International Centre
FOR MISSING & EXPLOITED CHILDREN

Studies in Child Protection:

Sexual Extortion and Nonconsensual Pornography

October 2018

The Koons Family Institute
on International Law & Policy

ICMEC.org
Building a Safer World for Children

Studies in Child Protection:

Sexual Extortion and Nonconsensual Pornography

About Us

The International Centre for Missing & Exploited Children (ICMEC) works around the world to advance child protection and safeguard children from abduction, sexual abuse and exploitation. Headquartered in Alexandria, Virginia, U.S.A., ICMEC also has regional representation in Brazil and Singapore. Together with an extensive network of public and private sector partners, ICMEC's team responds to global issues with tailored local solutions.

The Koons Family Institute on International Law & Policy (The Koons Family Institute) is ICMEC's in-house research arm. The Koons Family Institute combats child abduction, sexual abuse and exploitation on multiple fronts by conducting and commissioning original research into the status of child protection laws around the world, creating replicable legal tools, promoting best practices, building international coalitions, bringing together great thinkers and opinion leaders, and collaborating with partners in the field to identify and measure threats to children and ways ICMEC can advocate change.

Our Mission

For nearly 20 years, ICMEC has been identifying gaps in the global community's ability to properly protect children from abduction, sexual abuse and exploitation, and expertly assembling the people, resources, and tools needed to fill those gaps.

ICMEC works every single day to make the world safer for children by eradicating child abduction, sexual abuse and exploitation. We focus on programs that have an impact on addressing these complex issues, and we offer support to governments, policymakers, law enforcement, prosecutors, industry, civil society, and many others across the globe.

We ADVOCATE **for children around the world** by proposing changes to laws, treaties, and systems based on rigorous research and the latest technology.

We TRAIN **partners on the front lines** by providing tools to professionals who interface with children to improve prevention, facilitate treatment for victims, and increase the efficacy of the identification and prosecution of people who victimize children.

We COLLABORATE **with key stakeholders** by building international networks of professionals across disciplines to anticipate issues, identify gaps, and develop crosscutting solutions.

Table of Contents

Acknowledgements

We would like to thank the following organizations and individuals for their assistance and guidance with researching sexual extortion and nonconsensual pornography in relation to child protection:

- The invaluable legal research interns who compiled the research for this report: Jordan Aebli, Spencer Beall, Andy Carr, Gemma Forest, Matt Hensch, and Julia Navarro;
- Stacy L. Comp, Attorney, who served as a peer reviewer and provided expert input and advice;
- Our donors, without whom our work would not be possible.

Introduction

The rapid evolution of technology and the increasingly widespread use of the Internet, have changed the face of child sexual exploitation globally.[1] Child sexual exploitation includes, but is not limited to: enticing, manipulating, or threatening a child into performing sexual acts in front of a webcam; grooming children online with the goal of sexually exploiting them; and distributing child sexual abuse material online.[2] Sex offenders have become proficient in using technology to engage in child sexual abuse by utilizing the Internet as a vehicle to meet children in order to prepare them for sexual encounters, or even to target, manipulate, and lure them into sex trafficking.[3] While the vulnerability of children to sexual predators is not new, the tools predators use and the language to describe various types of online child sexual abuse have changed remarkably.[4] Two forms of online child sexual exploitation have emerged as pervasive threats to children's safety around the world: sexual extortion, commonly referred to as "sextortion,"[5] and nonconsensual pornography or nonconsensual sharing of intimate images, also often referred to as "revenge pornography."[6,7]

Sexual extortion is the process through which one person is blackmailed by another "to extort sexual favors, money, or other benefits" under the threat of sharing the victim's intimate images, videos, or other sexualized media without their consent.[8] If the victim fails to provide the requested sexual favors, additional intimate images, money, or other benefits, their images may be posted online for the purpose of causing humiliation or distress, or coercing the individual into generating additional sexually explicit material.[9] The perpetrator may be motivated either by sexual gratification or financial gain.[10] While frequently discussed in relation to adult victims, children are equally as vulnerable to victimization through sexual extortion.[11]

Today, the term "sextortion" is widely used to refer to coercive or blackmail-based abuses. However, at the time of its conception a decade ago, it was introduced by the International Association of Women Judges (IAWJ) as "corruption involving sexual exploitation" and was initially defined much more broadly.[12] The IAWJ is credited with coining the term in different contexts, ranging "from government officials granting permits in exchange for sexual favors, to teachers and employers trading good grades

---

1 *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*, Interagency Working Group on Sexual Exploitation of Children, Luxembourg, Jan. 28, 2016, D.4.iii, 27-28, *at* http://luxembourgguidelines.org/english-version/ (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

2 *Id.*

3 U.S. Department of Justice, *The National Strategy for Child Exploitation Prevention and Interdiction: A Report to Congress – April 2016* 74-76, *at* https://www.justice.gov/psc/file/842411/download (last visited Oct. 7, 2018) (on file with the International Centre for Missing & Exploited Children).

4 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, *supra* note 1, *at* 23.

5 The terms "sexual extortion" and "sextortion" are used interchangeably throughout this report.

6 The terms "nonconsensual pornography" and "revenge pornography" are used interchangeably throughout this report.

7 It should be noted that while discussing sexual extortion and nonconsensual pornography, minors are too young to consider the consequences of sharing personal images online, even if they intended to do so, and therefore it should be understood that a child cannot consent to any of the abovementioned acts. See, World Health Organization, *Guidelines for medico-legal care for victims of sexual violence – Definition of Child Sexual Abuse, at* http://www.who.int/violence_injury_prevention/resources/publications/en/guidelines_chap7.pdf (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

8 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, *supra* note 1, *at* 52.

9 *Id.*

10 Europol, European Cybercrime Centre, *Online sexual coercion and extortion as a form of crime affecting children: Law Enforcement Perspective* 15, May 2017, *at* https://www.europol.europa.eu/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

11 *Id.*

12 Thomson Reuters Foundation, International Association of Women Judges, and Marval O'Farrell Mairal, *Combating Sextortion: A Comparative Study of Laws to Prosecute Corruption Involving Sexual Exploitation* 9, 2015, *at* http://www.trust.org/contentAsset/raw-data/588013e6-2f99-4d54-8dd8-9a65ae2e0802/file (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

and career opportunities for sex with students and employees."[13] The IAWJ subsequently selected the term "sextortion" to reflect both the corruption and the sexual elements of the acts committed.[14]

Sextortion increasingly targets children in the digital realm, as minors use the Internet and social media more extensively, thereby allowing the creation and sharing, or theft, of intimate images to occur more easily. Moreover, as increasingly younger children have access to the Internet and related technologies, a wider age range of children are susceptible to online sexual exploitation.[15] According to a 2015 survey of 2,290 parents in the United States, 96% responded that their child had a mobile phone; the average age at which a child in the United States receives their first mobile phone is age six.[16] In that same survey, parents responded that 75% had purchased Internet-accessible tablets for their child and 71% had purchased a handheld gaming console.[17] A survey conducted in Singapore showed that, in 2015, 79.8% of children ages 0-14 had accessed the Internet and on average started going online at age six.[18] The study further showed that 86.1% of children used smartphones to access the Internet, while 78.3% used a tablet and 74.5% used a handheld gaming device.[19] Similarly, a 2016 German survey of 1,229 children ages 6-13 years found that 51% had a smartphone or mobile phone and nearly half had a portable gaming console.[20] Additionally, in a 2017 UK survey, 49% of children between the ages of 5-15 reported having a mobile phone, 46% had a smartphone, and 49% had a tablet.[21]

As access to the Internet has increased, so has the proliferation of social media sites and applications. The plethora of social media sites available today provides offenders with easy access to children. According to the 2015 Singapore survey mentioned above, 65% of children ages 0-14 use social media.[22] In the United Kingdom in 2017, 24% of children ages 8-11 and 75% of children ages 12-15 had a social media profile.[23] This increased use of social media by minors mirrors a correlating increase in social media manipulation by offenders. A report by the Brookings Institution found that this manipulation is "[b]y far the most common feature of sextortion cases" and entails the perpetrator tricking the victim into sending compromising images that can then be used to extort the victim.[24] This type of manipulation was found in 91% of cases involving minor victims reviewed in the report.[25] !

One particularly chilling example of sexual extortion is the case of a 32-year old hacker, Luis Mijangos, who developed malware[26] to retrieve sexual photos and videos from his female victims, many of whom

---

13 *Id.* at 13-14

14 *Id.* at 14.

15 Iain Ramage, *String of extortion threats over naked pictures in the north of Scotland*, THE PRESS & JOURNAL, Oct. 3, 2016, *at* https://www.pressandjournal.co.uk/fp/news/highlands/1044597/vigilance-call-over-web-abuse/ (last visited Oct. 8, 2018).

16 *Study Finds Average Age of Kids When They Get First Cell Phone Is Six*, ABC 13 EYEWITNESS NEWS, Apr. 7, 2015. *at* http://abc13.com/technology/study-53%-of-kids-get-a-cell-phone-at-age-6/636328/ (last visited Oct. 8, 2018).

17 *Id*.

18 Media Development Authority Singapore, *MDA Zero-to-Fourteen Consumer Experience Study 2015*, *at* https://www.imda.gov.sg/-/media/imda/files/industry-development/fact-and-figures/for-public-release-cs-2015-final.pdf?la=en (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

19 *Id*.

20 *KIM study 2016 - Childhood, internet, media: Basic study on the media handling of 6- to 13-year-olds in Germany,* Media Education Research Association Southwest, *at* https://www.mpfs.de/fileadmin/files/Studien/KIM/2016/KIM_2016_Web-PDF.pdf (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

21 *Children and parents: media use and attitudes report* 42, Nov. 2017, Ofcom, *at* https://www.ofcom.org.uk/__data/assets/pdf_file/0020/108182/children-parents-media-use-attitudes-2017.pdf (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

22 Media Development Authority Singapore, *supra* note 18.

23 Children and parents: media use and attitudes report, *supra* note 21, at 101.

24 Benjamin Wittes, Cody Poplin, et al., *Sextortion: Cybersecurity, teenagers, and remote sexual assault (Report)* 12, Brookings Institution, May 11, 2016, *at* https://www.brookings.edu/wp-content/uploads/2016/05/sextortion1-1.pdf (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

25 *Id.*

26 Offenders may deploy malware to hack into a victim's computer system to steal existing – and capture new – intimate photos or videos. Malware is defined as software which is specifically designed to disrupt, damage, or gain authorized access to a computer system. See, Oxford English Dictionary, *Malware*, *at* https://en.oxforddictionaries.com/definition/malware (last visited Sep. 13, 2018).

were minors.[27] The malware allowed Mijangos to access all content on victims' computers, record his victims' keystrokes, and turn on the computers' web cameras to catch the victims in intimate moments.[28] When Mijangos was arrested in 2010, federal investigators discovered thousands of webcam video captures, audio recordings, and screen captures related to approximately 230 victims, 44 of whom were minors.[29]

Nonconsensual pornography, also referred to as "nonconsensual sharing of intimate images" or "revenge pornography," is the distribution of sexually explicit materials without consent of one or more of the individuals involved.[30] It is considered by some to be a form of cyber-harassment (e.g., "when a perpetrator uses the Internet to annoy, embarrass, or emotionally distress another individual").[31] The explicit images or videos are most often shared publicly in order to embarrass or humiliate the victim, although "not all perpetrators are motivated by vengeance" as some are, instead, financially motivated.[32]

