has involved a small sample of 64 (predominantly female) respondents, all of whom had self-reported suffering IBA (Short, Brown, Pitchford & Barnes, 2017). Consequently, while providing useful data about the dynamics of the offence and its impacts and consequences, the study cannot provide any indication of the proportion of internet users who experience such victimization i.e. its prevalence.

In Australia, by contrast, a 2017 nationwide survey of 4,200 respondents found that 20% had experienced IBA; a previous 2014 survey by the same researchers placed this figure at 10.7%, clearly indicating a rapid increase in victimization rates (Henry, Powell & Flynn, 2017). The survey also found that perpetrators are, in more than 90% of incidents, either partners, ex-intimates or "otherwise known" to the victim (Ibid.: 6). A 2016 survey of 3,000 Americans found a somewhat lower victimization rate, with 4% of respondents having be subjected to the threat and/or actuality of non-consensual sharing of intimate images (Lenhart, Ybarra & Price-Feeney, 2016). This discrepancy in comparison with the figures from Australia may be an artefact of the kinds of images that were deemed to constitute "revenge porn" in the US study, namely "nude or nearly nude photos or videos" (ibid.). The Australian study also appears to have included within its definition of the problem "upskirting" and "downblousing" images that, while invasive and sexualized, may not include nudity (e.g. of the breasts or genitals). These differences notwithstanding, we can discern that IBA of this kind is a significant and seemingly growing problem, one that causes significant psychological, emotional and social harm to victims (Franklin, 2014; Scheller, 2015; Henry et al., 2017).

## *2. THE CRIMINALIZATION OF IMAGE-BASED ABUSE*

Despite recorded incidents dating back at least as far 2000 (Linkous, 2014), targeted criminal law measures specifically addressing IBA or non-consensual pornography did not start to appear on a widespread scale until some years later. The earliest such statute was introduced in the state of New Jersey in 2004 (New Jersey Code 2C: 14-9), which made it "a felony to disclose a person's nude or partial nude image without that person's consent" (Martinez 2014, p.239). A similar measure was introduced in Alaska in 2005, but almost a decade was to pass before another state, California, was to pass a similar law (Penal Code § 647(j)(4)). Other states rapidly followed in the ensuing years, and as of 2017 a total of 38 states, as well as the District of Columbia (DC) had enacted legislation (FindLaw, 2019).

It is important to note the significant variation in such provisions across a number of dimensions. For example, the California statute's definition of an offence requires not only the act of distributing the image without consent, but that it be done "with the intention to cause serious emotional distress", and that such distress be demonstrably suffered (Martinez, 2014, p. 241-3). Additionally, while some states made non-consensual pornography a felony punishable by up to 6 years in prison, others treat it as a far less serious misdemeanor offence punishable either by much shorter custodial sentences or a fine (FindLaw, 2019). In addition to these specifically-focused laws, IBA has also been prosecuted under laws related to harassment and stalking, as well as the use of civil remedies such as the assertion of copyright by the victims to force removal of content (Levendowski, 2013). Outside the US, the Philippines was the first country to take action

when it passed the Anti-Photo and Video Voyeurism Act which included provisions for custodial sentences of up to 7 years (Franks, 2016). Subsequently, similar criminal laws have been introduced in Israel, Canada and Japan (2014), and New Zealand (2015).

In Australia, state and federal legislation has been introduced to address IBA. At a state level, Queensland, New South Wales, Victoria, South Australia, Australian Capital Territory and Northern Territory have passed amendments to their respective criminal codes to specifically criminalize offences related to distributing and threatening distribution of intimate images without consent. New South Wales was the first Australian jurisdiction to explicitly include 'altered images' within its criminal definitions related to IBA. Altered images can include such manipulation of images including body alterations or face swapping (Crimes Amendment (Intimate Images) Amendment Act 2017 (NSW)). Western Australia has provisions within their Restraining Orders Act 1997 (WA). Tasmania remains the only Australian state or territory with no specific IBA laws.

In 2018 the Australian Government moved to amend federal legislation. The Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018 (henceforth EOSA) amends the Enhancing Online Safety Act 2015 (Cth) and the Criminal Code Act 1995 (Cth), making it an offence to non-consensually share "intimate images". As will be discussed in more detail later, the Act incorporates provisions for punitive actions, both criminal and civil. The Act allows for custodial sentences of up to 7 years and establishes a civil penalties regime allowing penalties against internet and social media companies who fail to comply with orders to remove offending content. These are innovations yet to be seen in any other legislation around image-based abuse (EOSA, 2018b). Taken together, the provisions of the Act constitute the most far-reaching attempts to use criminal law to tackle non-consensual image sharing.

