Adult Cyber-harassment and Image Based Sexual Abuse.

Afroditi Pina

Unquestionably, internet usage has grown exponentially around the world over the last few years (Internet World Stats, 2019). Global statistics in July 2019 showed that over 4.5 billion people were active internet users, which indicates a growth rate of 900% between 2010 and 2016 (Internet World Stats, 2019; Statista, 2019). The Office for National Statistics (ONS) in the UK reported that almost all young adults in the UK are recent internet users (aged 16-34; ONS, 2017) and people of all ages use mobile devices in the UK; between 2005 and 2018 the proportion of adults using mobile phones saw a steady increase of 14% (98% of adults in 2018; Statista, 2019). The internet, and the devices that connect us to it, have become an integral part of most adults’ lives, upon which communication, information gathering, maintaining relationships, friendships and even livelihoods depend.

While Ofcom (2018a) reported that the majority of internet users find their online experiences positive, in the last 10 years, researchers, stakeholders and policy makers have recognised that the internet is being used for committing crime and antisocial behaviours and that internet users are at risk of different types of victimisation online (Kowalski, Giumetti, Schroeder & Lattanner, 2014; Duggan et al., 2015; Cybersmile Foundation, 2017; Davidson et al., 2019). Some groups of internet users (such as children and people over 75) present with differing but notable risks of exploitation and harm and a significant body of research has outlined and studied in depth children’s risks and ways to counteract them (for reviews please see Spielhofer, 2010; Livingstone, Davidson & Bryce, 2017; Bentley et al., 2019) as well as senior citizen risks online (Grimes, Hough, Mazur & Signorella, 2010; Home Instead, 2013; Age UK, 2019). In this chapter I will focus on adults’ experiences with particular types of antisocial and criminal behaviour online -as young adults are likely to be the most active internet users (Duggan et al., 2015; ONS, 2017)- and delineate recent research that has identified different typologies, perpetration and victimisation rates for adults.

Of particular interest to researchers and scholars has been the nature and the specific features of online technology and the internet and how that may facilitate or enable certain individuals to engage in antisocial or criminal behaviour (Davidson et al., 2019). Specifically, Brown (2017) concluded that there are four unique features in online technology that separate it from the offline world: *anonymity, invisibility, community and instantaneousness* (p. 304). As Brown elaborates, information spreads with record speeds and the rapid nature of thinking and typing often will result in people being more unfiltered and inconsiderate. Furthermore, anonymity makes users less easily identifiable and allows for the expression of aggressive or hateful thoughts, as people often presume anonymity equals unaccountability, or lack of consequences (2017). Additionally, the inherent physical distance between users and the ease of going offline creates a sense of invisibility; it is the distance and lack of cues that people normally rely on for empathy (such as facial and emotional expressions) that may facilitate online aggression (Brown, 2017). Finally, the ease with which people can select groups and forums and the algorithmic amplification with which some sites operate (Davies, 2019; Sadagopan, 2019) mean that users can engage more easily with likeminded others in distant parts of the world, have a sense of community and feel that many others agree with and legitimise their views, often leading to group polarisation and extremes.

**Conceptual challenges and outline:**

As with offline harassment (see Pina, Gannon & Saunders, 2009), a significant problem is

that a universally accepted and parsimonious legal or academic definition does not exist for online harassment. There are several behaviours and experiences that could fit the category of harassment, and some behaviours occur as a direct or indirect consequence of other similar behaviours that may or may not be criminal. However, some scholars and researchers have provided definitions and identified different online aggressive and antisocial behaviours that would fit under an umbrella term of online harassment (Blackwell, Dimond, Schoenebeck & Lampe, 2017; Pew Research Center, 2017; Davidson et al., 2019).

Terminologies are used interchangeably in research, policy documents and the media (including a variety of similar terms used to describe a category of allied behaviours/offenses) and there are frequently significant overlaps in definitions or descriptions (Universities UK, 2016). Therefore, accurate prevalence rates and recording of harm remain serious issues in this field of research. Prevalence of online harassment is hard to quantify due to the aforementioned variability in definitions, and often large representative surveys do not report on specific definitions used or materials used (Davidson et al., 2019). This conceptual and empirical overlap of the different behaviours that would fit online harassment will be discussed in the sections below. Blackwell et al.’s definition of online harassment as “a broad spectrum of abusive behaviours enabled by technology platforms and used to target a specific user or users” is adopted for this chapter (Blackwell et al., 2017, p.24; Davidson et al., 2019).

As online harassment experiences and behaviours are similar in impact but often distinct in mode and motivation, in this chapter they are also separated into two categories of non-sexual and sexual online harassment to mirror offline harassment legislation and definitions (Equality Act, 2010). As research has also identified that sexual and non-sexual behaviours often have different motivators and people who perpetrate sexual and non-sexual offending behaviours often present with different characteristics, prior experiences and risks, it is proposed that it will be useful to examine them separately (Butler & Seto 2002; Robertson & Knight, 2014).

**Online Non Sexual Harassment:**

As technology advances at rapid speeds, so do the modes and categories of criminal and antisocial activity, some of which closely mirror offline behaviours, and some present with completely new characteristics and unchartered challenges. It is important to accurately define the different types of antisocial and criminal activities that present risks online and use harmonised definitions, as much as possible, so that we can ensure that behaviours are correctly identified, quantified and managed, as well as treating distinct categories of behaviours separately in terms of risks and management (Davidson et al., 2019). As offline harassment and bullying are often used interchangeably in the literature, the same applies to cyber-harassment and cyberbullying, where also some of the behaviours described under each category could be applied to the other, therefore distinction and differentiation is not always straightforward (Davidson et al., 2019). However, as Fenton argued in the Universities UK 2016 report, online harassment is a better term to use to describe the experience/behaviours to signify the legal implications, as there exist harassment laws that criminalise some of these behaviours.

There is substantial debate in the literature as to whether online harassment is simply an extension of offline harassment sharing similar characteristics (e.g. repetition, power imbalance and intention to harm; Barkoukis et al., 2015), or whether it is a distinct and different form of harassment (e.g. Kowalski et al., 2014 argue that repetition with some of the online harassment behaviours is not necessary, and intention to cause harm is not legally necessary to prove harassment) but it is generally accepted that online harassment presents with unique characteristics whilst sharing some similarities with offline harassment (Universities UK, 2016). Some of the non-sexual behaviours included in the broad definition of online harassment have been individually defined and researched and they are presented below, however the reader will notice that there is significant overlap in concepts and terminology as well as mode and impact between each category:

*Cyber-harassment/Cyberbullying:*

These, often interchangeable, terms are used to describe aggression that is repeatedly and intentionally carried out online (and by variable means and technology) against a person who cannot easily defend themselves (Olweus, 2013; Kowalski et al., 2014). It tends to be “persistent enough to amount to a course of conduct rather than an isolated incident” and inflicts substantial emotional distress (Citron, 2014, p.3) Examples of this behaviour include flaming (online fighting with vulgar language), denigration (offensive name-calling), outing (posting personal information about individuals’ sexual preferences), trickery (convincing someone to provide personal information and then reveal to the public) online impersonation and exclusion (intentionally preventing someone from joining a group or network) (Willard, 2007; Kowalski et al., 2014).