Nonconsensual pornography shares some characteristics of sextortion – sharing or threatening to share intimate materials for personal gain – but should be distinguished from sextortion's pecuniary or sexual gratification aims. While sextortion is "dependent on secrecy," nonconsensual pornography "derive[s its] effectiveness from public damage to the victim's reputation." [33] Nonconsensual pornography is "generally a crime of distribution or publication, not of creation or production in the first instance."[34] The focus is on the disclosure of an intimate image that already exists. Sextortion, on the other hand, "consists of both the issuance of an extortionate threat in order to compel someone to produce pornography – whether or not that person actually complies – and, separately, of the compulsion of an act of sex or nudity by means of such a threat" and does not require the material be released.[35]

Children as young as age 11 have been targeted and victimized in cases of nonconsensual pornography, with UK law enforcement working as many as five cases each week involving images of minors that have been shared online without consent.[36] This number is likely underestimated due to the victims' embarrassment or fear of reporting incidents to the authorities.[37]

According to a British Broadcasting Corporation (BBC) investigation, there were 1,160 reported incidents of revenge pornography in England and Wales from April-December 2015.[38] Three of those victims were 11 years old, with around 30% of offenses involving young people under the age of 19.[39] While approximately 4% of all Internet users in the United States "have … had sensitive images posted

---

27 Benjamin Wittes, et al., *supra* note 24, at 2.
28 *Id.*
29 *Id.*
30 Danielle K. Citron and Mary A. Franks, *Criminalizing Revenge Porn* 346, 49 WAKE FOREST LAW REVIEW 345 (2014) (on file with the International Centre for Missing & Exploited Children).
31 Mudasir Kamal, MD & William J Newman, MD, *Revenge Pornography: Mental Health Implications and Related Legislation,* J AM ACAD PSYCHIATRY LAW 44:359 – 67, 359 & 361, 2016, *at* http://jaapl.org/content/44/3/359 (last visited Sep. 8, 2018).
32 *Id.* at 361.
33 Jedidiah Bracy, *Why 'sextortion' is part of a larger privacy and cybersecurity issue*, IAPP, May 13, 2016, *at* https://iapp.org/news/a/why-sextortion-is-part-of-a-larger-privacy-and-cybersecurity-issue/ (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).
34 Benjamin Wittes, Cody Poplin, et al., *Closing the Sextortion Sentencing Gap: A Legislative Proposal* 7, Center for Technology Innovation at Brookings, May 2016, *at* https://www.brookings.edu/wp-content/uploads/2016/05/sextortion2.pdf (last visited Oct. 8, 2018).
35 *Id.*
36 Will Worley, *Revenge Porn: Hundreds of Images of Children Shared on Facebook and Instagram*, THE INDEPENDENT (UK), Jan. 24, 2016, *at* http://www.independent.co.uk/news/uk/home-news/revenge-porn-hundreds-of-images-of-children-shared-on-facebook-and-instagram-a6830736.html (last visited Oct. 2, 2018).
37 *Id.*
38 Peter Sherlock, *Revenge Pornography Victims as Young as 11, Investigation Finds,* BRITISH BROADCASTING CORPORATION (BBC), Apr. 27, 2016, *at* https://www.bbc.com/news/uk-england-36054273 (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).
39 *Id.*

without their permission [online] or had someone threaten" to do so, approximately one in 14 (7%) of users under age 30 reported experiencing some form of threatened or actualized revenge pornography. One in 10 young women under the age of 30 experienced these threats – a higher rate than for older women and men of any age.[40]

Addressing sextortion and nonconsensual pornography presents unique challenges. Often times such offenses are transnational and occur across multiple countries and jurisdictions, posing investigative challenges for law enforcement.[41] Governments may not keep data on such offenses, which makes it difficult to speak to the scope of the problem and the number of prosecutions.[42] There may be no consistency as to the legal grounds of prosecution; in the United States, for example, sextortion cases may be prosecuted as child sexual abuse material, hacking, extortion, stalking, or a variety of lesser offenses; some cases may be prosecuted under federal law while others may be prosecuted under state law, which generally impose lighter punishment.[43]

There is a general lack of awareness of the harm caused to child victims when intimate imagery is circulated,[44] which can have long-term and serious mental health implications.[45] Often times victims must cope with the consequences well into their adult lives.[46] The distress that one is likely to face includes depression-like symptoms such as low self-esteem, withdrawal, worthlessness, anger, guilt, and even suicide.[47] Victims of nonconsensual pornography often face humiliation, shame, and may even face more tangible consequences such as being kicked out of their home or having increased difficulty gaining future employment.[48]

Nonconsensual pornography also poses a challenge to technology companies attempting to remove images of child sexual abuse and exploitation from their platforms, as it can be difficult to identify and requires significant manpower to review flagged content.[49]

The purpose of this paper is to define and analyze sexual extortion and nonconsensual pornography as they impact children, as well as to better understand obstacles to prevention, policy intervention, and prosecution. This paper, framed with a global perspective, also presents effective, model legislative responses and highlights global efforts that are readily adaptable by individual countries to combat the growing number of cases of children who are exploited via sexual extortion and the nonconsensual sharing of intimate images.

---

40 Amanda Lenhart, Michele Ybarra, and Myeshia Price-Feeney, *Nonconsensual Image Sharing: One in 25 Americans Has Been a Victim of "Revenge Porn"* 5, Dec. 13, 2016, DATA & SOCIETY RESEARCH INSTITUTE (on file with the International Centre for Missing & Exploited Children).

41 *Revenge porn is just one part of a changing picture of harassment*, The Conversation, Jul. 8, 2015, *at* https://theconversation.com/revenge-porn-is-just-one-part-of-a-changing-picture-of-harassment-43703 (last visited Aug. 27, 2018).

42 *See e.g.,* Benjamin Wittes, Cody Poplin, et al., *Sextortion: The Problem and Solutions,* LAWFARE, May 11, 2016, *at* https://www.lawfareblog.com/sextortion-problem-and-solutions (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

43 *Id.*

44 Mudasir Kamal, MD & William J Newman, MD, *supra* note 31.

45 *Id.*

46 *Id.; See,* Janis Wolak and David Finkelhor. *Sextortion: Findings from a Survey of 1,631 Victims*, 78, Jun. 2016, University of New Hampshire (CCRC), *at* http://www.unh.edu/ccrc/pdf/Sextortion_RPT_FNL_rev0803.pdf (last visited Oct. 4, 2018) (on file with the International Centre for Missing & Exploited Children). *See also,* Sameer Hinduja, *Sextortion*, Cyberbullying Research Center, Jun. 28, 2016, *at* https://cyberbullying.org/sextortion (last visited Oct. 4, 2018).

47 *Id.*

48 *Id.*

49 Charlotte Alter, *'It's Like Having an Incurable Disease': Inside the Fight Against Revenge Porn*, Jun. 13, 2017, TIME, http://time.com/4811561/revenge-porn/ (last visited Oct. 4, 2018) (on file with the International Centre for Missing & Exploited Children).

The report is further intended to support and promote the United Nations Sustainable Development Goals (SDGs), in particular SDG 16.2[50] on ending the abuse, exploitation, trafficking, and all forms of violence against and torture of children, and contribute to reaching the goals of the 2030 Agenda for Sustainable Development [51] by demonstrating our organizational commitment, helping raise awareness of the issues, and promoting the rule of law at the national and international levels. Additionally, the report contributes to the Implementation and Enforcement of Laws strategy, the first of the seven INSPIRE strategies developed by the World Health Organization (WHO), in particular core indicators 3.1 through 3.6 (i.e., laws and policies, awareness of laws, review of legal and policy framework)[52]; and helps to implement the WePROTECT Global Alliance to End Child Sexual Exploitation Online Model National Response (MNR) – specifically capabilities 2 (Research, Analysis and Monitoring) and 3 (Legislation) under Policy and Governance[53].

[50] UN Sustainable Development Goals, *Goal 16: Peace, Justice and Strong Institutions, at* https://www.un.org/sustainabledevelopment/peace-justice/ (last visited Sep. 30, 2018).

[51] Resolution adopted by the General Assembly on 25 September 2015 [without reference to a Main Committee (A/70/L.1)] 70/1. *Transforming our world: the 2030 Agenda for Sustainable Development,* Oct. 2015, *at* http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E (last visited Sep. 30, 2018).

[52] World Health Organization (WHO), *INSPIRE: Seven Strategies for Ending Violence Against Children*, 2016, *at* http://www.who.int/violence_injury_prevention/violence/inspire/en/ (last visited Oct. 26, 2018) (on file with the International Centre for Missing & Exploited Children).

[53] WePROTECT Global Alliance, *Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response*, *at* https://www.weprotect.org/the-model-national-response/ (last visited Oct. 26, 2018) (on file with the International Centre for Missing & Exploited Children).

Sexual Extortion

Sexual extortion (sextortion; also referred to as online sexual coercion and extortion[54]) involving a child is an emerging form of online child sexual exploitation.[55] The offender (a "sextortionist") blackmails[56] or coerces the victim to produce and provide sexually exploitative images and/or videos, sexual favors, money, and other benefits under the threat of the victim's intimate images, videos, and other media being shared with their family, friends, and others.[57] Sextortion has been referred to as "virtual sexual assault" because of the similar emotional and psychological effects on victims.[58] Sextortion is committed primarily online, and with the rise of the Internet and related information and communications technologies (ICTs), the risk of victimization has increased.[59] As explained in a Brookings Institution report, "[f]or the first time in the history of the world, the global connectivity of the Internet means that you don't have to be in the same country as someone to sexually menace that person."[60] The U.S. Department of State's 2017 Trafficking in Persons Report noted the role of increased technology access in the sexual exploitation of children, and cited sextortion as a growing threat to children, thus demonstrating growing global recognition of this issue.[61]

Sextortion offenses can be committed against individuals of any age, but children are particularly vulnerable. According to the 2016 U.S. Department of Justice's National Strategy for Child Exploitation Prevention and Interdiction report, sextortion "is by far the most significantly growing threat to children."[62] The report indicated that sextortion cases often have "more minor victims per offender than all other child sexual exploitation offenses" as offenders commonly communicate with hundreds of potential victims at one time.[63] In addition, according to a 2015 U.S. Federal Bureau of Investigation (FBI) analysis of 43 sextortion cases, "at least 28%…had at least one victim who committed or attempted suicide."[64] Since the U.S.-based National Center for Missing & Exploited Children (NCMEC) began tracking sextortion in 2013, it has experienced a dramatic increase in the number of reports made to its CyberTipline, with reports up 150% from 2014 to 2016.[65]

In one highly-publicized sextortion case, the 2012 suicide of Amanda Todd, a Canadian teenager from British Columbia, captivated the media, brought attention to the issue of sextortion of children, and emphasized the importance of addressing sextortion and cyberbullying.[66] Amanda, aged 15, sent an intimate image to an online acquaintance, with whom she had been communicating for about a year

---

54 Europol, *supra* note 10.

55 National Center for Missing and Exploited Children (NCMEC), *Sextortion*, *at* http://www.missingkids.com/theissues/onlineexploitation/sextortion (last visited Oct. 7, 2018) (on file with the International Centre for Missing & Exploited Children).

56 The National Crime Agency (NCA) of the United Kingdom also refers to sexual extortion as webcam blackmail. *See generally*, National Crime Agency, *Sextortion (webcam blackmail), at* http://www.nationalcrimeagency.gov.uk/crime-threats/kidnap-and-extortion/sextortion (last visited Oct. 7, 2018).

57 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, *supra* note 1, *at* 52.