Particularly noteworthy is the fact that the Act does not confine the definition of "intimate images" to only those explicitly containing nudity (of the genitals, breasts, etc.). Rather, it also encompasses material depicting "the person's genital area or anal area (whether bare or ***covered by underwear*** – emphasis added)" – thereby encompassing within its scope the kinds of images commonly associated with "upskirting" photos. Moreover, it also counts instances in which "because of the person's religious or cultural background, the person consistently wears particular attire of religious or cultural significance whenever the person is in public…the material depicts, or appears to depict, the person without that attire" – a definition that would, for example, cover the non-consensual sharing of images of a Muslim woman without the niqab she would normally wear in public, or the depiction of a Sikh man without his turban (EOSA, 2018b: 24).

Turning to England & Wales, the 2015 Criminal Justice and Courts Act[4] (henceforth CJCA) introduced specific provisions (S.33-35) to criminalize the distribution of "private sexual materials" (prior to this Act, IBA cases had been prosecuted under other statutes such as the Malicious Communications Act (1988) and the Protection from Harassment Act (1997)). Again, it is noteworthy that the Act takes a potentially broader interpretation

[4] The separate jurisdictions of Scotland and Northern Ireland introduced their own subsequent provisions in 2016, which differ in some aspects from that enacted in England & Wales e.g. in terms of defining the kinds of material covered and the duration of custodial sentences that may be handed down.

of material to which its provisions are applicable, by not simply tying the notion of "sexual material" to nudity alone. Instead, it additionally allows for a potentially more capacious definition – material that "shows something that a reasonable person would consider to be sexual because of its nature, or […] its content, taken as a whole, is such that a reasonable person would consider it to be sexual" (Criminal Justice and Courts Act 2015, S.35). This would appear to allow, in principle, the inclusions of sexually provocative but non-nude images. However, unlike the Australian EOSA, it does not go so far as to cover being pictured without "attire of religious or cultural significance" that a victim would normally wear in public. Likewise, no liability or penalties are imposed upon internet companies and social media providers, although consultations are currently under way about proposals for introducing a system of fines for companies that fail to act effectively to remove prohibited content (Yar, 2018; we return to this issue later in our discussion). Additionally, like the California statute, the Act might be criticized for requiring that the image disclosure be done "with the intention of causing that person distress" (Criminal Justice and Courts Act 2015 Explanatory Notes). In terms of penalties, the Act allows for custodial sentences of up to 2 years and/or an unspecified fine. And finally, the Act has been criticized by campaigners and victims' advocates because its provisions only apply in instances where the images/recordings in question have actually been distributed. They point out that the threat of such disclosure in and of itself causes very significant distress and harms to those targeted, irrespective of whether the offenders does, in the final instance, deliver on that threat (Robinson & Dowling, 2019).

## *3. PROSECUTIONS OF IMAGE BASED ABUSE*

We now turn to consider the exercise of the above Acts in terms of prosecutions brought since their introduction. Given the very recent enactment of Australia's EOSA (1 September 2018) there are as yet no figures available. However, there are corresponding figures available in relation to the State laws in Victoria, South Australia, and New South Wales. In England & Wales, the Crown Prosecution Service's annual Violence against Women and Girls (VAWG) report includes data on the number of offences prosecuted under the CJCA since 2015. In 2015-16, there were 206 such prosecutions (although this figure is for part year, as the provisions came into force in April of 2015), and the range of sanctions were applied upon conviction including (suspended) custodial sentences, fines, restraining orders, tagged curfews, and payment of compensation (CPS, 2016: 11, 90-91). The corresponding figures for the two subsequent 12-month periods were 460 and 464 (CPS, 2017: 17, A43; CPS 2018: 190). New sentencing guidelines came into force from October 2018, recommending harsher sentences for those who repeatedly re-post offending content after it has already been taken down (BBC News, 2018a). Thus, in cases combining "higher culpability" ("intended to maximize distress", "images circulated widely", "significant planning", "repeated efforts to keep images available for viewing") and high harm ("very serious distress caused", "significant psychological harm", "considerable practical impact") the recommended starting point is a 12-month custodial sentence (Sentencing Council, 2018: 22). However, these efforts notwithstanding, one third of complaints made since 2015 (2,813 out of 7,806) were dropped. According to Julia Mulligan, Police and Crime Commissioner for North Yorkshire, this may be driven by the fact that, being classed as a "communicative offence" rather than a "sexual

offence", IBA cases do not allow victims to remain anonymous and the prospect of being publicly named serves to deter victims (BBC News, 2018b). Despite public calls for a change to the law in order to grant victims anonymity, no change appears to be planned at present.

## *4. MECHANISMS FOR REPORTING OF IMAGE-BASED ABUSE*

In this section we turn to consider the mechanisms and systems for reporting incidents of IBA that have been established in parallel with the legislative changes outlined in the preceding discussion.