A National Society for the Prevention of Cruelty to Children (NSPCC) survey conducted in 2016 during anti-bullying week in the UK identified that online abuse had risen by 88% in five years. Due to the broad definitions applied and the overlap between the two terms, prevalence rates are difficult to accurately establish, however studies indicate that nearly 50% of younger adults (16-34) experience some form of online harassment and 66% witness it happening to others (Pew Research Center, 2017). Men are overall more likely to be victims of online harassment of the flaming, and denigrating kind, whereas women are twice as likely to suffer from sexualised forms of online harassment compared to men (Pew Research Center, 2017). Men and women also differ in their perceptions of online harassment harm (which mirrors research on offline harassment; Rotundo, Nguyen & Sackett, 2001; Banerjee & Sharma, 2011) with women being more likely to recognise online harassment and think it is a problem than men. Women are also reported to be victims of a particular type of online harassment (cyber gender harassment) where they are exposed to misogynistic language and sexual violence threats online (see also Hate Speech), however no systematic prevalence evidence of this behaviour exists, and reports come predominantly from anecdotal or qualitative evidence from victims (Henry & Powell, 2018).

The impact of online harassment is manifold and extensive; victims report an array of physical and psychological negative consequences (e.g. social anxiety, depression, self-harm) as well as an impact on how they conduct their everyday lives (withdrawal from social media and social life). Due to the nature of the online world, the abuse can be long-lasting, the abusers many, and the audience limitless (Universities UK, 2016). Finally, there is existing research on the psychological characteristics of adolescent or child cyberbullying (Ybarra & Mitchell, 2004) but there is little examination of adult characteristics and psychological profile. Predominant motivations or target characteristics for online harassment are in order of frequency: political views, physical appearance, gender, race/ethnicity, sexual orientation, occupation and disability (Davidson et al., 2019).

*Online Hate Speech:*

Hate speech is a complex phenomenon and it normally describes any form of language used online to attack a person or a group based on one or more of their personal protected characteristics [Awan, 2016; Her Majesty’s Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS), 2018]. These personal characteristics include race, ethnicity, gender, religion, sexual orientation and physical or mental disability with the purpose or effect of “promoting hate and inciting violence” (Awan, 2016, p.2). It is often described as *hate content*, *hate material* or *online hate* and can be perpetrated in various ways (words, pictures, symbols, videos and music), by individuals or groups (e.g. cyber-mobs, organised hate groups such as Neo Nazis or the Ku Klux Klan or socio-political organisations; Citron, 2014; Ghafoori et al., 2019). Hate speech can be found on various outlets such as social media, chat rooms, news websites and instant messaging (Bliuc, Faulkner, Jakubowicz & McGarty, 2018).

The scale of the problem is difficult to assess as there are issues with police recording and underreporting by victims due to fears of embarrassment or reprisals from the perpetrator(s), or being unhappy with the outcome of reporting (Littler & Feldman, 2015; Anstead, 2017). However, Ofcom’s Media Use and Attitudes Report (2018b) of nearly 2000 participants showed that almost half had seen online hate in the last year, and of those, younger individuals (16-34) were more likely to have seen online hate. Spikes of online hate speech are positively correlated with high profile events (e.g. terrorist attacks or parliamentary elections; Hambly, Rixom, Singh & Wedlake-James, 2018). Indicatively, over 4 million tweets were identified as containing anti-Islamic content between March and June 2016 (Miller et al., 2016), and a YouGov survey of 5000 LGBT people’s experiences identified that 10% of LGBT people had experienced online hate speech in the space of one month alone (Bachman & Goode, 2017). Furthermore, high profile women, (such as politicians, journalists and experts) or women who assert their views, defend their identity or challenge norms, are frequently victimised via online violence and gender-based hate speech (European Parliament FEMM Committee Rerport 2018). The Inter-Parliamentary Union of the Council of Europe reported alarming statistics of nearly 60% of EU female parliamentarians having been victims of online sexist attacks and rape threats (2018). Rape threats in particular, depending on the context can be viewed as straddling several of the online harassment categories as they can be conceptualised as gender-based hate speech, but also as part of trolling, cyberstalking (as they can make the recipient feel threat against their physical safety) as well as cyber-sexual harassment.

Hate speech has a significant emotional, psychological and physical impact on its victims as well as a significant impact upon society. Drawing from the research on hate crimes, Ghafoori et al (2019) in a briefing paper outlining the traumas of hate based crime conclude that hate speech is part of a pyramid of hatred and intolerance, preceded by prejudice, negative stereotypes and distortions about particular individuals or groups and often followed by hate-based crimes and violence (e.g. threats as well as actual violence and death). The purpose of hate-based violence is “to instil fear and anxiety, inflict psychological damage, diminish a sense of belonging, and to exclude a group identified as ‘other’” (p.5). Victims report post-traumatic disorder (PTSD) symptomatology, depression, anxiety and substance abuse, feelings of anger, guilt, shame and powerlessness. Victims often silence themselves, limit their online activity or change their appearance and behaviours (by being less vocal or visible) in order to feel safer from attacks. Hate speech affects entire groups and communities by making them feel unwelcome and unsafe and that negative impact is linked to the unwillingness to report and the consequent underrepresentation of the phenomenon (Klonoff, Landrine & Ullman, 1999; Ghafoori et al., 2019).

*Trolling:*

Trolling is an activity associated with online forums, where opinion sharing and debate is carried out and encouraged [Department for Digital Culture, Media and Sport (DCMS), 2019] This is considered to be one of the most insidious of the harassing behaviours because of its initial conceptualisation as a humorous and non-offensive exchange with the sole intent of wasting someone’s time or provoking alternative thinking. One of the earliest definitions of trolling described it as luring online users into pointless and time-consuming activities (Herring, Job-Sluder, Scheckler & Barab, 2002). Since then, definitions of trolling have evolved into a malicious and intentional disruptive and abusive behaviour that includes elements of flaming, with offensive and denigrating language used and is equated in the eyes of the public with cyber-harassment and cyberbullying (Buckels, Trapnell & Paulhus, 2014; March & Marrington, 2019).

The true extent of trolling is difficult to estimate due to methodological limitations (survey methodology and lack of confidence intervals and different populations) as well as varying definitions (DCMS, 2019), however an Ofcom report on adult media use and attitudes (2017) stated that 1% of adult internet users are trolling victims and that number rises to 5% if young adults (16-24) are examined. In terms of victimisation, there is difficulty uncoupling the rates of trolling from cyberbullying which often is examined concurrently, and prevalence rates rise from 1-3% to 30-45% when cyberbullying behaviours are included in measures (DCMS, 2019). However, evidence shows that certain groups are more at risk of trolling than others (e.g. women, people of Muslim faith and LGBT communities; DCMS, 2019).

Trolling has a wide impact on its victims with the DCMS (2019) reporting experiences of paranoia, anger, fear, withdrawal from social life or personal relationships and in extreme cases, self-harm and suicide. Trolling is one of the few online behaviours where some information about particular adult psychological perpetrator traits has emerged: studies have found that internet trolls display the “dark tetrad” of narcissism, psychopathy, Machiavellianism and sadism, with sadism being most closely associated with trolling (Buckels, Trapnell & Paulhus, 2014; Cracker & March, 2016; Maltby, 2016).

*Doxing (also spelled doxxing):*

Doxing is recognised as a form of cyber-bullying and harassment and often refers to searching, obtaining and disclosing information of others without their consent (Cambridge Dictionary, 2019). The information is personal, private and sensitive but often not sexual or explicit (thus differs from image based sexual abuse/revenge porn) and the person obtains and triangulates information on personal facts and location freely available online (and not by trickery; Willard, 2007) and ultimately invites others to harass the victim(s). The important consequence of doxing is the link between online and offline harassment as doxers often invite harassment and consequences for victims that can be perpetrated in person (since they share information about physical location, employment details as well as political beliefs; Chen, Cheung & Chan, 2019). Few studies on adults exist, but those who do, characterise doxing as technically simple and perpetrators as often able to collect and deduce information from what is publically available, with differing motivations such as competition, revenge for unfair behaviour on self or a third party, or vigilanteism such as de-anonymising KKK members or child abusers or sometimes harassment and rape victims (Snyder, Doerfler, Kanich & McCoy, 2017). Doxing can result in long lasting and serious effects on its victims (e.g. termination of employment, self-harm and suicide) who tend to be internet users of all ages and genders (but typically gamers and people in the public eye such as politicians and celebrities; Snyder et al., 2017).