58 Benjamin Wittes, et al., *supra* note 24, at 2.

59 Josh Saul, *Online 'Sextortion' Is on the Rise*, NEWSWEEK, Dec. 1, 2016, *at* http://www.newsweek.com/2016/12/09/sextortion-social-media-hacking-blackmail-527201.html (last visited Sep. 13, 2018) (on file with the International Centre for Missing & Exploited Children).

60 *Id.*

61 U.S. Department of State, *2017 Trafficking in Persons Report* 32, *at* https://www.state.gov/documents/organization/271340.pdf (last visited Oct. 7, 2018) (on file with the International Centre for Missing & Exploited Children).

62 U.S. Department of Justice, *supra* note 3, at 75.

63 *Id*.

64 Benjamin Wittes, Cody Poplin, et al., *supra* note 42.

65 National Center for Missing and Exploited Children, *supra* note 55.

66 Rohan Smith, *New research sheds light on tragic, public suicide of sextortion victim Amanda Todd*, NEWS.COM.AU, May 14, 2016, *at* http://www.news.com.au/lifestyle/real-life/new-research-sheds-light-on-tragic-public-suicide-of-sextortion-victim-amanda-todd/news-story/d1ea63aa8e744c868212c72479daced9 (last visited Oct. 7, 2018) (on file with the International Centre for Missing & Exploited Children).

– and who then threatened to share the image with Amanda's social media connections if she did not provide additional sexually explicit material.[67] The image was eventually shared online and Amanda committed suicide following the resultant distress.[68]

Aydin Coban, a 35-year-old man from the Netherlands, was arrested in January 2014 for online harassment of numerous victims. Investigators found Coban's actions ultimately led to the victimization of 39 individuals from six countries, one of whom was Amanda Todd. In 2017, he was found guilty of 72 charges – including child sexual abuse materials and attempted sexual assault of multiple girls, and one count of webcam blackmail – and was sentenced to 11 years in prison. The Dutch Government approved his extradition to Canada in April 2017 for his alleged exploitation of Todd.

Source: Yvette Brend, *Amanda Todd's mom 'numb' to news that Aydin Coban may be extradited,* Jun. 28, 2016, CBC NEWS, *at* https://www.cbc.ca/news/canada/british-columbia/amanda-todd-carol-cyberbully-the-netherlands-extradite-1.3656004; *See also, Dutch man charged in Amanda Todd case allegedly targeted 2nd Canadian child*, Jan. 25, 2017, CBC NEWS, *at* http://www.cbc.ca/news/canada/british-columbia/amanda-todd-aydin-coban-1.3951334; *Dutch court clears extradition of Amanda Todd's alleged cyber extortionist*, Apr. 4, 2017, CBC NEWS, *at* http://www.cbc.ca/news/canada/british-columbia/amanda-todd-aydin-coban-extradition-1.4054283 (last visited Oct. 8, 2018).

Child victims of sextortion are typically between 10-17 years of age, but victims as young as nine have been documented.[69] Increasingly, cases are arising in which the offender manipulates one child into abusing younger siblings or friends.[70] Both male and female children can fall victim to sextortion; NCMEC's study found that 78% of reports involved girls and 15% involved boys ranging from ages 8-17 years.[71] In an analysis of 78 sextortion cases conducted by the Center for Technology Innovation at the Brookings Institution, 71% of the cases were found to involve a victim under the age of 18.[72] Sextortion of children is believed to be underreported; thus, the true number of children who are victimized is unknown.[73]

Sextortionists can be adults or other young people; they may or may not know the victim.[74] Several studies have shown that sextortionists typically are male.[75] Individuals may be targeted through social media sites, dating sites, or other similar platforms.[76] Sextortion also is committed by organized criminal networks that operate "out of business-like locations similar to call centres," often targeting hundreds of individuals simultaneously to increase the chances of finding a victim.[77] Reportedly, girls and boys as young as 14 have been victimized by these organized gangs, many of which operate from overseas locations.[78]

---

67 *B.C. girl's suicide foreshadowed by video*, CBC NEWS, Oct. 11, 2012, *at* http://www.cbc.ca/news/canada/british-columbia/b-c-girl-s-suicide-foreshadowed-by-video-1.1217831 (last visited Oct. 7, 2018) (on file with the International Centre for Missing & Exploited Children).

68 *Aydin C. Trial: Accused in Amanda Todd Cyberbullying Case Gets 11 Years in Dutch Prison*, HUFFINGTON POST (Canada), Mar. 16, 2017, *at* http://www.huffingtonpost.ca/2017/03/16/aydin-c-trial_n_15403720.html (last visited Oct. 7, 2018) (on file with the International Centre for Missing & Exploited Children).

69 Josh Saul, *supra* note 59. *See also,* U.S. Department of Justice, *supra* note 3, at 75.

70 Shelley Lynch – Public Affairs Specialist, *Sextortion Affecting Thousands of U.S. Children,* FBI.gov, Jun. 20, 2016, *at* https://www.fbi.gov/contact-us/field-offices/charlotte/news/press-releases/sextortion-affecting-thousands-of-u-s-children (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

71 National Center for Missing and Exploited Children, *supra* note 55.

72 Benjamin Wittes, et al., *supra* note 24, at 12.

73 Janis Wolak and David Finkelhor, *supra* note 46, at 43.

74 *Id*.

75 Benjamin Wittes, et al., *supra* note 24, at 12. *See also,* Janis Wolak and David Finkelhor, *supra* note 46, at 12.

76 INTERPOL, *Online Safety – Sextortion*, *at* https://www.interpol.int/Crime-areas/Cybercrime/Online-safety/Sextortion (last visited Oct. 8, 2018).

77 *Id. See also, Philippines dismantles 'sextortion' groups, arrests 58 people*, REUTERS, May 2, 2014, *at* http://www.reuters.com/article/us-philippines-crime-idUSBREA4105520140502 (last visited Oct. 3, 2018).

78 Lizzie Dearden, *Five British men have killed themselves after falling victim to online 'sextortion' police reveal*, THE INDEPENDENT, May 4, 2018, *at* https://www.independent.co.uk/news/uk/crime/blackmail-online-sextortion-suicides-videos-photos-sexual-police-advice-a8337016.html (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

According to NCMEC, 39% of the 1,428 sextortion cases reported to the CyberTipline from October 2013-April 2016 captured the length of time between the offender obtaining the sexually explicit materials/content and the moment the victim was blackmailed with that material.[79] In 80% of those cases, it appeared that the blackmailing occurred on the same day the content was received.[80] A prolonged period of time between the events, sometimes years, was noted in 20% of the cases.[81]

Offenders use a variety of platforms to gain access to and communicate with children online. One study showed that 54% of sextortion cases analyzed began on social networking sites, 41% on messaging and photo apps, 23% on video voice calling apps, 9% on dating apps, and 4% on gaming platforms.[82] Increased use of web cameras and camera-enabled mobile devices has led to a rise in live-streaming child sexual exploitation online.[83] Video chat allows offenders to engage in virtual "face-to-face" online interaction, which strengthens their influence over a victim.[84]

A 14-year-old victim of sexual exploitation explains how she was coerced into providing intimate materials and then eventually stood up to her exploiter: "He told me if I didn't send him [pictures] he would damage my social life and personal life. He also said how he found out all my information from searching me. I got scared so I did what he asked, but every time I got brave enough to say no and tell him off he would threaten me worse. I don't know what happened but after the last time he threatened me I just told him off and ignored the rest of his messages. He kept trying to get me to talk to him...and then I had to block him and just hope for the best."

Source: Janis Wolak and David Finkelhor, *supra* note 46.

Manipulation and coercion are core principles of sexual extortion.[85] Sextortion "'is designed to be secretive' and to 'enslave the victim'," with the threat of exposure allowing the perpetrator to maintain control over the victim.[86] Offenders most often exploit children by threatening to post previously acquired sexual material on the Internet, or otherwise threatening to share intimate material with the child's family, friends, and social contacts.[87] Offenders may acquire such material through various tactics including grooming, direct communication, hacking, or other methods.[88]

One tactic offenders use to sexually extort their victims is to initiate/build an online relationship with the victim for the purpose of manipulating them into online or offline sexual contact, often referred to as "online grooming."[89] In an online grooming scenario, an offender develops an emotional connection with the child through "psychological manipulation that is usually very subtle, drawn out, calculated,

---

79 *Sextortion Factsheet: Trends identified in Cybertipline sextortion reports,* National Center for Missing & Exploited Children, 2016, *at* http://www.missingkids.com/content/dam/ncmec/en_us/documents/sextortionfactsheet.pdf (last visited Oct. 7, 2018) (on file with the International Centre for Missing & Exploited Children).

80 *Id.*

81 *Id.*

82 Janis Wolak and David Finkelhor, *supra* note 46.

83 U.S. Department of Justice, *supra* note 3, at 75.

84 Juliane Kloess, Catherine Hamilton-Giachritsis, and Anthony Beech, *Offense Processes of Online Sexual Grooming and Abuse of Children Via Internet Communication Platforms*, Jun. 2017, SEXUAL ABUSE: A JOURNAL OF RESEARCH AND TREATMENT (on file with the International Centre for Missing & Exploited Children). *See also,* Kemal Veli, *Sexual Extortion of Children in Cyberspace*, Dec. 2016, INTERNATIONAL JOURNAL OF CYBER CRIMINOLOGY, 10(2), *at* http://www.cybercrimejournal.com/Kemalvol10issue2IJCC2016.pdf (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

85 National Center for Missing and Exploited Children, *supra* note 55.

86 Jedidiah Bracy, *Why 'sextortion' is part of a larger privacy and cybersecurity issue*, IAPP, May 13, 2016, *at* https://iapp.org/news/a/why-sextortion-is-part-of-a-larger-privacy-and-cybersecurity-issue/ (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

87 The Sextortion Factsheet, *supra* note 79.

88 Europol, *supra* note 10.

89 "Grooming for sexual purposes" is also known interchangeably as "[online or offline] solicitation of children for sexual purposes." *See*, Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, *supra* note 1, at 51.

controlling, and premeditated," in order to lower the child's inhibitions[90] and manipulate the child into performing or permitting the desired sexual exploitation which often includes the creation of sexual images or videos.[91] Through the grooming process, an offender tries to gain the child's compliance to maintain secrecy, and to avoid detection and punishment.[92]

Online grooming often "overlap[s] with incidents of online child sexual…extortion" though the two are analytically distinct from one another.[93] While sextortion can occur without the online grooming process, in some cases online grooming may lead to sexual extortion.[94] The "influence and manipulation typical of groomers" can rapidly escalate into "threats, intimidation, and coercion once the person has been persuaded to send the first sexual images of her/himself."[95]

Lucas Michael Chansler, a 31-year-old from Florida, victimized hundreds of children in a grooming and sextortion scheme. From 2007 to early 2010, he pretended to be a friend or admirer of his victims on social networking websites. After he gained the trust of his victims, he would engage in live video chat and coerce girls into exposing themselves while he secretly recorded the acts. He would then threaten to send the video to their family and friends if they did not send more graphic images and webcam videos. He admitted to targeting girls ages 13-18 as he felt they were more likely than adult women to fall for his scheme.

When Chansler was finally arrested in January 2010, the FBI reported that he had 80,000 child sexual abuse images and videos of his victims in his possession. In his court testimony, Chansler said he targeted 350 child victims posing as a 15-year-old boy using 135 different fake screen names and personas to trick girls from 26 U.S. states, three Canadian provinces, and the United Kingdom. In November 2014, Chansler was sentenced to 105 years in federal prison.