### *4.1. Australia: Office of eSafety – Online Portal for reporting and available statistics*

In late 2017 the Australian Government-funded Office of eSafety, launched an initiative to assist victims of IBA. The image-based abuse portal, believed to be a world-first, provides victims with reporting options, support and resources for those who have experienced IBA. The portal provides victims, as well as family, friends and bystanders, a central location where IBA can be reported. The portal assists victims to report IBA to seek its removal, it also provides advice and resources focused on managing the impact of IBA.

Reports submitted to the online portal are assessed as either a complaint or an objection notice (Office of eSafety, 2019a). A complaint can be made by a victim, or on behalf of a victim, when the image has been posted or threatened to be posted without consent; the post or threatened post is to a social media service, website or other electronic means; there is an Australian connection (victim lives in Australia; the person who posted or threatened to post the image lives in Australia; the image is hosted in Australia). An objection notice is determined when simply an intimate image has been posted and can still be lodged if initially the person had consented to the posting but now wants it removed.

The Office of eSafety can take removal action in either case, but only take action against the person who posted or threatened to post when the report meets the criteria of a complaint (Office of eSafety, 2019a). The Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018 provides the Commissioner of eSafety a number of options in responding to IBA. Actions include formal warnings, infringement notices and seeking injunctions, or enforcing an undertaking or civil penalty order from a court. In the 2018-19 federal budget, the Australian Government committed $4 million over four years to support the eSafety Office to implement a civil penalty regime. Individuals may be subject to civil penalties of up to $105,000 and corporations up to $525,000 for failure to comply with a request from the eSafety Commissioner to remove intimate images (Reichert, 2018).

The eSafety Commissioner Annual Report (2017-2018) indicates that between October and June 2018, 259 reports of image-based abuse were received by eSafety. Victim reports were predominately from female victims (78.5%). Most reports related to anonymous posting of images (40%), consensually taken images that were then on-shared (24%) and sextortion (22%). The 259 reports related to 401 individual URL's and/or locations of IBA and images appeared across 130 different platforms. Reports of IBA were most likely to relate to images posted on pornography sites (44%), followed by social

media (25%) and held by a third party (17%). One of the major challenges for victims who seek to have images removed, relates to images being hosted on platforms operating outside of the country in which the victim resides. The online portal and advocacy of the Office of eSafety on behalf of victims constitutes a promising approach to overcoming such difficulties. It was reported that despite most material being hosted in overseas locations in approximately 80 per cent of reported cases eSafety was successful in having the material removed (eSafety Commissioner Annual Report, 2017-2018).

### *4.2. UK: Reporting Dynamics and Regulatory Absences*

In sharp contrast to the recently-established Australian reporting system for IBA, the UK has yet to see the establishment of a centralized mechanism with responsibility for receiving and acting upon such abuse. This lacuna is part of a wider problem (currently the subject of intense debate and significant policy discussion) about the absence of a statutory regulator with the power to monitor and act as necessary to compel social media platforms to remove offending content, and/or to sanction them for a failure to do so. The recently published government White Paper on tackling online harms includes a consultation on establishing a system of statutory regulation. It proposes the creation of an "independent regulator" (or the extension of statutory responsibilities held by an existing regulatory body) which would oversee a legally-enshrined "duty of care" on the part of online platforms towards their users; oversee the implementation of "redress mechanisms" available for users; and take "prompt and effective enforcement action in the event of non-compliance" (Online Harms White Paper, 2019, p.54). Quite what form enforcement action might take is not specified in the proposals, but one idea that has been proposed by government Ministers and others is to include a regime of administrative fines along the lines of those seen not just in Australia but also in Germany (Achten, 2018). However, internet industry bodies (such as the Internet Association) have expressed staunch resistance to any extension of legal liability for offending content so as to include the platforms or services through which that content is shared (so-called third-party liability) (Rajan, 2019). The situation regarding digital service providers' legal responsibilities regarding online content is further complicated by the UK's departure from the European Union (so-called Brexit), as EU regulations and directives exercise significant control in this area (for example through its Electronic Commerce Directive (2000) and General Data Protection Regulation (2018) – Baistrocchi 2003, Tankard 2016). Given this context, it remains profoundly uncertain just what kind of regulatory architecture might emerge, and when it might eventually take effect.

In the absence of any statutory provision or state-sanctioned mechanisms for reporting and responding to IBA, the response has thus far been left to 'third sector' and voluntary actors. There are presently two online platforms that enable victims of IBA to report their experiences, both established in 2015 coterminous with the introduction of the aforementioned legal provisions in the CJCA. The first of these is Victims of Internet Crime: Speak Out (voic.org.uk). Established by a survivor of IBA, the forum creates a space for victims to bear witness to and speak out about their abuse experiences, as well as offering general advice about how to report victimization and seek redress from social media services through content removal. It also signposts visitors to psychological support services and relevant news via its Twitter feed, Facebook page, Pinterest, and Instagram.