*Cyberstalking:*

Cyberstalking and cyber-harassment are also terms that may be used interchangeably in media coverage and as with the legal definition of stalking, there is similarity in what behaviours are recognised as part of the phenomenon. For example, cyberstalking is considered to include repetitive emails, texts or instant messages that are offensive or threatening, posting comments about the recipient online, online impersonation, tracking the victim, and sharing intimate photos or videos online (this also could be image based sexual abuse/revenge pornography which will be outlined in the next section). Nevertheless, there are some key distinctions that separate the terms according to scholarly and legal definitions: for Brown, Gibson and Short (2017) the key difference between cyber-harassment and cyberstalking is the “repetitive and deliberate use of the internet and electronic communication tools to frighten, intimidate or harass someone” (p. 57). Therefore, even though the purpose, or effect, of harassment is necessary for cyber-harassment, cyberstalking is distinguished by repetitive behaviour perpetrated by the same person, and targeting the same person or persons causing them to feel fear for their safety (Strawhun, Adams & Huss, 2013).

Cyberstalking appears to have grown in prevalence in the last 10 years, which could be attributed to better legislation and recognition of behaviours, as well as broader definitions of cyberstalking. Epidemiological studies are lacking and most existing evidence comes from student surveys with self-identifying victims (Cavezza & McEwan, 2014). Different studies involving students, conducted 10 years apart, showed that in 2009-2010 student victims of cyberstalking were between 9-13% (Paullet, Rota & Swan, 2009; Kraft & Wang, 2010), where as in 2019 nearly 50% of students reported having been affected by cyberstalking (Maran & Begotti, 2019). According to the Pew Research Center (2017), in the US incidences of online harassment (including cyberstalking) have risen by 10% in 3 years, and similarly to all online harassment behaviours, self-identified victims of cyberstalking tend to be younger adults (18-29), female (Straude-Muller et al., 2012) and more traumatised than victims of other harassment types. Cyberstalking victims experience a profound and continued state of anxiety and fear that often results in changes of living habits, coupled with feelings of anger paranoia, insomnia and depression (Maran & Begotti, 2019), and 34% of victims experience PTSD (Maple, Short & Brown, 2011).

The available data for adult perpetrator characteristics are sparse and not conclusive and there needs to be significant further research, however, males are identified as the more likely perpetrators. Three large studies concluded that cyberstalking is not distinguishable from, or a subset of offline stalking in terms of pattern and frequency of behaviours as well as impact (Sheridan & Grant 2007; Maple et al., 2011; Nobles, Rayns, Fox & Fisher, 2014). In their findings, despite variability in categories recognised and victim characteristics, all three concluded that the majority of victims were female (with males more likely to be cyberstalking victims than offline stalking victims), they were mostly victims of cyberstalking or a crossover between offline and online stalking, and the perpetrators were more likely to be acquaintances and ex partners (depending on the mode of stalking). Cavezza and McEwan (2014) conducted a study comparing individuals convicted of offline and cyberstalking and found that there weren’t many distinguishing characteristics between the two samples: the majority of offenders from both groups were diagnosed with a personality disorder or displayed problematic personality traits, had the same median duration of stalking (36 weeks), and they predominantly targeted women. One significant difference found between online and offline stalkers in that group was that the cyberstalkers were more likely to target ex partners than offline stalkers with the motivation of either resuming the relationship or exacting revenge for its demise (Cavezza & McEwan, 2014).

**Online Sexual Harassment and Abuse:**

Years of research on sexual violence point to a global and significant problem, with young women (16-24) widely recognised as at significant risk of sexual victimisation at the hands of men who are known to them (e.g. boyfriends, friends or acquaintances) and 55% of women in the European Union having experienced sexual harassment at least once since the age of 15 (EU Agency for Fundamental Rights, 2014; Henry & Powell, 2018). It is of no surprise that current digital technologies are used as ways to facilitate and commit such sexual harms, and the varied nature and prevalence of such online behaviours against adults have commanded the attention of researchers and policy makers alike. Again, the conceptual but also behavioural overlap between many of these online abusive behaviours has made it a challenge for scholars to distinguish a clear line between sexual and non-sexual harms, or to indeed separate gendered from non-gendered abuse, but as the European Institute for Gender Equality (2017) noted, online harassment and abuse against women has not yet been fully conceptualised or examined, with no EU or global survey on the prevalence and harms of these particular types of behaviours against women, and nascent research at national level within member states (Henry & Powell, 2018; Davidson et al., 2019).

*Technology Facilitated Sexual Violence (TFSV)*

Technology Facilitated Sexual Violence (TFSV) is an umbrella term coined by Nicola Henry and Anastasia Powell (2018) in their review of the sexualised online abuse against adults literature, to describe an array of sexually harassing and aggressive behaviours that enable online and offline sexual abuse that can be criminal or civil (Henry & Powell, 2018). The authors distinguish 4 different categories of TFSV which encompass various facets of online sexual harassment; *cyber sexual harassment*, *cyber gender harassment*, *cyberstalking*, and *image based sexual abuse* (otherwise referred to as revenge pornography; Henry & Powell, 2018). While a vast array of sexual and non-sexual aggressive behaviours would fall within these categories, for this part of this chapter we will focus on two of these sexual abuse behaviour categories; cyber-sexual harassment (encompassing online sexual solicitation) and image based sexual abuse and the particular modes of conduct associated with them (cyberstalking has been discussed in the previous section and cyber gender harassment has been discussed in brief in the online harassment section).

*Cyber sexual harassment*

Similarly to Henry & Powell’s 2018 review, Barak’s (2005) more narrow definition of online sexual harassment as unwanted sexual attention online, with unwelcome behaviours that explicitly convey unwanted sexual desires and intentions towards a person, is adopted in this section. This can be perpetrated in public or private online forums, using words or images, via texting, internet or email (Henry & Powell, 2018). Cyber sexual harassment includes unwanted sexually explicit emails, texts or messages, repeated requests for chats or dates, “coercive sexting” (being pressured into sending intimate images; Drouin, Ross & Tobin, 2015; Englander, 2015), receiving unsolicited nude or sexual images (e.g. “dick pics”; Powell & Henry 2017). Similarly to all other categories examined, the overall prevalence and impact of cyber-sexual harassment are difficult to establish because some of these behaviours are included on cyberstalking or cyberbullying surveys (the Pew Research Centre includes cyber sexual harassment in the 41% of young US people; 2014). There is, however some tentative evidence of prevalence of receiving nude or sexual images with 1 in 2 women (aged 18-34) having received “dick pics” at least once, and 78% of those pics were unsolicited (YouGov, 2017). Interestingly, 50% of women characterised such content as unwelcome and disgusting in the YouGov survey, whereas 30% of men labelled it as sexy compared to only 9% of women, indicating a misperception of the impact of sending such material (2017). Finally, most of the available evidence on coercive sexting comes from studies with children or adolescents, therefore establishing a clear prevalence and pattern is challenging. However, there are some studies that examined adult sexting behaviour, establishing that it is relatively common among young people [between 43% in Gordon-Messer, Bauermeister, Grodzinski & Zimmermann (2013) and 66% in Gamez-Quadix, Almendros, Borrajo & Calvete (2015)] and that between 20% (Drouin, Ross & Tobin, 2015) and 70% (Englander, 2015) had experienced some form of pressure to sext. Commonly victims of this form of cyber-sexual harassment are younger women and non-heterosexuals (Gamez-Quadix et al., 2015; Henry, Flynn & Powell, 2019).