Source: Jo Brown, *FBI searches for hundreds of teen victims in sextortion case,* WBTW NEWS 13, Jul. 7, 2015, *at* https://www.wbtw.com/news/fbi-searches-for-hundreds-of-teen-victims-in-sextortion-case/959861899; *See also*, *Sextortion and the Lucas Chansler Case*, FBI.gov, Jul. 9, 2015, *at* https://www.fbi.gov/audio-repository/news-podcasts-inside-sextortion-and-the-lucas-chansler-case.mp3/view (last visited Oct. 7, 2018).

In some cases, the offender may not actually possess any explicit images or videos of a target victim; rather they may blackmail victims for intimate images by threatening to post intimate images they do not actually possess, hoping to intimidate victims into cooperating with demands.[96] Convicted offender Richard Finkbiner used image-editing software to make his underage victims think that he had posted nude videos of them on pornography websites – even though the videos never involved the filming of his actual victims – to frighten the children into creating bona fide sexually exploitative videos for him.[97] These cases illustrate how victims, believing the offender is in possession of intimate material based solely on the offender's threats, may then give in to ever-escalating demands.

---

90 *Betrayal of Trust: Inquiry into the Handling of Child Abuse by Religious and Other Non-Government Organisations* xxxvii, Parliament of Victoria Family and Community Development Committee (2013), *at* https://www.parliament.vic.gov.au/images/stories/committees/fcdc/inquiries/57th/Child_Abuse_Inquiry/Report/Inquiry_into_Handling_of_Abuse_Volume_1_FINAL_web.pdf (last visited Sep. 13, 2018) (on file with the International Centre for Missing & Exploited Children). *See also*, Tony Krone et al., *Online child sexual exploitation offenders: A study of Australian law enforcement data*, Report to the Criminology Research Advisory Council, Jan. 2017, *at* http://crg.aic.gov.au/reports/1617/58-1213-FinalReport.pdf (last visited Sep. 13, 2018) (on file with the International Centre for Missing & Exploited Children).

91 *Grooming Cybervictims: The Psychosocial Effects of Online Exploitation for Youth* 11-13, 2003 (on file with the International Centre for Missing & Exploited Children). *See also*, Tony Krone, et al., *supra* note 90.

92 Dr. Zsuzsanna Rutai, *Online Grooming of Children: Experiences to be used in Cyprus* 7, 2013, Hope for Children UNCRC Policy Centre, *at* http://www.uncrcpc.org/assets/images/Online-Grooming-of-Children_final.pdf (last visited Sep. 13, 2018) (on file with the International Centre for Missing & Exploited Children).

93 Europol, *supra* note 10, at 10.

94 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, *supra* note 1, at 52.

95 *Id.*

96 Janis Wolak and David Finkelhor, *supra* note 46, at 13-14.

97 *United States v. Finkbiner,* Jun. 18, 2018, Government's Sentencing Memorandum, Cause No. 2:12-CR-0021-WTL-CMM. Filed 06/18/13, at 8, *at* https://www.brookings.edu/wp-content/uploads/2016/05/Finkbiner-Sentencing-Memo.pdf (last visited Oct. 8, 2018).

Along with grooming, hacking[98] also has become a powerful tool for offenders to target children online anywhere in the world, albeit less prevalent given the more sophisticated skillset required to deploy malware and other hacking methods.[99] An offender may use technology tools to gain access to a victim's social media profile photos, posts, and other non-sexual content, save the photos onto their hard drive, and threaten to digitally alter the materials to make them *appear* sexually explicit.[100] One report describes the case of a 15-year-old victim of sexual extortion whose predator altered her social media profile photo by placing her face on a naked woman's body.[101]

A 16-year-old UK boy, who goes by the pseudonym Jacob, was conned out of £800 after a hacker recorded him naked. After receiving an explicit webcam video of himself, Jacob received a phone call. As he listened to the male voice on the other end, "the guy was so aggressive on the phone. He said he was a pro hacker." Jacob recounted his story:

"He sent me a list of all my Facebook friends and said, 'I will ruin your life.' My heart was beating out of my chest. I was shaking. I remember looking at myself in my bedroom mirror thinking 'what have I done?' I went into panic mode and kept thinking about the worst case scenarios-all my friends and family and people at school seeing the video and looking at me differently. I just wanted it to stop. I asked him what he wanted. I didn't care about the money, all I could think about was trying to prevent that video getting out. I could earn all the money back but I didn't think I could get my reputation back as easily. You hear about this stuff happening but there's nothing that can prepare you for it. It felt like he was in total control."

Source: Liz Dunphy, *Brave teen's powerful warning about 'sextortion' after he was conned out of* £800 *for getting naked on webcam,* MIRROR UK, Mar. 19, 2018, *at* https://www.mirror.co.uk/news/uk-news/brave-teens-powerful-warning-sextortion-12214514 (last visited Oct. 8, 2018).

In some cases, hackers have embedded self-designed malware to extort sexually explicit photos from underage children.[102] In one U.S. case, a computer hacker's methods included "sending trojan emails and instant messages…embedded with [malware]," giving him "*complete* access to and control over" recipients' computers.[103]

After getting victims to infect their own computers with malware, hackers are able to: record intimate moments by manipulating computer cameras[104]; gain access to email accounts[105]; access personal contacts and conversations; and potentially pose as the victim's partner to encourage the victim to create sexual photos and videos for future sextortion.[106] All of the aforementioned methods may be utilized depending on the perpetrator's technological skill and goals, and all constitute sextortion – and abuse/exploitation.

Once the victim is tricked into downloading malware, the hacker has access to all of their information, including files, photos, and videos[107] that are stored on a victim's hard drive, sometimes through a

98 Hacking is defined as modifying or altering computer software and/or hardware to accomplish a goal. *See,* https://cyber.laws.com/hacking (last visited Oct. 8, 2018).

99 Jack W. Lightfoot, *Law Enforcement's Perceptions and Preparedness to Address Child Exploitation via Hacking*, Spring 2016, 37, GEORGIA SOUTHERN UNIVERSITY, Department of Criminal Justice & Criminology, *at* http://digitalcommons.georgiasouthern.edu/cgi/viewcontent.cgi?article=2500&context=etd (last visited Oct. 8, 2018).

100 Janis Wolak and David Finkelhor, *supra* note 46, at 19.

101 *Id*. at 19.

102 Mijangos's malware programs—Poison Ivy and SpyNet—were specifically designed to be undetectable by antivirus software programs. Benjamin Wittes, et al., *supra* note 24, at 2.

103 United States v. Luis Mijangos, CR No. 10-743-GHK, Jul. 19, 2011 (emphasis added), *at* https://www.brookings.edu/wp-content/uploads/2016/05/Mijangos_0.pdf (last visited Oct. 8, 2018).

104 Benjamin Wittes, et al., *supra* note 24, at 2.

105 Janis Wolak and David Finkelhor, *supra* note 46, at 19.

106 *Id*. at 22.

107 Benjamin Wittes, et al., *supra* note 24, at 2.

Remote Access Trojan (RAT) program.[108] Across Asia, RAT programs are common tools for hackers who disseminate them via popular video games, with many victims reported in Hong Kong, Malaysia, Singapore, and Taiwan.[109] These programs are especially notable for their relative ease of use and distribution, as well as their wide availability[110]; there are even tutorials and guides available online at major video-sharing websites instructing future hackers on their use.[111]

Although hackers are able to deceive people of all ages, studies show that teenage girls are targeted more often.[112] Feelings of helplessness, embarrassment, shame, and guilt often cause victims of sexual extortion to feel uncomfortable and prevent them from confiding in family, friends, or the authorities.[113]

In some cases, self-generated images that are willingly produced or produced under coercion of an offender may result in the sexual extortion of that person. "Sexting" is the "self-production of sexual images" or the "exchange of sexual messages or images."[114] "Sexting" can include both consensual sexting, "where consenting adolescents…derive pleasure from the experience," and "unwanted sexting."[115] Unwanted sexting refers to " sharing or receiving unwanted sexually explicit photos, videos, or messages, for instance by known or unknown persons trying to make contact, put pressure on, or groom the child."[116] Another example of unwanted sexting is when a child is pressured by their boyfriend or girlfriend to send a sexualized image, which is then distributed by that individual amongst their peer network.[117]

In May 2018, the UK Internet Watch Foundation (IWF) published a report looking at trends in online child sexual exploitation. This study assessed 2,082 images and videos which were publicly available online over a three-month period in 2017 and had been "recorded from a live broadcast stream; in which the child(ren) consciously interacted with a remote" third party via webcam.[118] The study found that 98% (2,037) of the images/videos portrayed children assessed to be 13 years old or younger, 28% (588) portrayed children under the age of 10.[119]

In Queensland, Australia, nearly 1,500 minors have been found guilty of child exploitation crimes in the past decade.[120] The majority of the convicted offenders engaged in sexting-based offenses, either production, distribution, or possession.[121] Of those convicted, only 28 were sentenced in court while the remaining minors were able to avoid a criminal record by participating in a diversion program.[122]

---

108 *RAT Infestation: Your Family Privacy at Risk*, Jun. 2016, Asia Digital Alliance, *at* http://www.asiadigitalalliance.com/wp-content/uploads/2016/05/ADA- RAT-infestation-Your-family-privacy-at-risk .pdf (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

109 *Id.*

110 *Id.*

111 *Id*. at 4.

112 *Id*. at 1. *See also,* Katy Murphy, *'Sextortion' – blackmail often targeting teens – will be a crime in California*, THE MERCURY NEWS, Oct. 6, 2017, *at* https://www.mercurynews.com/2017/10/06/sextortion-blackmail-often-targeting-teens-will-be-a-crime-in-california/ (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

113 Sameer Hinduja, *supra* note 46.

114 "Sexting" is the self-production of sexual images or the exchange of sexual messages or images. *See*, Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, *supra* note 1, at 44.

115 *Id.*

116 *Id.*

117 *Id.*

118 Internet Watch Foundation, *Trends in Online Child Sexual Exploitation: Examining the Distribution of Captures of Live-streamed Child Sexual Abuse* 8, 10, May 2018, *at* https://www.iwf.org.uk/sites/default/files/inline-files/Distribution%20of%20Captures%20of%20Live-streamed%20Child%20Sexual%20Abuse%20FINAL.pdf (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

119 *Id.* at 10.

120 Elle Hunt, *Sexting to Blame for Nearly 1,500 Children Convicted for Child Exploitation,* THE GUARDIAN, May 9, 2017, *at* https://www.theguardian.com/australia-news/2017/may/09/sexting-guidelines-created-by-queensland-police-as-child-convictions-soar (last visited Oct. 8, 2018). (on file with the International Centre for Missing and Exploited Children).

121 *Id*.

122 *Id*.