However, there is no indication in the site's communications that reports of IBA are forwarded to law enforcement. Moreover, judging by its social media following (in the low hundreds) its reach amongst users (while not negligible) is clearly, thus far, limited.

The second avenue available for victims of IBA is provided by the Revenge Porn Helpline (https://revengepornhelpline.org.uk/). The site, as its name indicates, offers a helpline for victims (available by phone and email) that can provide advice, assistance with reporting abusive images to social media services, and legal advice including guidance on the evidence a victim will need in order to report an offence to the police. However, the helpline does not directly report incidents to the police on victims' behalf, nor does it assist victims from outside the UK or those who are under 18 years of age (the latter being directed to the Internet Watch Foundation (IWF) which deals with child sex abuse imagery). The hotline reports that, in the 3 years following its establishment (2015-2018), it was contacted by 4,078 individuals seeking advice in cases of abuse, and in over 80% of cases the offending content they reported on behalf of victims was successfully removed. Of the victims contacting the hotline, 67% are female and 33% male. Of cases 13.3% involve 'sextortion' (using the threat of disclosing intimate images to extort sexual favors from victims). Some 16-17% of the incidents entail the sharing of images via social media platforms, and in about 25% of cases there is a threat to disclose images but that threat is not followed-through[5]. In addition to receiving these reports from victims, it also provides users with direction to counselling and support services, to free legal advice provided by a university partner, and hosts various informational resources. While in no sense an official agency of the state (it is operated by a not-for-profit charitable trust), the helpline is nevertheless funded by the UK Government's Equalities Office.

The non-statutory nature of the present provision for reporting IBA in the UK is clearly subject to limitations. Firstly, there are a number of different actors to whom victims and other concerned parties might report an offence (in addition to the IBA-specific channels discussed above, individuals may also approach voluntary organizations supporting victims of sexual abuse or more-broadly targeted services such as the national charity Victim Support). This variety of avenues may well result in (a) uncertainty on the part of victims as to whom to best contact; and (b) uneven and irregular kinds of advice and assistance being offered e.g. some actors will have better and more strongly-rooted relationships with social media platforms, enabling them to more easily and effectively facilitate content removal. As already noted, since there is no mandatory mechanism for responding to user complaints, content removal or remedial actions are very much up to the responsiveness of social media platforms themselves. Further, for those wishing to see action taken against offenders by the criminal justice system, it is left to the victims to contact the police and report the offence, by telephone or in-person at a police station. Given the sensitive and distressing nature of IBA, this requirement for direct disclosure (including potentially sharing details about the nature and content of intimate images and recordings), may serve to deter victims (as has been shown to be the case with other kinds of sexual offences – Taylor & Gassner, 2010). For all these reasons, there is a potentially strong argument for the UK adopting or adapting the Australian approach to tackling IBA

[5] This data was provided by the Revenge Porn Helpline in response to an email inquiry from one of the authors.

as it considers how it will implement the recently-announced regulatory proposals in the Online Harms White Paper. In the next section, we assess the Australian approach, highlighting its advantages and possible drawbacks, as a viable template for best-practice in the UK and elsewhere.

## *5. MOVING FORWARD: DOES AUSTRALIA PROVIDE A VIABLE MODEL FOR TACKLING IBA?*

The Australian model provides an opportunity to explore the benefits and possible pitfalls of a proactive and concerted effort to tackle the challenges of reporting, reacting to, and preventing IBA. The current approach in Australia tackles IBA through a continuum of direct criminal and regulatory sanctions through to self-regulation. It is perhaps useful to examine the new approach adopted in Australia in light of the challenges that have continued to plague online crime more generally.

Consciousness-raising and education relating to cybercrime has proliferated in recent times, with numerous and varied government and non-government entities seeking to provide resources and support to potential and existing victims. Though well-intentioned, the maze and diversity of resources, spread across websites and educational programs, potentially results in a confusing mix of multi-faceted and non-focused responses that are in fact overwhelming. The Office of eSafety has seemingly provided a comprehensive and focused web resource that provides both education and support resources for victims, potential victims, families and bystanders of IBA. The proactive and early identification of the emergence and growth of IBA by the Australian Government through the Office of eSafety has resulted in a more coherent and centralized point for victims and related parties.