*Image Based Sexual Abuse:*

One form of online abuse that has garnered a significant amount of scholarly and public attention is the non-consensual sharing of intimate images and media (NCII; Walker & Sleath, 2017; Powell, Henry & Flynn, 2018), commonly referred to as “revenge pornography” or simply “revenge porn”. Such sharing of intimate media has troubled researchers and policy makers alike due to the proliferation of creating, uploading and sharing as well the practical difficulty of removing such content from various websites (Powell et al., 2018). Other names used in the literature to describe the phenomenon are “non-consensual pornography” (Citron & Franks, 2014; Eaton, Jacobs & Ruvacalba, 2017) and “involuntary pornography” (Burns, 2015), but the media generated “revenge porn” term still remains a popular identifier usually for a typical scenario of a dissolved relationship or a jilted ex-partner who then distributes explicit media to exact revenge on perceived or actual infidelity or wrongdoing.

Australian and UK scholars (McGlynn & Rackley, 2016; Powell et al, 2018) have argued that any terminology that contains the word “pornography” in a non-consensual context is trivialising and misleading and puts the focus on the product (content) rather than the perpetrators’ abusive and exploitative actions and the significant impact it has on the victims. Such material is shared without the original sender’s (creator’s) consent and it should not be viewed as pornography as it has not been generated for public consumption. The aforementioned scholars have put forward the new term of Image Based Sexual Abuse (IBSA) to denote the exploitative, violating and abusive nature of such acts, but to also encompass a variety of different behaviours that contain non-consensual distribution, threat of distribution, as well as creation of personal and explicit material (Powell et al., 2018).

Importantly, Powell and colleagues propose that the motivation behind such actions can be varied and complex and include revenge, monetary gain, notoriety, sexual gratification and voyeurism. In their typology of IBSA they recognise 5 main typologies: *relationship retribution*; where current or former intimate partners seek revenge by distributing intimate images; *sextortion,* where perpetrator(s) can either threaten to distribute intimate images (whether or not they exist) and use that threat to obtain further imagery, monetary gain or coerce sexual acts (physical or virtual); *sexual voyeurism,* where perpetrator(s) seek to create (via multiple methods including “upskirting” or “downblousing” towards often unsuspecting victims) or share intimate imagery for sexual gratification; *sexploitation,* where perpetrators seek to obtain money by sharing and trading intimate imagery; *and sexual assault,* where perpetrators or bystanders record sexual assaults or rapes and then distribute them (Powell et al., 2018, p.306). Davidson et al. (2019) also add a sixth category of *domestic violence*, where the images are either taken without consent or threats of consensual images are used to blackmail, coerce and control victims in an intimate partner violence context. This media is either recorded by the victims (in the form of selfies or videos), recorded by another person, stolen (hacked), or manipulated (by superimposing the face of a victim on existing naked images or pornographic videos also known as “fakeporn”; McGlynn, Rackley & Johnson, 2019).

In the last 6-7 years, several studies have attempted to record the prevalence, nature and impact of IBSA, with notable large scale studies conducted in the US (Eaton et al., 2017), Australia (Powell & Henry, 2016, 2017; Powell, Henry, Flynn & Scott, 2019) and the UK (McGlynn et al., 2019). Data shows that prevalence rates vary from 1 in 5 adults experiencing non-consensual taking of personal images, and 1 in 10 experiencing non-consensual distribution, or threat of distribution, of personal images, while 11% of adults admitted to having perpetrated IBSA (Eaton, et al., 2017; Henry et al., 2019). Despite IBSA having been traditionally conceptualised as a gendered issue with women being overwhelmingly victimised (Citron, 2014; Powell et al., 2018), newer data shows that IBSA victimisation is not significantly different between genders (Henry et al., 2019), but is different between ages (younger adults 16-29 years of age), sexualities (LGBT adults victimised at a higher rate than heterosexual adults) and disability (disabled adults reported significantly higher rates of victimisation than non-disabled). The same study shows however that females are more likely to be victimised by a male perpetrator and male victims more likely to be victimised by a female perpetrator, although overall more than half of the perpetrators were reportedly male (Henry et al., 2019).

The emotional, psychological and physical impact of IBSA is deleterious and wide ranging and can lead to serious and long-lasting consequences for the victims. Victims are often reported to struggle with shame, self-blame, helplessness, paranoia and isolation and mention a loss of integrity, dignity, security and self-esteem (McGlynn & Rackley, 2016; McGlynn et al., 2019). Mental health problems include anxiety, depression, anorexia, PTSD and self-harm and suicide (attempted and completed). Victims of IBSA are also at a high risk of secondary victimisation such as online harassment including cyberstalking, hate speech, as well as offline assault, stalking and even murder (Kitchen, 2015; McGlynn & Rackley 2017). The impact of IBSA victimisation extends to the professional and social lives of the victims, with employment, education and relationships significantly affected, causing the victims job loss, difficulty finding new employment (as imagery is often easily accessible and difficult to remove), financial loss, reputational damage, and social isolation (Citron & Franks, 2014; Scheller, 2015; McGlynn et al., 2019). McGlynn and colleagues suggest that IBSA harms need to be viewed holistically and use the term “social rupture” to encapsulate and recognise the experiences of significant devastation and alteration of victims’ lives, as well as the level of intrusive violation of bodily integrity and privacy that they experience, coupled with the inhibition of their sexual autonomy and expression (2019).

Research examining the characteristics and motivations of perpetrators is nascent and significantly behind that of IBSA victimisation. Some studies have examined the motivations of perpetrators (Garcia et al., 2016; Eaton et al., 2017; Hall & Hearn, 2017; Uhl, Rhyner, Terrance & Lugo, 2018) showing that they vary from amusement, to vengeance, to social status and masculinity affirmation, to sexual gratification, with many perpetrators reporting that they shared the contents with their friends meaning no harm to the victim. A UK based study is one of the only ones to have examined personality traits and perpetration of IBSA (Pina, Holland & James, 2017) and found that Machiavellianism and narcissism as well as sexist beliefs were significant predictors of the proclivity to engage in IBSA. Furthermore, a recent Australian study on perpetration of IBSA (Powell et al., 2019) found that males were significantly more likely than females and LGB adults more likely than heterosexuals to report perpetrating IBSA but their target victims were equally likely to be males or females. Additionally, victims were more likely to have been intimate or ex-partners, family members and acquaintances than strangers, which authors suggested is indicative of IBSA being a method of harassment and abuse both in intimate relationships as well as non-partner contexts (Powell et al., 2019). Finally, participants who were more likely to believe in and accept myths about IBSA, and more likely to blame the victim for the abuse experience, and having been victims of IBSA themselves, were also more likely to have perpetrated IBSA.