As a result of the significant increase in young people participating in "sexting," law enforcement in Queensland has formally adopted a policy of educating minors about the risks, instead of punishing them.[123] However, it should be noted that there is still concern in Queensland that young people will not report incidences of image-based abuse or harassment because of a fear of prosecution.[124]

While children and adolescents may willingly produce sexual images of themselves, when these images result in the exploitation of the child or the abusive use and distribution of the content, it should be noted that the child is neither responsible for nor consented to such uses.[125] Even if a child claims that they intended to have these images/videos shared online, a child lacks the maturity necessary to fully grasp the consequences of the decision. Thus, it should be understood that a child cannot consent to any of these acts as a child cannot consent to any form of sexual abuse or exploitation.[126]

Offenders also use techniques to manipulate children online by, for example, posing as a similarly-aged child in the same geographic area or simply one with similar interests, using a tailored alias.[127] This tactic is known as "catfishing,"[128] the misleading actions of a "person [i.e., the 'catfish'] who creates a fake online profile…to fraudulently seduce someone."[129] Creating such false profiles or personas is easy; offenders mask their real age, gender, or other personal details while gaining the confidence of children.[130] The use of fake profiles makes it easier to coerce and manipulate children into participating in sexualized conversations and exchanging sexual materials, including images or videos of the child victims.[131] Use of this tactic is especially ubiquitous on social media websites and messaging apps.[132] Popular social networking apps on which conversations and posted photos cannot be publicly viewed are potentially dangerous for child users as parents are left without means to monitor activity.[133]

According to a 2016 study conducted by the Brookings Institution, "catfishing" on social media sites and mobile applications accounted for nearly 91% of U.S. sextortion cases involving underage victims[134] and most often targeted children between the ages of 10-17.[135] The same study analyzed

---

123 *Id*.

124 *Id*.

125 Internet Watch Foundation, *supra* note 118.

126 *Id*. *See also,* World Health Organization, *Guidelines for Medico-Legal Care for Victims of Sexual Violence* 76, *at* http://apps.who.int/iris/bitstream/handle/10665/42788/924154628X.pdf?sequence=1 (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

127 *Sextortion: Help the FBI Locate Additional Victims of an Online Predator*, PASADENA INDEPENDENT, Jul. 2, 2015, *at* http://www.pasadenaindependent.com/news/sextortion-help-the-fbi-locate-additional-victims-of-an-online-predator/ (last visited Oct. 8, 2018). (on file with the International Centre for Missing & Exploited Children).

128 Catfish is defined by Merriam-Webster's Dictionary as a person who sets up a false personal profile on a social networking site for fraudulent or deceptive purposes. Catfish, Merriam-Webster.com, *at* https://www.merriam-webster.com/dictionary/catfish (last visited Oct. 2, 2018). *See also*, Benjamin Wittes et al., *supra* note 24, at 12.

129 Aisha Harris, *Who coined the term "catfish"?*, SLATE (Culture Blog), Jan. 18, 2013, *at* http://www.slate.com/blogs/browbeat/2013/01/18/catfish_meaning_and_definition_term_for_online_hoaxes_has_a_surprisingly.html (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

130 Child Crime Prevention & Safety Center, *Children and Grooming/Online Predators, at* https://childsafety.losangelescriminallawyer.pro/children-and-grooming-online-predators.html (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

131 Shelley Lynch, *supra* note 70.

132 Janis Wolak and David Finkelhor, *supra* note 46, at 15.

133 Cosima Marriner, *Police warning on social media messaging app, Kik*, THE SYDNEY MORNING HERALD, Dec. 1, 2013, *at* http://www.smh.com.au/national/police-warning-on-social-media-messaging-app-kik-20131130-2yimo.html (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children). *See also,* Thomas Fox-Brewster, *This $1 Billion App Can't 'Kik" Its Huge Child Exploitation Problem,* FORBES, Aug. 3, 2017, *at* https://www.forbes.com/sites/thomasbrewster/2017/08/03/kik-has-a-massive-child-abuse-problem/#4ad9f95a1a14 (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

134 Benjamin Wittes et al., *supra* note 24, at 12.

135 Donna St. George, *As online 'sextortion' against children grows, feds urge back-to-school awareness*, THE WASHINGTON POST, Sep. 20, 2016, *at* https://www.washingtonpost.com/local/education/online-sextortion-against-children-growing-feds-urge-back-to-school-awareness/2016/09/19/395a6cbe-7b5b-11e6-beac-57a4a412e93a_story.html (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

78 sextortion cases and found that 83% of the cases reportedly involved social media manipulation.[136] As children are generally trusting and more likely than adults to accept or initiate social contact with strangers on social media platforms, offenders can quickly and easily begin manipulating children for sexual exploitation.[137]

Technological changes and the rise of catfishing have led to widespread, high-profile cases of child sexual abuse, including sextortion. Abusers utilize diverse methods and tactics. Casual conversations turn from "innocent enough" to "asking for pictures," becoming more and more sexual, according to a then-16-year-old girl, who mentioned her "very low self esteem" and the perpetrator's pressure as her reasons for compliance.[138] An offender may simply send an explicit photo to a young victim making the victim feel "obligated to 'reciprocate'" by taking a nude photo.[139] Other young victims of catfishing mentioned predators inventing personal tragedies to gain sympathy: cancer diagnoses, deceased children, dying siblings, or threats by the perpetrator to commit self-harm in order to manipulate victims into compliance. Others – over prolonged conversations – become lured into feeling deep romantic attachments to misrepresented persons, or fear of "seem[ing] like a baby" to a nascent romantic interest.[140] The reasons for engaging in initial conversations and for remaining engaged in them vary, but these contacts and methods provide predators with broad opportunities for escalating abuse.[141]

Offenders commit acts of sextortion for various reasons: the desire to obtain sexually explicit material of the victim (e.g., images, videos); to coerce the victim into performing sexual favors or other face-to-face sexual acts; or to force the victim to pay money.[142] According to a June 2016 U.S. online survey of 1,631 sextortion victims[143], 66% of online sextortion offenders were motivated solely to obtain additional sexual material from victims, rather than money.[144] In cases of online sexual coercion and extortion of children, 83% of offenders were sexually motivated, and their goal was to obtain materials and acts of a sexual nature from their victims.[145] Approximately 40% of all respondents in the study were 18 years old at the time of the survey, although the vast majority of them reported being victimized while under age 17.[146]

The effects of sextortion are far-reaching. Victims suffer depression and anxiety, engage in cutting and other forms of self-harm, and in some cases, attempt or commit suicide.[147] Child victims also may experience fear and a sense of hopelessness.[148] The analysis conducted by NCMEC of sextortion cases reported from October 2013 to April 2016 found that approximately one in three children who had fallen victim to sextortion had engaged in self-harm, threatened suicide, or attempted suicide as a

---

136 The Brookings Institution conducted a study analyzing "78 cases in 52 jurisdictions, 29 states or territories, and three foreign countries." Of these 78 cases, 71% involved only minor victims, 18% involved a mix of minor victims and adult victims, and 12% of cases, all victims were adults. Benjamin Wittes et al., *supra* note 24, at 12.

137 Shelley Lynch, *supra* note 70.

138 Janis Wolak and David Finkelhor, *supra* note 46, at 13.

139 *Id.*

140 *Id.* at 13, 17.

141 Janis Wolak and David Finkelhor, *supra* note 46.

142 *Id.*

143 The study focused on sextortion against children age 17 and younger (i.e., at the time of the contact or abuse), primarily, but respondents ranged in age from 18 to 25; nearly 40% of all respondents were 18 at the time they completed the survey. Janis Wolak and David Finkelhor, *supra* note 46, at 7-8.

144 *Id*. at 22.

145 Europol, *supra* note 10, at 10.

146 Janis Wolak and David Finkelhor, *supra* note 46, at 7.

147 U.S. Department of Justice, *supra* note 3, at 76.

148 The Sextortion Factsheet, *supra* note 79.

result.[149] A 2015 FBI analysis of 43 sextortion cases involving child victims found that 28% of the cases had at least one sextortion victim who attempted or committed suicide.[150]

Ronan Hughes, a 17-year-old Northern Irish boy from Co Tyrone, committed suicide in June 2015 after 31-year-old Iulian Enache of Romania tricked Hughes into sending intimate photos of himself, which he later sent to Hughes' friends after he failed to pay ransom. Enache pleaded guilty to charges of blackmail and the production and distribution of indecent images of children and was sentenced to four years in prison in Romania. The complex investigation was a joint operation between Romanian police, Police Service of Northern Ireland, Europol, and the UK National Crime Agency.

Source: Hannah Summers, *Man jailed over blackmail plot that led to Tyrone boy's suicide,* Aug. 30, 2017, THE IRISH TIMES, *at* https://www.irishtimes.com/news/crime-and-law/man-jailed-over-blackmail-plot-that-led-to-tyrone-boy-s-suicide-1.3203188 (last visited Oct. 8, 2018).

In many cases, child victims of sextortion are often reluctant to report the victimization to law enforcement because they are embarrassed and ashamed, or they do not realize they were victimized.[151] The earlier-mentioned 2016 U.S. study of 1,631 victims showed that only 16% of those surveyed reported the incidents to law enforcement, while nearly half (45%) did not even go to family or friends for help.[152] A majority of respondents (77%) said they did not ask for help from family or friends because they were too ashamed or embarrassed."[153]

Legislation in some countries shames victims by treating them as offenders because taking a nude photograph and sending it online is criminalized as production and distribution of child sexual abuse material.[154] According to Europol, "this shaming of the victim perpetuates the child's victimisation and creates a culture that is not conducive to disclosing victimisation."[155]

149 *Id.*
150 U.S. Department of Justice, *supra* note 3, at 76.
151 Europol, *supra* note 10, at 21.
152 Janis Wolak and David Finkelhor, *supra* note 46, at 42, 48.
153 *Id.* at 42.
154 Europol, *supra* note 10, at 21.
155 *Id.*

Nonconsensual Pornography

Nonconsensual pornography (also known as nonconsensual sharing of intimate images or revenge pornography) is the distribution of sexually explicit materials without consent of one or more of the individuals involved.[156] Nonconsensual pornography may be motivated by the desire to inflict shame and humiliation on the victim,[157] and/or to use the victim for the "sexual entertainment" of online strangers.[158]

Traditionally, revenge pornography and related discussions focused largely on conduct among adults. In recent years, however, minors have become increasingly susceptible to revenge pornography.[159] For instance, police in Uruguay reported that 30 complaints were received from adults for dissemination of intimate images without consent in 2014 and 2015, while cases involving minors for the same period exceeded 600.[160] This increase may be due in part to the growing trends in mobile technology, such as easier and faster image and video-sharing, including of sexual content (sexting).[161] In Australia, sexting comprised 4% of all cases reported to the Office of the eSafety Commissioner from April 2016 through the end of June 2016[162]; since that time, however, sexting complaints have significantly increased to 16% of all reports.[163]

When children are victims of nonconsensual pornography, it is typically carried out against them through one of two approaches: the perpetrator initially gains materials *with* the victim's consent (i.e., the victim willingly and intentionally conveys the images or videos), or the perpetrator does so *without* their consent.[164] In the first instance, the offender disseminates intimate photos or videos which they obtained consensually from the victim, often pursuant to a current or past relationship. For example, in one instance, a 16-year-old girl's nude photos were sent to her friends, family, and school principle as an act of revenge by her boyfriend with whom she refused to have sex.[165] Sometimes, however, there may be no direct relation between the offender and the victim at all, as when someone conveys private materials of their partner's former significant other.[166] In both scenarios, the initial conveyance

---

156 Danielle K. Citron and Mary A. Franks, *supra* note 30.

157 The Crown Prosecution Service (CPS), *Revenge Pornography – Guidelines on Prosecuting the Offence of Disclosing Private Sexual Photographs and Films*, *at* http://www.cps.gov.uk/legal/p_to_r/revenge_pornography/ (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

158 Cyber Civil Rights Initiative, *Frequently Asked Questions, at* https://www.cybercivilrights.org/faqs/ (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

159 Mark O'Regan, *Children as young as 12 are victims of revenge pornography – warns charity*, INDEPENDENT.IE, NOV. 20, 2016, *at* https://www.independent.ie/irish-news/children-as-young-as-12-are-victims-of-revenge-pornography-warns-charity-35229838.html (last visited Oct. 8, 2018).