Reporting continues to be a significant issue, first in terms of impact that the lack of reporting has on understanding the prevalence and characteristics (victims, offenders, offenders' methods) of cybercrime. This results in a lack of data about the true prevalence of crimes. Without accurate prevalence data we are unable to determine trajectory and growth of crime and we are unable to lobby for resources in proportionate response to the problem. Further, without data we lack knowledge about perpetrators and the modus operandi of IBA. In turn, we are unable to accurately determine the impact of interventions designed to prevent and reduce this crime. Second, police and other responsible regulatory agencies are unable to police, prevent and react to cybercrime without victim reports. One of the greatest challenges is to encourage and assist victims to report (van de Weijer, Leukfeldt & Bernasco, 2018). Even when victims overcome their concerns and fears about reporting, they are then often confused about how to report their victimization (Button, Lewis & Tapley, 2014). As such, victims continue to be victimized and offenders continue to perpetrate their crimes without constraint.

The approach taken by the Office of eSafety overcomes a number of the issues that have been identified regarding reporting. It is proposed that the development and facilitation of a centralized reporting portal provided on the Office of eSaftey website is a crucial pillar in successfully addressing IBA. It provides a central reporting facility that is simple and accessible to victims of IBA. This seems to go some way in addressing the barrier often faced by victims who seek to report but are confused about where and how to report. This central reporting portal also maximizes the likelihood that a more

comprehensive dataset on IBA can be collected. It must be noted, however, that in order to take wholistic action on IBA this data must be shared by the Office of eSafety and included in official crime statistics datasets. Often with crime we look exclusively to police agencies and court records, the Office of eSafety as a regulatory agency must ensure that their data is used to work closely with other stakeholders such as police to promote prevention and disruption of IBA.

As indicated earlier, the Office of eSafety website provides victims with assistance in the removal of IBA images and/or videos. It has been noted, however, that a frustration for victims of cybercrime more broadly is the lack of perceived action that is taken when victims do report. For most cybercrimes, police are simply unable to investigate many of the offences that are reported due to jurisdictional and geographic boundaries, with offenders located off-shore. The approach taken in Australia to IBA, whilst still potentially suffering the same frustrations as other kinds of cybercrime regarding perpetrators, has focused on the actions that are within an achievable remit of preventing further IBA and disrupting the crime. Legislative changes to the Enhancing Online Safety Act 2015 were made in order for victims to be assisted by the Office of eSaftey to remove intimate images or videos. The changes to legislation provide a support mechanism for victims to assist them having images and videos removed which in the first instance is likely to be the most important outcome for victims. The approach taken in Australia has embraced the concept that responses to reducing crimes such as IBA must look to the entities that facilitate interaction between potential victims and perpetrators. In cyberspace, crime occurs within legitimate platforms such as social media. It is proposed that providing legislative support for the capacity and reach of the Office of eSafety will likely multiply its impact and success. It centers regulatory coercion and power within the mandate of the Office of eSaftey that is able to be used as levers within the space that IBA is typically occurring, specifically legitimate social media platforms. Other countries who are considering adopting the Australian approach need to evaluate the need for legislative changes to support the initiative. A reliance on voluntary compliance by social media platforms may prove much more challenging.

A strength of the resources provided by the Office of eSafety website, particularly in respect to reporting, it that it goes beyond its own scope and purview of control in the IBA space and provides information to victims about other reporting mechanisms, such as reporting to police. This approach gives power to victims to meet their intended goals. Whilst the Office of eSafety is able to assist in achieving the removal of IBA images and/or videos and coercing social media platforms and others to comply with removal, victims may also seek to pursue criminal outcomes against the perpetrators. It is crucial that information is provided to victims informing them of all their options. Victims need to be clearly informed about their options and rights not only to stop the abuse but also, seek retribution through criminal sanctions.

Looking to the regulation of social media and the responses to IBA in the UK, the lessons learned thus far from developments in Australia ought to be considered carefully by the government as it consults on formulating a statutory online harms regulator. Firstly, it is important that the regulatory body that is ultimately created or empowered provides a clearly visible, accessible and effective mechanism through which victims and others may report incidents of IBA. This will, as noted above, help to ensure that (a) as many

incidents as possible are reported and drawn to the attention social media platforms, so as to facilitate speedy removal of offending content; (b) that incidents in breach of criminal law provisions of the 2015 Act are drawn to the attention of the police for investigation and potential prosecution, and (c) robust and reliable data about levels and trends in IBA, and about victims, offenders, and the sites/channels/platforms where incidents occur, are recorded and made available for criminal justice actors, policy makers and researchers.

Secondly, that the powers of the regulator to compel compliance from social media platforms, and any corresponding regime of penalties for non-compliance, be sufficiently stringent to incentivize large and powerful media corporations to prioritize their duty of care toward users. Pressure to invest the appropriate levels of care and resources to preventing and tackling IBA is needed.