**Criminalisation/Legislation of Online Harassment Behaviours:**

Despite recent governments’ tenets that what is illegal offline is also illegal online, there is widespread recognition and concern among scholars and policy makers that offline laws largely predate the internet, do not sufficiently cover all the possible negative online experiences and cannot accurately reflect the number of victims affected or perpetrators involved (Strickland & Dent, 2017; Davidson et al., 2019). There have been numerous consultations and parliamentary committees over the last few years that resulted in differing conclusions regarding the suitability of current legislation for online abuse; in July 2014, a report by the House of Lords Communications Committee concluded that “although much of the relevant law predated social media, it was still generally appropriate” (Strickland and Dent, 2017; p.11), whereas in 2017 the Home Affairs Select Committee recommended a complete revision of the legislative framework that examines online harassment, hate speech and extremism. Currently there are no separate laws that cover online harassment as a whole or distinct form of online abuse, however there exist a number of offenses that can be applied to aspects of online harassment such as trolling, cyberbullying, hate speech and cyber-harassment (Strickland & Dent, 2017; p. 7):

* harassment - section 2, 2A, 4 & 4A of the Protection from Harassment Act 1997.
* improper use of a public electronic communications network - section 127 of the Communications Act 2003.
* sending indecent, grossly offensive, false or threatening communications - section 1 of the Malicious Communications Act 1988

*Cyberstalking*: In the United Kingdom, the Protection from Harassment Act (1997) covering stalking, now contains cyberstalking, which was introduced into the act through the Protection of Freedoms Act 2012. Depending on the act committed, a person may also be committing offences as outlined by the Offences Against the Person Act 1861 (threats to kill); the Sexual Offences Act 2003 (sending indecent images); and the Malicious Communications Act 1998 (sending grossly offensive communications). Offences under these Acts in the UK could result in immediate prison sentences.

*Revenge pornography*: in the United Kingdom, Section 33 of the Criminal Justice and Courts Act 2015 makes a criminal offence - subject to up to 2 years imprisonment- to disclose a private, sexual image without the consent of the person in the image and with the intention of causing that person distress. This applies to online and offline images that can be shared both online or offline (Strickland & Dent, 2017). Despite being welcomed as a positive step in the right direction, this legislation has come under scrutiny and criticism in recent years, as we have come to understand the behaviours entailed better, as well as the motivations behind the offence, and also have had a chance to evaluate its effectiveness. McGlynn et al. (2019) state that lack of anonymity afforded to victims is preventing them from coming forward and could also expose them to further victimisation. Indeed the North Yorkshire Police, Fire and Crime Commissioner’s (NYPFCC, 2018) IBSA report states that victims of IBSA are afraid to report to the police for fear of being shamed and further harassed due to lack of anonymity, which is reflected in statistics showing that “as the numbers of cases reported have grown, the percentage of those resulting in charges have declined from 14% in 2015/16 to 7% in 2017/18” (p. 4) and that 1 in 3 are withdrawn by the victims. This report calls for effective revision of the current legislation to afford anonymity and include the wider range of IBSA identified behaviours (NYPFCC, 2018). Furthermore, McGlynn et al (2019) state that threats and altered images (“deepfakes” or “fakeporn”) as well as other motivations are not currently covered in England and Wales legislation (threats and altered images are included in Scottish legislation) and that the legal threshold is too high, with having to prove that the intention of the perpetrator was to cause harm and distress rather than also including recklessness (as Scottish legislation does). The Law Commission was reportedly (in July 2019, as part of its review) considering the case for providing IBSA victims automatic anonymity to match the current standard for sexual offences (Independent, 2019)

*Upskirting*: it is now a criminal offence in England and Wales to take an upskirt or downblouse video or image but only if the intention was to cause distress or for sexual gratification. While recording, photographing or viewing someone engaged in sexual activity or toileting against their consent is illegal, it is only so if done for sexual gratification. McGlynn et al. (2019) criticise that this narrow definition is excluding various forms of IBSA and places unbalanced weight on the differing motivations rather than the harm caused.

Despite a couple of high profile convictions of “revenge porn” website owners and the subsequent closure of their webpages (e.g. Kevin Bollaert’s conviction for ugotposted.com and Hunter Moore’s closure of isanyoneup?.com and subsequent conviction for identity theft), and the recognition and collaboration of major websites, social media platforms and dating sites (e.g. Facebook; Google; Twitter; OKCupid), removing IBSA content remains hugely problematic as different –often inconspicuous- websites and perpetrators still remain undetected due to legal loopholes, encryption, anonymity and obscurity.

Following the work of scholars, activists and campaigners, the UK government is now considering a new regulatory framework within which online businesses, internet providers and users have delineated responsibilities and rights and companies will have to adhere to a statutory duty of care towards their users and will be delimited by an independent regulator. The Online Harms White Paper (Home Office, 2019) invited a consultation of legal scholars, policy makers and internet providers and online businesses, which was open from April until July 2019 and invited advice and ideas on effective internet safety for users from a variety of criminal and non-criminal behaviour that can negatively affect users (including online harassment, abuse and exploitation, terrorism, radicalisation, online gangs). The White Paper is intended to include the closest thing to a comprehensive online harassment law that would include harassment, stalking, hate crime, revenge porn, identity theft, online grooming and trolling (Home Office in the Media, 2019).

**Looking to the future: conceptual harmonisation, practical implications and future research.**

Despite the ongoing research and policy interest and strides in its examination and demarcation, online harassment and abuse against adults in particular still remains an emerging field. Most of the research is limited in scope and numbers with virtually none examining all behaviours associated with online abuse at once, or indeed the context in which they occur. While often parallelised with offline harassment and sexual violence and thought to be sharing many characteristics and motivations, online harassment remains -to a large extent- still a mystery and evidence regarding the appropriateness of these offline analogies is lacking.

Perhaps the most consistent argument made throughout this chapter is the need for a comprehensive and harmonised definition of online harassment. The significant conceptual and empirical overlap between terminologies used to describe various facets of online abuse towards adults results in difficulty in addressing the prevalence, impact and epidemiology of the phenomenon, as well as making recommendations for its prevention and management. We currently still do not know enough about the motivations of adult perpetrators of this phenomenon, their characteristics, the role of bystanders and how they are implicated, or the specific victim vulnerabilities, so that appropriate sanctions, rehabilitation and support are put in place. As technology is evolving rapidly, researchers are always striving to keep up with developments and understand their impact on internet users. What is clear, however, from existing research is that online users are concerned about their safety and conduct and also experience and perpetrate abuse and harassment at alarming rates.

We have been given a powerful tool in the form of the internet, with no manual on how to appropriately use it and no full comprehension of the impact of our actions on others and ourselves. We appear to be more cognisant of the risks for particularly vulnerable groups of users such as children and young people; their media and internet literacy has been extensively examined (e.g. Livingstone, Bober & Helsper, 2005; Leung & Lee, 2012) and specific online safety recommendations have been rolled out to schools (Department for Education, 2019). Nevertheless, although adult advice for the risks of online abuse and how to avoid it does exist, there is no systematic campaign of awareness targeting adults, no unified messages for perpetrators and victims, and the expectation is that adults are responsible for their own education and risk awareness; which often results in victim blaming when they fall prey to different online abuse (Scott, Wiencierz & Hand, 2019). There is pressing need for a systematic campaign of awareness and advice for adults of all age groups if we are to minimise and prevent online abuse and harassment.

The research and policy arena examining online behaviours is a hive of activity and strides have been made in our understanding of this phenomenon. Many studies and reviews are being conducted at present looking into different facets of online abuse and harassment and its impact, with promising findings that bring us steps closer to an online world free of abuse. Nevertheless, there is pressing need for more representative samples of different cultures, as well as in depth qualitative studies in order to recognise and address the nature and manifestations, impact, needs and risks of the phenomenon of online harassment as a whole. Furthermore, comprehensive reviews of legislation, police responses, as well as organisational responses (such as higher education institutions and schools) are necessary to harmonise actions taken and identify best practice. For higher education in particular, a significant investment was made for the tackling of sexual misconduct, online harassment and hate speech, and the results of studies funded though the Office for Students (OfS, 2019) are now steadily being published (for a recent report of online harassment and hate crime in Higher Education Institutions see Phippen & Bond 2020; also Universities UK 2019). It is now pertinent that the results of these studies are collated and examined in parallel and best practice identified as a whole rather than focusing on individual organisational responses so that all affected are responded to effectively, fairly and consistently.