160 *When intimacy serves as revenge (Cuando la intimidad sirve de venganza)*, EL PAIS, Jan. 31, 2016 *at* https://www.elpais.com.uy/que-pasa/intimidad-sirve-venganza.html (last visited Oct. 8, 2018).

161 "Sexting" is defined as a practice in which "children and young people…[post] sexually provocative images of themselves online or [send] them to friends using mobile technologies." *See*, *Guidelines for Policy Makers on Child Online Protection*, 2009, 14, International Telecommunications Union, *at* http://www.itu.int/en/cop/Documents/guidelines-policy%20makers-e.pdf (last visited Oct. 8, 2018).

162 Lauren Martyn-Jones, *Sexting has led to a rise of revenge porn and 'sextortion'*, THE COURIER MAIL, Oct. 14, 2016 (on file with the International Centre for Missing & Exploited Children).

163 *Id*.

164 Dr. Asia Eaton, Dr. Holly Jacobs, & Yanet Ruvalcaba, *2017 Nationwide Online Study of Nonconsensual Porn Victimization and Perpetration: A Summary Report* 3, Cyber Civil Rights Initiative, Jun. 2017, *at* https://www.cybercivilrights.org/wp-content/uploads/2017/06/CCRI-2017-Research-Report.pdf (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

165 Janis Wolak and David Finkelhor, *supra* note 46, at 28.

166 One recent example in Canada involved a 16-year-old girl who distributed intimate photos of her new boyfriend's former girlfriend (taken during the boyfriend's former relationship) online and via sexting in order to "get revenge" on her boyfriend's ex. Gaby Dunn, *Canadian Teen Convicted of Child Porn in Revenge Sexting Case*, THE DAILY DOT, Jan. 14, 2014, *at* http://mashable.com/2014/01/14/teenager-canada-sexting/#nqHrO9PgMgqY (last visited Oct. 8, 2018); *see also, Sexting Teen Guilty of Distributing Child Porn*, CBC NEWS, Jan. 10, 2014, *at* http://www.cbc.ca/news/canada/british-columbia/sexting-teen-guilty-of-distributing-child-porn-1.2491605 (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

of materials was willing and intentional, but the subsequent passage of those materials – via social media platforms, for example – is not consensual. Older children are particularly susceptible to this form of revenge pornography, as they are more likely to share intimate photos of themselves with a significant other via sexting, or through their use of adult dating apps.[167]

A 20-year-old man in New South Wales, Australia, was sentenced to three years of home detention after sending sexually exploitative photos of a 14-year-old girl to her parents and friends. The two met on a popular social media site and began a relationship in late 2015, when he was 18 and she was just 14. At his request, she sent naked photos, some of which showed her face. Over time, he became verbally abusive and threatened to send the photos to her family and friends to coerce her into sending additional photos and videos. He also threatened her family with physical violence. During a trip to Adelaide with her parents, she told them about the "aggressive and threatening" messages and they contacted police. On 27 January 2017, the man was arrested as he arrived at the airport in Adelaide. He pled guilty, but took no responsibility for his actions. During the trial, the judge noted that the man admitted that he "sent sexually exploitative photographs of the victim to her parents and other family members in an act of revenge" and that he demonstrated "a disturbing lack of remorse, contrition and insight" for his actions.

Source: Mitch Mott, *Revenge porn sender to serve three year sentence on home detention despite sending "obscene" photos of 14-year-old girl*, ADELAIDE NOW, Oct. 31, 2017 (on file with the International Centre for Missing & Exploited Children).

A growing number of children, including those as young as 10,[168] are engaging in sharing intimate material and using social networking apps in an attempt to become "more popular," or sexting to gain the favor of their peers,[169] and they are vulnerable to victimization via revenge pornography. In January 2016, UK police reported that 191 out of 1,232 revenge pornography victims who were reported since April 2015 were under age 18 and some were as young as 11 and 12 years old.[170] These are concerning figures, given the rapid pace of ever-younger children accessing and learning to use ICTs. "Very young children" increasingly "handle mobile devices that can both take pictures, produce videos and access social networks with little supervision," consequently leading to the potential for increased "opportunities for sexual extortion."[171] The corresponding increase in self-produced materials and higher rates of ICTs and mobile use by younger children suggest future challenges.[172] The UK National Crime Agency (NCA) reported that "self-broadcast live-streaming is a growing concern with 1 in 8 teens having broadcast on Instagram and 1 in 10 on Facebook, and children being coerced and extorted into streaming" penetrative and non-penetrative sexual content.[173] The NCA further noted that these images "can be harvested and redistributed leading to blackmail and extortion for further images by

---

167 *See generally,* Jack Blanchard, *Tinder and Grindr Dating Apps Linked to More than 500 Crimes Including Murder, Rape and Child Abuse*, MIRROR, Dec. 30, 2016, *at* http://www.mirror.co.uk/news/uk-news/tinder-grindr-dating-apps-linked-9537441 (last viewed Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

168 Internet Watch Foundation, *Emerging Patterns and Trends Report #1 – Online-Produced Sexual Content*, Mar. 10, 2015, *at* https://www.iwf.org.uk/sites/default/files/inline-files/Online-produced_sexual_content_report_100315.pdf (last visited Aug. 2, 2018); *See also,* David Barrett, *Sexting: Girls as young as seven in explicit videos online,* THE TELEGRAPH, Mar. 10, 2015, *at* https://www.telegraph.co.uk/news/health/children/11460757/Sexting-Girls-as-young-as-seven-post-explicit-videos-online.html (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

169 Mark Seguin, *Children and Revenge Porn: There are No Private Moments,* TBG Solutions, Inc., Apr. 17, 2015 (on file with the International Centre for Missing & Exploited Children). *See also*, Murray Lee, et al., *Sexting and Young People – Report to the Criminology Research Advisory Council* 33, Nov. 2015, *at* http://www.criminologyresearchcouncil.gov.au/reports/1516/53-1112-FinalReport.pdf (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

170 Tim Calver, *At Least 200 Children, Some as Young as 11, Have Been Victims of 'Revenge Porn' in Past Nine Months*, THE TELEGRAPH, Jan. 23, 2016, *at* http://www.telegraph.co.uk/news/uknews/law-and-order/12117342/At-least-200-children-some-as-young-as-11-have-been-victims-of-revenge-porn-in-past-nine-months.html (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

171 Europol, *Child sexual exploitation online – Future threats and developments*, *at* https://www.europol.europa.eu/iocta/2014/chap-3-3-view3.html (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

172 *IWF Annual Report 2016*, 9, Internet Watch Foundation, *at* https://www.iwf.org.uk/sites/default/files/reports/2017-04/iwf_report_2016.pdf (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

173 National Crime Agency, *National Strategic Assessment of Serious and Organised Crime* 29, 2018, *at* http://www.nationalcrimeagency.gov.uk/publications/905-national-strategic-assessment-for-soc-2018/file (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

sexually and financially motivated offenders, which in turn increases the risk of self-harm and suicide by victims."[174]

As in sextortion cases, a perpetrator may disseminate photos or material obtained through hacking the victim's computer or smartphone, or by using a hidden camera to record the victim without their knowledge.[175] A former boyfriend/girlfriend can digitally post a video that they secretly took during a sexual encounter with a former significant other without their knowing or – similar to sextortion cases – a hacker can infect the victim's computer to retrieve intimate digital content and upload it on the Internet or to social networking apps.[176]

A 2014 article discussing the leak of approximately 90,000 Snapchat photos and 9,000 videos revealed that the responsible hackers may have intended to target children directly, as half of all Snapchat users are children between the ages of 13-17.[177] A 2016 UK study found that 12 out of 25 reported revenge pornography cases involved victims under age 18, whose photos were shared via Facebook, Snapchat, Instagram, WhatsApp, and Twitter.[178] Cases like these underscore the importance of talking to children about the implications of taking and/or sharing explicit images as well as who to contact if they are approached online.

In 2017, Facebook received reports that sexual videos were being shared through its Messenger platform. After deleting the material and notifying authorities in the United States, Europol and the Danish police were contacted. Denmark's National Cyber Crime Center began investigating the case and determined that more than 1,000 children and young people in Denmark had shared and redistributed a sexual video featuring two 15-year-olds having sex. Since then, 1,004 alleged offenders ranging from 15-20 years old have been charged with redistributing child sexual abuse material.

Source: Ray Downs, *Denmark charges 1,000 with child porn for sharing sex videos*, Jan. 15, 2018, NBC NEWS, *at* https://www.upi.com/More-than-1000-Danish-youths-charged-in-child-revenge-porn-case/2391516081408/ (last visited Oct. 2, 2018) (on file with the International Centre for Missing & Exploited Children).

Regardless of how materials are obtained or whether initial consent was given, all revenge pornography shares overarching qualities: the perpetrator's primary goal is to harm the victim, either by inflicting public shame and embarrassment,[179] or by using the victim's photos/videos for the offender's own sexual pleasure without knowledge or consent.[180] Both goals have equally devastating consequences. Dissemination of explicit material without consent allows the posted material to be visible to close associates (e.g., family members, peers, and school officials) and potentially thousands of strangers, and it can be copied and re-shared on thousands of web domains.[181] Within days or even just hours, the material can "dominate the first several pages of 'hits' on the victim's name in a search engine."[182]

174 *Id.*
175 Danielle K. Citron and Mary A. Franks, *supra* note 30.
176 Janis Wolak and David Finkelhor, *supra* note 46, at 19.
177 Radhika Sanghani, *Nude photo leak: Now the hackers are going after children on Snapchat*, THE TELEGRAPH, Oct. 13, 2014, *at* http://www.telegraph.co.uk/women/womens-life/11158863/Snapchat-nude-photo-leak-Now-the-hackers-are-going-after-children.html?ref=hihidnews (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).
178 Rob Helliwell, *Derbyshire revenge porn victims include children as young as 12*, BURTON MAIL, Apr. 27, 2016 (on file with the International Centre for Missing & Exploited Children).
179 The Crown Prosecution Service (CPS), *supra* note 157.
180 Dr. Asia Eaton et al., *supra* note 164, at 4.
181 Danielle K. Citron and Mary A. Franks, *supra* note 30, at 350.
182 Cyber Civil Rights Initiative, *supra* note 158.

Like sextortion and other forms of sexual abuse and exploitation, revenge pornography is profoundly damaging to its victims, who may experience shame and humiliation as well as a variety of mental health effects, including anxiety and depression.[183] Feelings of shame indicate that victims may deem themselves somehow responsible for their own victimization.[184] Further, they may be confronted by strangers who encounter the nonconsensually posted images or videos and teens may have difficulty finding employment.[185] Victims of revenge pornography may experience a general, deep loss of trust in others.[186] Many victims also report experiencing emotional issues regarding their self-esteem, confidence, and inability to control the nonconsensual distribution of their intimate images.[187] According to research conducted by the Cyber Civil Rights Initiative under its End Revenge Porn campaign, 51% of revenge pornography survivors had suicidal thoughts.[188]

An eight-year-old girl in Great Britain fell victim to revenge pornography. She was the youngest victim of the 277 revenge pornography offenses reported between April 2015 and December 2017 to the South Yorkshire Police. Eight other young girls ages 11, 12, 14, and 15 also were victimized during the same time period. Charges were brought against nine suspects and four others received cautions, though in most of the cases the victims did not support prosecution and thus the cases did not go to court.