Thirdly, that the regulator plays a pivotal role in informing and educating users about the harms of IBA and the kinds of activities that fall under the banner of such abuse, and in directing victims to appropriate resources and forms of support. Ultimately, however, any such regulatory regime needs the underpinning support from legislation that provides protection to victims by prohibiting IBA. In this regard, as has been noted earlier, the law in England & Wales may be deficient in two main respects. Firstly, by classifying IBA as a 'communication offence' rather than a sexual offence, victims are denied the anonymity that applies in instances of other kinds of sexual abuse. This lack of anonymity has been identified a key impediment to victims reporting incidents and pursuing resolution through the criminal justice system. Secondly, and perhaps even more significant, the law around IBA at present does not criminalize threatening to distribute private sexual materials, but rather only those incidents in which the offender follows-through on such threats. Given that threatening short of actual disclosure is experienced by a significant proportion of victims, and in and of itself is the source of considerable harm and distress, the extension of the definition of IBA is needed to more fully address the problem in its various manifestations (as is the case in Australian law). It is only through a coherent and thorough articulation of law and regulatory action that the UK can make effective inroads when it comes to tackling IBA.

## *Conclusion*

This paper provided an analysis of the rise in IBA as a modern-day issue that continues to increase and impact on individuals across the world. Our analysis, in light of the broader context of online misogyny, gender-based victimization, "toxic masculinity" and patriarchal control, calls for a wide-encompassing debate in light of existing socio-cultural sexism and discrimination. Importantly, this paper reviewed moves in England & Wales and Australia, and formative developments in countries such as the United States, to criminalize IBA and the associated challenges of crime control initiatives in effectively responding to the problem. Based on this analysis, the authors were able to map the types of user-oriented crime prevention initiatives that are being developed in Australia and England & Wales. It is concluded that, despite the potential pitfalls that can be identified in the journey towards more robust criminalization of IBA, important and positive steps are being taken and achieved. Further, particularly in Australia, significant consideration is being given to both prevention and responding to IBA. Australia has developed a model that clearly acknowledges the need for criminal recourse and sanctions, has identified and

developed resources to assist victims navigate the complexity and confusion often associated with removal of images and videos and has responded to the need for better crime prevention education.

As demonstrated throughout this paper, we need to be cognizant of the actions and progress being made in relation to IBA response and prevention across the world. There is potentially much to be learnt from those who have been early responders to IBA. As countries successively tackle IBA through their own criminal justice systems and stakeholder engagement, they would be wise to reflect on instances of best practice already established elsewhere. IBA is not a geographically bound issue, it goes beyond borders and occurs in uncharted cyberspace, it is likely that the most effective efforts in responding to IBA, just as we have seen in other emerging cybercrimes, will involve a simultaneous approach at both a domestic and global level.

### *References*

Achten, N. (2018). Social Media Content Moderation: The German Regulation Debate. *Lawfare*, 27 December. Retrieved from https://www.lawfareblog.com/social-media-content-moderation-german-regulation-debate.

Baistrocchi, P. A. (2002). Liability of intermediary service providers in the EU Directive on Electronic Commerce. *Santa Clara Computer & High Technology Law Journal*, *19*, 111-130.

BBC News (2015). 'Revenge porn' site owner convicted of extortion. *BBC News*, 3 February. Retrieved from https://www.bbc.co.uk/news/technology-31112599.

BBC News (2018a). New guidelines for 'revenge porn' crimes. *BBC News*, 5 July. Retrieved from https://www.bbc.co.uk/news/uk-44713953.

BBC News (2018b). Revenge porn: One in three allegations dropped. *BBC News*, 14 June. Retrieved from https://www.bbc.co.uk/news/uk-england-44411754.

Bennett, R. R. (2004). Comparative criminology and criminal justice research: The state of our knowledge. *Justice Quarterly*, *21*(1), 1-21.

Button M, Lewis C, Tapley J (2014) Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal, 27(1),* 36–54.

Calvert, C. (2013). Revenge porn and freedom of expression: Legislative pushback to an online weapon of emotional and reputational destruction. *Fordham Intellectual Property, Media & Entertainment Law Journal*, *24*, 673-702.

Cox, J. (2015) Revenge Porn Returns to the Dark Web. *Motherboard*, June 29. Retrieved from https://motherboard.vice.com/en_us/article/53988z/revenge-porn-returns-to-the-dark-web.

Criminal Justice and Courts Act 2015 (2015). Retrieved from http://www.legislation.gov.uk/ukpga/2015/2/contents/enacted.

Criminal Justice and Courts Act 2015 Explanatory Notes (2015). Retrieved from https://www.legislation.gov.uk/ukpga/2015/2/notes/data.xht?view=snippet&wrap=true.

Crimes Amendment (Intimate Images) Amendment Act 2017 (NSW). Retrieved from https://legislation.nsw.gov.au/#/view/act/2017/29/full.

Crofts, T., Lee, M., McGovern, A., & Milivojevic, S. (2016). *Sexting and Young People*. Houndsmills, Basingstoke: Springer.