The calls for changes in legislation that have resulted from years of research and campaigning by scholars and activists are finally being met and the White Paper recommendations for a legislative framework that would protect against online abuse and harassment as a wholistic category of interrelated offences, are eagerly awaited. Despite legitimate criticisms about the impact on individual freedoms (Penney, 2018) new legislation or guidelines will have a significant impact on forensic psychologists and mental health practitioners and how they manage risk and rehabilitation of those implicated, as well as provide support for the victims affected. As a field we must be vigilant and agile to adapt our practices to new developments so that we can ensure better safeguarding for all.

References:

Age UK (2019). Staying safe online. Available at: <https://www.ageuk.org.uk/information-advice/work-learning/technology-internet/internet-security/>

Anstead, A. (2017) Dealing with hate crime. EU: European Network Against Racism. Available at: <https://www.ukren.org/uploads/Dealing%20with%20hate%20crime.pdf>.

Awan, I. (2016). Islamophobia on Social Media: A Qualitative Analysis of Facebook’s Walls of Hate. *International Journal of Cyber Criminology, 10* (1), 1-20.

Bachmann, C. & Goode, B. (2017) LGBT in Britain - Hate crime and discrimination. London: Stonewall. Available at: <https://www.stonewall.org.uk/lgbt-britain-hate-crime-and-discrimination>

Banerjee, A., & Sharma, B. (2011). Gender differences in perception of workplace sexual harassment among future professionals. *Industrial Psychiatry Journal, 20*, 21-24

Barak, A. (2005). Sexual harassment on the internet. *Social Science Computer Review, 23*(1), 77-92

Barkoukis, V., Brighi, A., Casas, J. A., Del Rey, R., Gobel, K., Guarini, A., Plichta, P., Pyzalski, J., Scheithauer, H., Smith, P. K., Schultze-Krumbholz, A., Thompson, F., Tsorbatzoudia, H. (2015). A comparison of classification approaches for cyberbullying and traditional bullying using data from six European countries. *Journal of School Violence, 14* (1), 47-65

Bentley, H., Burrows, A., Hafizi, M., Kumari, P., Mussen, N., O’Hagan, O., & Peppiate, J. (2019). How safe are our children? 2019. An overview of data on child abuse online. London: NSPCC Available at: <https://learning.nspcc.org.uk/research-resources/how-safe-are-our-children/>

Blackwell, L., Dimond, J., Schoenebeck, S., & Lampe, C. (2017). Classification and its consequences for online harassment: Design insights from HeartMob. *Proceedings of the ACM on Human-Computer Interation 24* doi:10.1145/3134659

Bliuc, A-M., Faulkner, N., Jakubowicz, A., & McGarty, C. (2018). Online networks of racial hate: A systematic review of 10 years of research on cyber-racism. Computers in Human Behavior, 87, 75-86.

Brown, A. (2017). What is so special about online (as compared to offline) hate speech? *Ethnicities 18*(3), 297-326.

Brown, A., Gibson, M. & Short, E. (2017). Modes of cyberstalking and cyberharassment: Measuring the negative effects in the lives of victims in the UK. *Annual Review of CyberTherapy and Telemedicine, 15*, 57-63.

Buckels, E. E., Trapnel, P. D., & Paulhus, D. L. (2014). Trolls just want to have fun. *Personality and Individual Differences, 67*, 97-102.

Burns, A. (2015). In full view: Involuntary porn and the postfeminist rhetoric of choice. In C. Nally & A. Smith (Eds), *Twenty-first Century Feminism: Forming and Performing Femininity.* Springer Nature.

Butler, S. M., & Seto, M. C. (2002). Distinguishing two types of adolescent sex offenders. *Journal of the American Academy of Child and Adolescent Psychiatry 41*(1), 83-90. doi: [10.1097/00004583-200201000-00015](https://doi.org/10.1097/00004583-200201000-00015)

Cambridge Dictionary (2019). Doxing. Available at: <https://dictionary.cambridge.org/dictionary/english/doxing>

Cavezza, C. & McEwan, T. (2014). Cyberstalking versus offline stalking in a forensic sample. *Psychology, Crime and Law, 10*, 955-970.

Chen, M., Cheung, A. S. Y., & Chan, K. L. (2019). Doxing: What adolescents look for and their intentions. *International Journal of Environmental Research and Public Health, 16*(2), 218.

Citron, D. K. (2014). *Hate crimes in cyberspace.* Harvard University Press. ISBN 978-0-674-36829-3.

Citron, D. K. & Franks, M. A. (2014). Criminalizing Revenge Porn. *Wake Forest Law Review, 49*, 345

Cracker, N., & March, E. (2016). The dark side of Facebook: The Dark Tetrad, negative social potency and trolling behaviours. *Personality and Individual Differences, 102*, 79-84

Cybersmile Foundation (2017). Stop Cyberbullying Day Survey 2017. Retrieved December 15 2019 from: <https://www.cybersmile.org/wp-content/uploads/Stop-Cyberbullying-Day-Survey-2017.pdf>

Davidson, J., Livingstone, S., Jenkins, S., Gekoski, A., Choak, C., Ike, T., & Phillips, K. (2019). Adult online hate, harassment and abuse: A rapid evidence assessment. UK Council for Internet Safety (UKCIS) Available at: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811450/Adult_Online_Harms_Report_2019.pdf>

Davies, S. (2019). Decoding the social media algorithms in 2019. The ultimate guide. Available at: <https://www.stedavies.com/social-media-algorithms-guide/>

Department for Culture Media and Sport (2019). Rapid Evidence Assessment: The prevalence and impact of online trolling. DCMS Available at: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811449/DCMS_REA_Online_trolling_.pdf>

Department for Education (2019). Teaching online safety in school. London: DfE. Available at: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf>

Drouin, M., Ross, J., & Tobin, E. (2015). Sexting: A new digital vehicle for intimate partner aggression? *Computers in Human Behavior, 50*, 197–204.

Duggan, M., Ellison, N. B., Lampe, C., Lenhart, A., & Madden, M. (2015). Social Media Update 2014. Pew Research Center, January 2015 Available at: <https://www.pewresearch.org/internet/2015/01/09/social-media-update-2014/>

Eaton, A. A., Jacobs, H., & Ruvacalba, Y. (2017). Nationwide online study of non-consensual porn victimization and perpetration: A summary report. Cyber Civil Rights Initiative Inc. Available at: <https://www.cybercivilrights.org/wp-content/uploads/2017/06/CCRI-2017-Research-Report.pdf>

Englander, E. (2015). Coerced sexting and revenge porn among teens. *Bullying, Teen Aggression & Social Media, 1*, 19–21.

Equality Act 2010. Available at: <http://www.legislation.gov.uk/ukpga/2010/15/contents>

European Institute for Gender Equality (2017). Cyber violence against women and girls. EIGE. Available at: <https://eige.europa.eu/publications/cyber-violence-against-women-and-girls>

European Parliament FEMM Committee (2018). Cyber violence and hate speech online against women. FEMM. Available at: <http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf>

European Union Agency for Fundamental Rights (2014). *Violence against women: an EU-wide survey. Main Results report.* Available at: <https://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report>

Gámez-Guadix, M., Almendros, C., Borrajo, E., & Calvete, E. (2015). Prevalence and association of sexting and online sexual victimization among spanish adults. *Sexuality Research and Social Policy, 12*, 145- 154.