Source: Thomas Burrows, *Eight-year-old girl victim of revenge porn,* FRASER COAST CHRONICLE, Jun. 17, 2018, *at* https://www.frasercoastchronicle.com.au/news/eightyearold-becomes-a-victim-of-revenge-porn/3444211/ (last visited Oct. 7, 2018).

As mentioned earlier, in 2016 at least 1,232 cases of revenge pornography were reported in the United Kingdom; these numbers include 191 teenagers with the youngest being only 11 years of age.[189]

In 2015, there were 1,143 complaints of revenge pornography in Japan.[190] Of the total complaints, only 276 were investigated by law enforcement.[191] In 2016, again, another 1,063 complaints of revenge pornography were reported to Japanese police, with the largest number of cases being threat-based.[192] The vast majority of targets (92.1%) were women; however, 35 cases involved child victims of prostitution and/or child sexual abuse material.[193] A key challenge to effective prosecution in Japan is the stigma surrounding being identified as a victim, with many simply expressing a desire to have "the material…deleted quickly, without people knowing, [and even] without having to report it to the police" or without seeking punishment of the perpetrators.[194]

183 Mudasir Kamal, *supra* note 31, at 362.
184 Janis Wolak and David Finkelhor, *supra* note 46, at 34.
185 Mudasir Kamal, *supra* note 31, at 363.
186 Samantha Bates, *Revenge Porn and Mental Health: A Qualitative Analysis of the Mental Health Effects of Revenge Porn on Female Survivors,* 2016, 9, FEMINIST CRIMINOLOGY, *at* https://www.biscmi.org/wp-content/uploads/2016/08/Revenge-Porn-and-Mental-Health-A-Qualitative-Analysis-of-the-Mental-Health-Effects-of-Revenge-Porn-on-Female-Survivors.pdf (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).
187 *Id.* at 13. See also, Mudasir Kamal, *supra* note 31, at 362.
188 Melanie Ehrenkranz, *We Need to Study the Effects of Revenge Porn on Mental Health,* Jun. 22, 2018, *at* https://gizmodo.com/we-need-to-study-the-effects-of-revenge-porn-on-mental-1823086576 (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).
189 Tim Calver, *supra* note 170.
190 *The Repercussions of revenge porn*, THE MAINICHI, Jan. 23, 2017, *at* https://mainichi.jp/english/articles/20170123/p2a/00m/0na/012000c (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).
191 *Id.*
192 Shimpachi Yoshida, *'Revenge porn' complaints to police top 1,000 for second year*, THE ASAHI SHIMBUN, Apr. 10, 2017 (on file with the International Centre for Missing & Exploited Children).
193 *Id*.
194 The Repercussions of revenge porn, *supra* note 190.

Good Practices

Legislative Responses

International

Since 1990, when the Convention on the Rights of the Child (CRC) was adopted by the United Nations (UN) General Assembly, the global community has recognized the importance of providing extra protection to children from sexual exploitation, trafficking, abuse, and other dangers. Since that time, the problem of online child safety has begun to receive attention at both the regional and international levels. Numerous initiatives addressing online child safety and child sexual exploitation have been developed, providing a foundation upon which new efforts may be based to address sextortion, nonconsensual pornography, and other emerging forms of child sexual exploitation.

Although sextortion and nonconsensual pornography are related to extant categories of prohibited crimes against children (such as child sexual abuse material under the CRC[195] and the Optional Protocol on the sale of children, child prostitution, and child pornography (OPSC)[196]), there have been no formal amendments to address these specific forms of online child sexual exploitation as distinct offenses. The United Nations Convention Against Transnational Organized Crime (UNTOC), introduced in 2000, presents a similar gap.[197] The UNTOC addresses the growing problem of technology-facilitated crimes, thereby providing a stronger foundation for assessing new ways predators are using ICTs to sexually exploit children; however, it does not specifically address sextortion and nonconsensual pornography that may occur in relation to organized crime networks.

In 2008, the World Congress III Against the Sexual Exploitation of Children and Adolescents helped make progress towards building a modern framework for addressing sexual extortion and revenge pornography. The resulting Rio Declaration summarizes the existing international laws and instruments focused on child protection; the preamble begins by highlighting then-emerging increases in sexual exploitation of children and adolescents, "in particular through abuse of the Internet and new and developing technologies,"[198] and recognizes in Article 11 that many States lack legislation to criminalize new forms of child sexual exploitation in conformity with international standards.[199]

Unlike earlier international instruments, the Rio Declaration specifically calls for nations to "undertake specific and targeted actions" to preclude predators from "using the Internet and [other] new technologies for the grooming of children…for the production and dissemination of child pornography and other materials."[200] Beyond recommending that governments establish online safety awareness and education programs for children, parents, schools, and child-care organizations,[201] the Rio Declaration also encourages States to criminalize "intentional production, distribution…access and

---

195 UN Convention on the Rights of the Child, Article 34, *at* https://www.ohchr.org/en/professionalinterest/pages/crc.aspx (last visited Oct. 8, 2018).

196 Optional Protocol to the UN Convention on the Rights of the Child on the sale of children, child pornography, and child prostitution, Article 10(1), *at* https://www.ohchr.org/en/professionalinterest/pages/opsccrc.aspx (last visited Oct. 8, 2018).

197 UN Convention Against Transnational Organized Crime, Article 29(1)(h), *at* https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf (last visited Oct. 8, 2018).

198 *The Rio de Janeiro Declaration and Call for Action to Prevent and Stop Sexual Exploitation of Children and Adolescents*—World Congress III against Sexual Exploitation of Children & Adolescents, Brazil, 2008, 2 (Preamble), *at* http://www.unicef.org/protection/Rio_Declaration_and_Call_for_Action.pdf (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

199 *Id.* at 3 (Art. 11).

200 *Id*. Art. 5, at 6.

201 *Id.* Art. 6, at 6.

viewing of [child sexual abuse materials, including] where there has been no physical contact with a child."[202]

Regional

Drawing from international initiatives, some regional efforts have sought to narrow the focus of digital threats to child safety to the more specific issue of online child sexual exploitation.

Entering into force in 2004, the Council of Europe Convention on Cybercrime (Budapest Convention)[203] has been ratified by 60 State Parties (43 Member States and 17 non-Member States), and signed but not yet ratified by 3 Member States and 1 non-Member State.[204] Although not tailored to addressing cybercrimes against children per se, the Budapest Convention contributes to the modern framework for addressing sextortion and nonconsensual pornography by specifically prohibiting certain computer-related, fraudulent, and digitally-facilitated offenses related to child sexual abuse material broadly.

Article 8 of the Budapest Convention requires Parties to adopt legislation or other necessary measures to criminalize intentional acts of computer-hacking conducted with "fraudulent or dishonest intent of procuring…an economic benefit for oneself or for another person."[205] Thus, in signatory countries this provision criminalizes the act of installing malware or using other means to steal victims' data for purposes of sextortion.[206]

Article 9 of the Budapest Convention focuses exclusively on cybercrimes related to child sexual abuse material.[207] It is significant in that it expressly includes in the characterization of such material not only that which depicts "a minor engaged in sexually explicit conduct," but also "a person appearing to be a minor" as well as "realistic images representing a minor" engaged in sexually explicit conduct.[208] Unfortunately, the Budapest Convention permits Parties to omit from national legislation the prohibition against the procurement or possession of child sexual abuse material through a computer system for oneself. It also permits Parties to derogate from implementing legislation punishing acts falling under this wider characterization of child sexual abuse material. The latter in particular potentially makes it more difficult to hold offenders liable for transmitting or possessing images of minors whose age is harder to determine.[209]

The Council of Europe took another step toward addressing online child sexual exploitation in 2007 with the Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse (Lanzarote Convention). In recognizing children's increased use of ICTs and the parallel rise of child sexual exploitation,[210] the Lanzarote Convention can be viewed as effectively condemning sextortion by requiring all Parties to formally criminalize the act of "recruiting…[or]…coercing a child into participating in pornographic performances or profiting from or otherwise exploiting a child for such purposes."[211] The Lanzarote Convention calls upon Parties to pursue "necessary legislative or other

---

202 *Id*. Art. 4, at 6.

203 Council of Europe Convention on Cybercrime, [Budapest Convention] opened for signature Nov. 23, 2001, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm entered into force Jul. 1, 2004 (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

204 Convention on Cybercrime (CETS 185): Chart of Signatures and Ratifications, *at* http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/201/signatures (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

205 *Id*. at Article 8(a)-(b).

206 It is important to note that while this provision addresses hackers solely seeking economic benefits, many offenders do not seek economic gain, but seek sexual gratification, particularly in child exploitation cases. *Id*.

207 *Id*. at Article 9 – Offences related to child pornography.

208 *Id*. at Article 9(2).

209 Id. at Article 9(4).

210 Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse (CETS 201) [Lanzarote Convention], Oct. 23, 2007, *at* http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/201 entered into force Jul. 1, 2010 (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

211 *Id.* at Article 21(1)(a)-(b).

measures"[212] to educate children on the dangers of sexual exploitation when using the Internet and other ICTs.[213] To promote incorporation of these aims into domestic policies, the Lanzarote Convention also established a Committee of Parties formed by representatives of the Member States.[214] As of August 2018, 44 Member States have ratified and 3 Member States have signed this Convention.[215]

The Memorandum on the protection of personal data and privacy in Internet social networks, specifically with regard to children and adolescents (Memorandum of Montevideo),[216] adopted in Montevideo, Uruguay, by a number of Latin American stakeholders in 2009, outlines a significant framework for addressing sextortion and revenge pornography in the Americas.

The Memorandum of Montevideo, while non-binding, constitutes a significant effort to combat online child sexual exploitation and is the only prominent regional instrument addressing online child safety developed outside of Europe to date. Unlike other regional instruments, the Memorandum advocates for increased protection of children's data and privacy on social networks, calling upon States to establish online safety education and awareness programs for children and caregivers.[217] Reflecting the principles of pre-existing international instruments, the Memorandum also underscores the importance of providing protections for minors in addition to those provided by national penal codes, recognizing that personal data and privacy of young children are especially vulnerable when they use social media websites and applications.[218]

One particularly unique legislative proposal appears in Provision 8 of the Memorandum of Montevideo, encouraging States to "legislate the right of children…to request access to any information on them included in public and private databases, and to the…removal of such information when necessary, in addition to their entitlement to express their opposition to the use of such information for any purpose whatsoever."[219] In helping minors assert their legal rights, this recommendation offers a strong basis for establishing cross-national legislation against revenge pornography by criminalizing the transmission of nonconsensual pornography and helping victims remove it from social media sites more quickly. The Memorandum of Montevideo further calls for social media corporations to "implement mechanisms for the reliable verification of the age of children…upon the creation of user accounts and/or access to specific content," envisioned as an important step in resolving the problem of children evading social networking websites' minimum user age policies and thus being more vulnerable to exploitation by adults.[220] Moreover, ICT industry participants are encouraged to collaborate with law enforcement by incorporating "efficient filtering [technologies]" into their websites to pinpoint child sexual abuse material, to immediately report any such material to relevant authorities, and to preserve data for investigations for up to six months – a necessity for successful prosecutions.[221]

In 2010, the League of Arab States enacted the Arab Convention on Combating Information Technology Offences (Arab Convention), a regional framework that enhances cooperation between

---

212 *Id*. at Article 6.
213 *Id*.
214 Council of Europe, *Lanzarote Committee*, *at* http://www.coe.int/en/web/children/lanzarote-committee (last visited Oct. 8, 2018).
215 Convention on Cybercrime (CETS 185): Chart of Signatures and Ratifications, *at* http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/201/signatures (last visited Oct. 3, 2018) (on file with the International Centre for Missing & Exploited Children).
216 *Memorandum of Montevideo,* formally known as the *Memorandum on the protection of personal data and privacy in Internet social networks, specifically in regard to children and adolescents,* Jul. 2009, *at* http://www.iijusticia.org/docs/MemoMVD_En.pdf (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).
217 *Id*. at 3-6.
218 *Id*. at 2, 8.
219 *Id*. at 6 (Provision 8).
220 *Id*. at 9 (Provision 23).
221 *Id*. at 17 (Provision 30).