CPS (Crown Prosecution Service). (2016). *Violence against Women and Girls Crime Report 2015-16.* London: CPS.

CPS (Crown Prosecution Service). (2017). *Violence against Women and Girls Crime Report 2016-17.* London: CPS.

CPS (Crown Prosecution Service). (2018). *Violence against Women and Girls Crime Report 2017-18.* London: CPS.

Davies, C. (2015). Revenge porn cases increase considerably, police figures reveal. *The Guardian*, July 15. Retrieved from https://www.theguardian.com/technology/2015/jul/15/revenge-porn-cases-increase-police-figures-reveal.

Douglas, D. M. (2016). Doxing: a conceptual analysis. *Ethics and Information Technology*, *18(3),* 199-210.

Enhancing Online Safety Act 2015 (Cth). Retrieved from https://www.legislation.gov.au/Details/C2017C00187.

EOSA (2018) Enhancing Online Safety (Non-Consensual Sharing of Intimate Images Bill) 2018. Canberra: Parliament of Australia.

EOSA (2018b) Enhancing Online Safety (Non-Consensual Sharing of Intimate Images Bill) 2018: Revised Explanatory Memorandum. Canberra: Parliament of Australia.

FindLaw (2019) Revenge Porn Laws by State. Retrieved from https://criminal.findlaw.com/criminal-charges/revenge-porn-laws-by-state.html.

Fletcher, G. (2014) Revenge porn has become too profitable to go away. *The Conversation*, April 24. Retrieved from http://theconversation.com/revenge-porn-has-become-too-profitable-to-go-away-25837.

Franklin, Z. (2014). Justice for revenge porn victims: Legal theories to overcome claims of civil immunity by operators of revenge porn websites. *California Law Review*, *102(5),* 1303-1335.

Franks, M.A. (2016). *Drafting An Effective "Revenge Porn" Law: A Guide for Legislators.* Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2468823.

Frye, J. (2018). From Politics to Policy: Turning the Corner on Sexual Harassment. *Center for American Progress*, January 31. Retrieved from https://www.americanprogress.org/issues/women/news/2018/01/31/445669/politics-policy-turning-corner-sexual-harassment.

Gault, M. & Cox, J. (2018). Police Have Seized Revenge Porn Site Anon-IB. *Motherboard*, April 25. Retrieved from https://motherboard.vice.com/en_us/article/mbxdwv/anon-ib-revenge-porn-site-seized-by-politie.

Henry, N., Powell, A. & Flynn, A. (2017). *Not Just 'Revenge Pornography': Australians' Experiences of Image-Based Abuse. A Summary Report.* Melbourne: RMIT University.

Hill, K. (2011). Revenge Porn with a Facebook Twist. Retrieved from https://www.forbes.com/sites/kashmirhill/2011/07/06/revenge-porn-with-a-facebook-twist/#53a01d1d2e6a.

Hunt, E. (2016) Victoria leads way in piecemeal approach to outlawing revenge porn. *The Guardian*, 5 September. Retrieved from https://www.theguardian.com/australia-

news/2016/sep/05/victoria-leads-way-in-piecemeal-approach-to-outlawing-revenge-porn

Lenhart, A. (2009). Teens and sexting. *Pew Internet & American Life Project, 1,* 1-26.

Lenhart, A., Ybarra, M. & Price-Feeney, M. (2016). *Nonconsensual image sharing: One in 25 Americans has been a victim of "revenge porn".* Center for Innovative Public Health Research. Retrieved from https://datasociety.net/pubs/oh/Nonconsensual_Image_Sharing_2016.pdf.

Levendowski, A. (2013). Using copyright to combat revenge porn. *NYU Journal of Intellectual Property & Entertainment Law, 3,* 422-446

Linkous, T. (2013). It's Time for Revenge Porn to Get a Taste of Its Own Medicine: An Argument for the Federal Criminalization of Revenge Porn. *Richmond Journal of Law & Technology, 20(4),* 1-39

Marganski, A. J. (2018) Feminist Theory and Technocrime: Examining Gender Violence in Contemporary Society. In K. F. Steinmetz & M. R. Nobles (eds.) *Technocrime and Criminological Theory.* New York & Abingdon: Routledge. 11-34

Martinez, C. (2014). An Argument for States to Outlaw 'Revenge Porn' and for Congress to Amend 47 USC § 230: How Our Current Laws Do Little to Protect Victims. *Pittsburgh Journal of Technology Law and Policy, 14(2),* 236-252.

Massanari, A. (2017). # Gamergate and The Fappening: How Reddit's algorithm, governance, and culture support toxic technocultures. *New Media & Society, 19(3),* 329-346.

McCormick, R. (2014). Hack leaks hundreds of nude celebrity photos. *The Verge*, September 1. Retrieved from https://www.theverge.com/2014/9/1/6092089/nude-celebrity-hack.