Garcia, J. R., Gesselman, A. N., Siliman, S. A., Perry, B. L., Coe, K., & Fisher, H. E. (2016). Sexting among singles in the USA: Prevalence of sending, receiving, and sharing sexual messages and images. *Sexual Health, 13*(5), 428-435.

Ghafoori, B., Caspi, Y., Salgado, C., Allwood, M., Kreither, J., Tejada, J.L., Hunt, T., Waelde, L.C., Slobodin, O., Failey, M., Gilberg, P., Larrondo, P., Ramos, N., von Haumeder, A., & Nadal, K. (2019). Global Perspectives on the Trauma of Hate-Based Violence: An International Society for Traumatic Stress Studies Briefing Paper. Available at: <https://www.istss.org/ISTSS_Main/media/Documents/ISTSS-Global-Perspectives-on-the-Trauma-of-Hate-Based-Violence-Briefing-Paper.pdf>

Gordon-Messer, D., Bauermeister, J. A., Grodzinski, A., & Zimmerman, M. (2013). Sexting among young adults. *Journal of Adolescent Health, 52*(3), 301-306.

Grimes, G. A., Hough, M. G., Mazur, E., & Signorella, M. L. (2010). Older adults’ knowledge of Internet hazards. *Educational Gerontology, 36*, 173-192.

Hall, M., & Hearn, J. (2017). Revenge pornography and manhood acts: A discourse analysis of perpetrators’ accounts. *Journal of Gender Studies, 28*(2), 158-170.

Hambly, O., Rixom, J., Singh, S., & Wedlake-James, T. (2018). Hate crime: a thematic review of the current evidence. London: Home Office Research Report 102. Available at: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/748140/hate-crime-a-thematic-review-of-the-current-evidence-oct2018-horr102.pdf>

Henry, N., Flynn, A., & Powell, A. (2019). Image-based sexual abuse: Victims and perpetrators. Trends & Issues in Crime and Criminal Justice, March 2019(572), 1-19.

Henry, N. and Powell, A., 2016. Sexual violence in the digital age: The scope and limits of criminal law. Social and Legal Studies, 25(4), pp.397-418.

Henry, N., & Powell, A. (2018). Technology-facilitated sexual violence: A literature review of empirical research. *Trauma, Violence & Abuse, 19*(2), 195-208.

Herring, S., Job-Sluder, K., Scheckler, R., & Barab, S. (2002). Searching for safety online: Managing “trolling” in a feminist forum. *The Information Society, 18*(5), 371-384.

HMICFRS (2018) Understanding the difference the initial police response to hate crime. London: HMICFRS. Available at: <https://www.justiceinspectorates.gov.uk/hmicfrs/wpcontent/uploads/understanding-the-difference-the-initial-police-response-to-hatecrime.pdf>

Home Instead (2013). Senior fraud protection toolkit: Helping seniors stay safely at home. Available at: <http://homeinstead.co.uk/resources/senior-fraud-toolkit.pdf>

Home Office (2019). Online Harms White Paper. London: Home Office Available at: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf>

Home Office in the Media (2019). Online Harms White Paper Factsheet. Available at: <https://homeofficemedia.blog.gov.uk/2019/04/08/online-harms-white-paper-factsheet/>

Independent (2019). *Revenge porn victims could be granted anonymity in review of online abuse laws*. Available at: <https://www.independent.co.uk/news/uk/home-news/revenge-porn-victims-anonymous-online-abuse-laws-review-a8974516.html>

Inter Parliamentary Union (2018). Sexism, harassment and violence against women in parliaments in Europe. IPU Issues Brief. Available at: <https://www.ipu.org/resources/publications/issue-briefs/2018-10/sexism-harassment-and-violence-against-women-in-parliaments-in-europe>

Internet World Stats (2019). Internet Growth Statistics 1995-2019. Retrieved December 18 2019 from: <https://www.internetworldstats.com/emarketing.htm>

Klonoff, E. A., Landrine, H., & Ullman, J. B. (1999). Racial discrimination and psychiatric symptoms among Blacks. Cultural Diversity and Ethnic Minority Psychology, 5(4), 329–339

Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin, 140*(4), 1073-1137 doi: 10.1037/a0035618

Kraft, E., & Wang, J. (2010). An exploratory study of the cyberbullying and cyberstalking experiences and factors related to victimization of students at a public liberal arts college. *International Journal of Technoethics, 1*, 74–91

Leung, L., & Lee, P. S. N. (2012). Impact of internet literacy, internet addiction symptoms and internet activities on academic performance. *Social Science Computer Review, 30*(4), 403-418.

Littler, M. & Feldman, M. (2015), Tell MAMA reporting 2014/2015: Annual monitoring, cumulative extremism, and policy implications. Teeside: Teesside University Press. Available at: <https://research.tees.ac.uk/ws/portalfiles/portal/4250550/Tell_Mama3.pdf>

Livingstone, S., Bober, M., & Helsper, E. (2005). *Internet literacy among children and young people: findings from the UK Children Go Online project* [online]. London: LSE Research Online.  
Available at: http://eprints.lse.ac.uk/archive/00000397

Livingstone, S., Davidson, J. & Bryce, J. (2017) *Children’s online activities, risks and safety*. London: DCMS. Available at: <http://www.lse.ac.uk/business-and-consultancy/consulting/assets/documents/childrens-online-activities-risks-and-safety.pdf>

Maltby, J., Day, L., Hatcher, R.M., Tazzyman, S., Flowe, H. D., Palmer, E. J., Frosch, C. A., O’Reilly, M., Jones, C., Buckley, C., Knieps, M., & Cutts, K. (2016). Implicit theories of online trolling: Evidence that attention-seeking conceptions are associated with increased psychological resilience. *British Journal of Psychology, 107*(3), 448-466.

Maran, D. A., & Begotti, T. (2019). Prevalence of cyberstalking and previous offline victimization in a sample of Italian university students. *Social Sciences, 8*, 30-40.

March E., & Marrington, J. (2019). A qualitative analysis of internet trolling. *Cyberpsychology, Behavior and Social Networking, 22*(3), 192-197.

Maple, C., Short, E., & Brown, A. (2011). *Cyberstalking in the United Kingdom: An analysis of the ECHO Pilot Survey.* Luton, UK: National Centre for Cyberstalking Research, University of Bedfordshire

McGlynn, C., & Rackley, E. (2016). Image-based sexual abuse: More than just “revenge porn”. University of Birmingham Research Spotlight: Available at: <https://www.birmingham.ac.uk/Documents/college-artslaw/law/research/bham-law-spotlight-IBSA.pdf>

McGlynn, C., & Rackley, E. (2017). Image-based sexual abuse. *Oxford Journal of Legal Studies, 37*(3), 534-561.

McGlynn, C., Rackley, E., & Johnson, K. (2019). Shattering lives and myths: A report on image-based sexual abuse. London: UK Supreme Court. Available at: <https://victimscommissioner.org.uk/publications/shattering-lives-and-myths-a-report-on-image-based-sexual-abuse-by-professor-clare-mcglynn-professor-erika-rackley-and-assistant-professor-kelly-johnson/>

Miller, C., Arcostanzo, F., Smith, J., Krasodomski-Jones, A., Wiedlitzka, S., Jamali, R., & Dale, J. (2016). Brexit: The digital aftermath. London: Demos Available at: <https://www.demos.co.uk/wp-content/uploads/2016/07/Dispatches-Brexit-Demos.pdf>

Nobles, M.R., Reyns, B.W., Fox, K.A., & Fisher, B.S. (2014). Protection against pursuit: A conceptual and empirical comparison of cyberstalking and stalking victimization among a national sample. *Justice Quarterly, 31*, 986–1014.

North Yorkshire Police, Fire & Crime Commissioner (2018). Suffering in silence: Image based sexual abuse report. Available at: <http://www.nomorenaming.co.uk/wp-content/uploads/2018/11/Suffering-in-Silence-2018.pdf>

NSPCC (2016). What children are telling us about bullying. London: NSPCC. Available at: <https://learning.nspcc.org.uk/research-resources/2016/what-children-telling-childline-about-bullying/>

Ofcom (2017). Adults’ media use and attitudes report 2017. Available at: <https://www.ofcom.org.uk/__data/assets/pdf_file/0020/102755/adults-media-use-attitudes-2017.pdf>

Ofcom (2018a). Communications Market Report. Available at: <https://www.ofcom.org.uk/__data/assets/pdf_file/0022/117256/CMR-2018-narrative-report.pdf>

Ofcom (2018b). Children and parents: Media use and attitudes report 2018. Available at: <https://www.ofcom.org.uk/__data/assets/pdf_file/0024/134907/children-and-parents-media-use-and-attitudes-2018.pdf>

Office for National Statistics (2017). Internet users in the UK 2017. How internet use is correlated to various socio-demographic characteristics such as age, sex, disability and geographical location. Available at: <https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2017>

Office for Students (2019). *Consultation on harassment and sexual misconduct in higher education*. Available at: <https://www.officeforstudents.org.uk/publications/consultation-on-harassment-and-sexual-misconduct/>

Olweus, D. (2013). School bullying: Development and some important challenges. *Annual Review of Clinical Psychology, 9,* 751–780. doi: 10.1146/annurev-clinpsy-050212-185516

Paullet, K. L., Rota, D. R., & Swan, T. T. (2009). Cyberstalking: An exploratory study of students at a mid-Atlantic university. *Issues in Information Systems, 10*, 640–49.

Penney, J. (2018). Can cyber harassment laws encourage online speech? In U. Gasser, R. Faris, A. Ashar & N. Bourassa (eds.), *Perspectives on harmful speech online*. Berkman Klein Research Publication 2017-98, Harvard University

Pew Research Center (2017). Online Harassment 2017. Available at: <https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/>

Phippen, A., & Bond, E. (2020). Online Harassment and Hate Crime in HEIs – Report from FOI. Retrieved January 30 2020 from: <https://www.uos.ac.uk/sites/www.uos.ac.uk/files/FOI-Report-Final-Jan-2020-rgb_0.pdf>

Pina, A., Gannon, T. A., & Saunders, B. (2009). An overview of the literature on sexual harassment: Perpetrator, theory and treatment issues. *Aggression and Violent Behavior 14*(2). 126-138.

Pina, A., Holland, J. E., & James, M. (2017). The malevolent side of revenge porn proclivity: Dark personality traits and sexist ideology. *International Journal of Technoethics, 8*(1), 30-43.

Powell, A., & Henry, N. (2016). Technology-facilitated sexual violence victimization: Results from an online survey of Australian adults. *Journal of Interpersonal Violence,34*(17), 3637-3665.

Powell, A., & Henry, N. (2017). *Sexual violence in a digital age*. London: Palgrave Mcmillan. ISBN 978-1-137-58046-7.

Powell, A., Henry. N., & Flynn, A. (2018). Image-based sexual abuse, in WS DeKeseredy & M Dragiewicz (eds), *Handbook of critical criminology*. New York: Routledge

Powell, A., Henry, N., Flynn, A., & Scott, A. J. (2019). Image-based sexual abuse: The extent, nature, and predictors of perpetration in a community sample of Australian residents. Computers in Human Behavior, *92*, 393-402.

Robertson, C. A., & Knight, R. A. (2014). Relating sexual sadism and psychopathy to one another, non-sexual violence and sexual crime behaviors. *Aggressive Behavior 40*(1), 12-23.

Rotundo, M., Nguyen D-H., & Sackett, P. R. (2001). A meta-analytic review of gender differences in perceptions of sexual harassment. *Journal of Applied Psychology, 86*(5), 914-922

Sadagopan, S. M. (2019). Feedback loops and echo chambers: How algorithms amplify viewpoints. *The Conversation*. Available at: <https://theconversation.com/feedback-loops-and-echo-chambers-how-algorithms-amplify-viewpoints-107935>

Scheller, S. H. (2015). A picture is worth a thousand words: The legal implications of revenge porn. *North Carolina Law Review, 93*(2), 551.

Scott, G. G., Wiencierz, S., & Hand, C. J. (2019). The volume and source of cyberabuse influences victim blame and perceptions of attractiveness. *Computers in Human Behavior, 92*, 119-127.

Sheridan, L., & Grant, T. (2007). Is cyberstalking different? *Psychology, Crime & Law, 13,* 627-640

Snyder, P., Doerfler, P., Kanich, C., & McCoy, D. (2017). Fifteen minutes of unwanted fame: Detecting and characterizing doxing. In IMC 2017 - Proceedings of the 2017 Internet Measurement Conference (Vol. Part F131937, pp. 432-444). Association for Computing Machinery.

Spielhoffer, T. (2010). Children’s online risks and safety. A review of the available evidence. Slough: National Foundation for Educational Research (NFER). Available at: <https://www.nfer.ac.uk/publications/COJ01/COJ01.pdf>

Statista (2019). Mobile phone usage in the United Kingdom (UK) 2005-2018). Available at: <https://www.statista.com/statistics/300378/mobile-phone-usage-in-the-uk/>

Statista (2019). Global number of internet users 2005-2019. Available at: <https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/>

Staude-Müller, F., Hansen, B. & Voss, M. (2012) ‘How stressful is online victimization? Effects of victim’s personality and properties of the incident’. *European Journal of Developmental Psychology, 9*(2), 260-274.

Strawhun, J., Adams, N. & Huss, M. (2013). The assessment of cyberstalking: An expanded examination including social networking, attachment, jealousy, and anger in relation to violence and abuse. *Violence and Victims, 28*, 715–730.

Strickland, P., & Dent, J. (2017). Online harassment and cyberbullying. House of Commons Library Briefing Paper. Available at: <https://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-7967#fullreport>

Uhl, C. A., Rhyner, K. J., Terrance, C. A., & Lugo, N. R. (2018). An examination of nonconsensual pornography websites. *Feminism & Psychology, 28*(1), 50-68.

Universities UK (2019). Changing the Culture: Tackling online harassment and promoting online welfare. London: UUK Available at: <https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2019/tackling-online-harassment.pdf>

Universities UK (2016). Changing the Culture: Report of the Universities UK Taskforce examining violence against women, harassment and hate crime affecting university students. London: UUK Available at: <https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2016/changing-the-culture.pdf>

Walker, K., & Sleath, E. (2017). A systematic review of the current knowledge regarding revenge pornography and non-consensual sharing of sexually explicit media. Aggression and Violent Behavior, 36, 9–24.

Willard, N. E. (2007). *Cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats and distress*. Champaign IL: Research Press; ISBN 978-0878225378

Ybarra, M. L., & Mitchell, K. J. (2004). Youth engaging in online harassment: Associations with caregiver-child relationships, internet use, and personal characteristics. *Journal of Adolescence, 27*, 319-336.

YouGov (2017). Fifty three percent of millennial women have received a naked photo from men. Available at: <https://today.yougov.com/topics/lifestyle/articles-reports/2017/10/09/53-millennial-women-have-received-dick-pic>