McGlynn, C., Rackley, E., & Houghton, R. (2017). 'Beyond 'Revenge Porn': the continuum of image-based sexual abuse. *Feminist Legal Studies, 25(1),* 25-46.

Mitchell, K. J., Finkelhor, D., Jones, L. M., & Wolak, J. (2012). Prevalence and Characteristics of Youth Sexting: A National Study. *Pediatrics*, *129(1),* 13-20.

Nagle, A. (2017). *Kill All Normies: Online Culture Wars from 4chan and Tumblr to Trump and the alt-right.* Alresford: John Hunt Publishing.

NSW Government (2017). *Revenge porn is a crime.* 25 August. Retrieved from https://www.nsw.gov.au/news-and-events/news/revenge-porn-is-a-crime.

Office of eSafety (2019a). *How to report image-based abuse to the eSafety Commissioner.* Retrieved from https://www.esafety.gov.au/image-based-abuse/action/remove-images-video/report-to-us.

Office of eSafety. (2018). *eSafety Commissioner Annual Report (2017-2018).* Retrieved from https://www.esafety.gov.au/about-the-office/corporate-reporting.

Online Harms White Paper (2019). Retrieved from https://www.gov.uk/government/consultations/online-harms-white-paper.

Powell, A. (2010). Configuring consent: Emerging technologies, unauthorized sexual images and sexual assault. *Australian & New Zealand Journal of Criminology, 43(1),* 76-90.

Rajan, A. (2019). Tech giants write to ministers to spell out views on internet regulation. *BBC News*, 28 February. Retrieved from https://www.bbc.co.uk/news/entertainment-arts-47400140.

Rau, J. (2016). *Revenge Porn – it's Not Okay. Government of South Australia Attorney General's Department, October 27.* Retrieved from https://www.agd.sa.gov.au/sites/default/files/revenge_porn_-_its_not_ok.pdf?v=1496713253.

Reichert, C. (2018). Australia passes 'revenge porn' legislation. *ZDNet*, August 16. Retrieved from https://www.zdnet.com/article/australia-passes-revenge-porn-legislation.

Restraining Orders Act 1997 (WA). Retrieved from https://www.legislation.wa.gov.au/legislation/statutes.nsf/main_mrtitle_822_homepage.html.

Robinson, B. and Dowling, N. (2019). Revenge porn laws 'not working', says victims group. *BBC News*, 19 May. Retrieved from https://www.bbc.co.uk/news/uk-48309752.

Salter, A. & Blodgett, B. (2017). Introduction: Actually, It's about Toxic Geek Masculinity. In A. Salter & B. Blodgett (eds.) *Toxic Geek Masculinity in Media: Sexism, Trolling, and Identity Policing*. London: Palgrave Macmillan. 1-16.

Scheller, S. H. (2014). A picture is worth a thousand words: The legal implications of revenge porn. *North Carolina Law Review*, *93(2),* 551-595

Sentencing Council. (2018). *Intimidatory Offences Definitive Guidelines.* London: Sentencing Council.

Short, E., Brown, A., Pitchford, M., & Barnes, J. (2017). Revenge Porn: Findings from the Harassment and Revenge Porn (HARP) Survey – Preliminary Results. *Annual Review of Cyber Therapy and Telemedicine*, *15,* 161-166.

Spratt, V. (2016). Here's How Many Cases Of Revenge Porn Have Been Reported Since It Became Illegal Last Year. *Grazia*, 29 April. Retrieved from https://graziadaily.co.uk/life/real-life/heres-many-cases-revenge-porn-reported-since-became-illegal-last-year.

Stokes, J. K. (2014). The indecent Internet: Resisting unwarranted Internet exceptionalism combating revenge porn. *Berkeley Technology Law Journal, 29,* 929-952.

Stroud, S. R. (2014). The dark side of the online self: A pragmatist critique of the growing plague of revenge porn. *Journal of Mass Media Ethics*, *29(3),* 168-183.

Tankard, C. (2016). What the GDPR means for businesses. *Network Security, 2016(6),* 5-8.

Taylor, S. C., & Gassner, L. (2010). Stemming the flow: challenges for policing adult sexual assault with regard to attrition rates and under-reporting of sexual offences. *Police Practice and Research: An International Journal*, *11*(3), 240-255.

van de Weijer, S.G.A., Leukfeldt, R. & Bernasco, W. (2018). Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology, 15,* 1-23.

Yar, M. (2018). A failure to regulate? The demands and dilemmas of tackling illegal content and behaviour on social media. *International Journal of Cybersecurity Intelligence & Cybercrime*, *1(1),* 5-20.

Yar, M. & Steinmetz, K.F. (2019) *Cybercrime and Society*. 3rd edition. London & New York: Sage Publications.