Arab countries on ICT offenses.[222] As of June 2017, 18 of the 22 Member States of the League of Arab States had signed on to the Arab Convention.[223] Article 12 criminalizes computer-related production, display, distribution, publication, purchase, and sale of child sexual abuse material. Additionally, Article 13 criminalizes sexual exploitation, and offenses against privacy by means of information technology are criminalized under Article 14, though both provisions lack greater detail.

The EU Directive on combating the sexual abuse and sexual exploitation of children and child pornography of 2011 does not directly address sextortion or nonconsensual pornography, but does contain provisions criminalizing child sexual abuse material and solicitation of children for sexual purposes (grooming).[224] The EU Directive has been transposed into national law by 27 Member States.[225]

In 2014, the African Union Convention on Cyber Security and Personal Data Protection (African Union Convention) was adopted by the Member States of the African Union and opened for signature.[226] As of March 2018, 10 of 55 Member States had signed the African Union Convention and another two had ratified.[227] Article 29 (3) criminalizes the production, dissemination, procurement, and possession of "an image or representation of child pornography through a computer system." It also criminalizes providing access to pornographic content to a minor. Though the African Union Convention does not address sextortion and nonconsensual pornography directly, it is another useful tool for addressing elements of each.

In May 2018, the EU General Data Protection Regulation (GDPR) came into effect and is applicable not only to EU Member States, but also to all entities that process and access data within the EU.[228] While the GDPR is not specifically focused on children, it acknowledges that "children merit specific protection" and requires that communications directed to children be clear and easily understandable allowing a child to give consent for the collection and use of their personal data.[229] Furthermore, it acknowledges that the collection, use, and disclosure of a child's data warrants a higher standard of

---

222 League of Arab States, Arab Convention on Combating Information Technology Offences (Arab Convention), 2010, *at* https://cms.unov.org/DocumentRepositoryIndexer/GetDocInOriginalFormat.drsx?DocID=3dbe778b-7b3a-4af0-95ce-a8bbd1ecd6dd (last visited Sep. 6, 2018) (on file with the International Centre for Missing & Exploited Children). *See also,* Joyce Hakmeh, *Cybercrime and the Digital Economy in the GCC Countries* 11-12, Chatham House, Jun. 2017, *at* https://www.chathamhouse.org/sites/default/files/publications/research/2017-06-30-cybercrime-digital-economy-gcc-hakmeh.pdf (last visited Aug. 9, 2018) (on file with the International Centre for Missing & Exploited Children).

223 UNODC, *Comprehensive Study on Cybercrime*, Feb. 2013, *at* https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_22/_E-CN15-2013-CRP05/Comprehensive_study_on_cybercrime.pdf (last visited Aug. 9, 2018) (on file with the International Centre for Missing & Exploited Children).

224 Directive 2011/93/EU of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, Articles 18-20 (Dec. 13, 2011), *at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:335:0001:0014:EN:PDF (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children). (Corrigendum to Directive 2011/92/EU, '2011/92/EU' to be read as '2011/93/EU', http://db.eurocrim.org/db/en/doc/1715.pdf (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

225 National transposition measures communicated by the Member States concerning**:** Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, *at* https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=celex:32011L0093 (last visited Aug. 2, 2018) (on file with the International Centre for Missing & Exploited Children).

226 African Union Convention on Cyber Security and Personal Data Protection, *at* https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

227 *List of Countries which have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection*, *at* https://au.int/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection.pdf (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

228 EU General Data Protection Regulation (GDPR), *at* https://gdpr-info.eu/ (last visited Aug. 9, 2018) (on file with the International Centre for Missing & Exploited Children).

229 *Id*. at Article 8.

protection.[230] Recital 38 of the GDPR explains that "[c]hildren merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data."[231]

National[232]

In addition to international and regional developments, there also has been progress at the national level. Some countries that do not have specific laws punishing sextortion and nonconsensual pornography are, nonetheless, creatively utilizing existing laws that contain elements of sextortion and nonconsensual pornography to prosecute offenders. Others are developing new legislation that directly addresses these crimes.

Europe

Legislation in **Russia** does not specifically define either sextortion or nonconsensual pornography, though Article 137 of the Criminal Code concerning violating the right to privacy has been used to prosecute revenge pornography,[233] and Article 133 on compelling or coercing another to commit actions of a sexual nature has been applied to sextortion cases.[234]

In **Ireland**, the Harassment, Harmful Communications and Related Offences Bill 2017 (Bill 63 of 2017) was put forth to create the new offense of distributing an intimate image without consent, and also punishes cyberbullying, harassment, and stalking.[235] The Bill notes that the commission of an offense against a child is considered an aggravating factor. In January 2018, the Bill progressed to the third stage of review, but has not yet been passed into law.[236]

Article 226-2-1 of **France**'s amended Penal Code punishes violations of privacy. In October 2016, France enacted Article 226-2-1, which imposes a greater penalty for revenge pornography; it increases the penalty from €45,000 to €60,000 for violations of privacy that involve the nonconsensual broadcast of another's *words or images of a sexual nature* that were taken in a public or private place with the express or presumed consent of the other person.[237]

Germany also has taken initiative to address revenge pornography via the courts. In 2014, the German High Court ruled that "intimate photographs of partners should be deleted if a partner calls for it,"[238] and consent to a photograph could be revoked even years after it is taken.[239] Oxford University

---

230 Tay Nguyen, *GDPR matchup: The Children's Online Privacy Protection Act,* Apr. 5, 2017, *at* https://iapp.org/news/a/gdpr-matchup-the-childrens-online-privacy-protection-act/ (last visited Aug. 9, 2018) (on file with the International Centre for Missing & Exploited Children).

231 EU General Data Protection Regulation, *supra* note 228, at Recital 38.

232 This section is intended to provide a sampling of national legislative initiatives and is not an exhaustive list. For additional information on countries that criminalize revenge pornography, *see Revenge porn laws across the world,* The Centre for Internet & Society, *at* https://cis-india.org/internet-governance/blog/revenge-porn-laws-across-the-world (last visited Oct. 8, 2018).

233 *Revenge Pornography in Russia: How to protect your most personal information,* HI-TECH@MAIL.RU, Feb. 13, 2018, *at* https://hi-tech.mail.ru/amp/review/pornomest-v-rossii-kak-zashchitit-samoe-lichnoe/ (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children). The term for revenge pornography in Russian is порноместь.

234 *Sextortion and Corruption: What is Sexual Extortion*, WONDERZINE, Mar. 22, 2018, *at* https://www.wonderzine.com/wonderzine/life/life/233967-sextortion (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children). The term for sexual extortion in Russian is сексуальное вымогательство.

235 Harassment, Harmful Communications and Related Offences Bill 2017, Bill 63 of 2017, Houses of the Oireachtas, *at* https://www.oireachtas.ie/en/bills/bill/2017/63/ (last visited Oct. 8, 2018).

236 *Id.*

237 Penal Code of France, Oct. 7, 2016, *at* https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070719&idArticle=LEGIARTI000033207318 (last visited Oct. 8, 2018).

238 Philip Oltermann, *'Revenge Porn' victims receive boost from German court ruling*, THE GUARDIAN, May 22, 2014, *at* https://www.theguardian.com/technology/2014/may/22/revenge-porn-victims-boost-german-court-ruling (last visited Oct. 8, 2018).

239 Kristen Brown, *After a break-up, Germans now have to delete nude photos,* SPLINTER, Jul. 1, 2016, *at* https://splinternews.com/after-a-break-up-germans-now-have-to-delete-nude-photo-1793853928 (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

Professor Viktor Mayer-Schönberger noted that the court's decision should "at the very least…embolden future claimants to pro-actively want to prevent revenge porn."[240]

Spain's Penal Code was amended in 2015 to include Article 197, criminalizing "any individual who, without authorization, seizes, uses or modifies, to the detriment of a third party, such private personal or family data of another individual as may be recorded on computer, electronic or telematic files or media, or in any other type of file or record, whether public or private."[241] The act is punishable by imprisonment from two to five years if the data is divulged, revealed, or transferred to third parties and a higher penalty will be imposed if the victim is a minor.[242]

Dr. Matthew Falder, a 29-year-old Cambridge University graduate, was sentenced to 32 years in prison for blackmailing dozens of young victims into performing depraved sexual acts online. He admitted to committing 137 offenses against 46 victims around the world, both male and female, ranging from teenagers as young as 14 to adults. Three of his victims attempted suicide after being coerced into sending explicit and demeaning images.

For eight years, Falder targeted more than 300 victims with a "relentless, obsessive desire to continue committing offences." He forced his victims to send "increasingly severe self-generated indecent images of themselves, the focus of these images being to humiliate and degrade," including encouraging one victim to rape a four-year-old boy. These images were then distributed using anonymizing software and dark web forums on "hurtcore" websites depicting images of rape, murder, sadism, torture, pedophilia, blackmail, humiliation, and degradation. Falder was arrested in June 2017 following an international intelligence operation involving law enforcement in the United Kingdom, United States, Israel, and Australia. He "admitted charges including encouraging the rape of a child, fraud, causing sexual exploitation, blackmail, making indecent images, sending communications with intent to cause distress and possession of extreme pornography depicting torture, death and bestiality." Matt Sutton, a senior investigating officer of the NCA, said, "[i]n more than 30 years of law enforcement I've never come across an offender whose sole motivation was to inflict such profound anguish and pain – Falder revelled in it."

Source: Lizzie Dearden, *Matthew Falder: One of Britain's most prolific paedophiles jailed for 32 years after blackmailing children on dark web,* INDEPENDENT, Feb. 19, 2018, *at https://www.independent.co.uk/news/uk/crime/matthew-falder-latest-paedophile-jailed-32-years-sexual-abuse-blackmail-children-dark-web-a8217581.html*; *See also*, Jessica Labhart, *Matthew Falder: How global taskforce caught Birmingham paedophile*, BBC NEWS, Feb. 19, 2018, *at* https://www.bbc.com/news/uk-england-birmingham-42921977 (last visited Oct. 7, 2018).

The **United Kingdom** (England and Wales) has taken some of the most significant steps to criminalize online sexual exploitation following increased incidents of revenge pornography, especially among young children.[243] The Parliament enacted a new law in April 2015 to criminalize revenge pornography as a separate offense from other cybercrimes, making it easier for victims to report and seek legal action against perpetrators who "disclose private sexual photographs and films with intent to cause distress" without the subject's consent.[244] **Scotland** and **Northern Ireland** followed suit and, in February and April 2016 respectively, also criminalized revenge pornography as a distinct offense.[245]

---

240 *Id*.

241 Penal Code of Spain, 2015, Article 197 – On the Discovery and Revealing of Secrets, *at* http://www.wipo.int/edocs/lexdocs/laws/es/es/es179es.pdf (last visited Oct. 8, 2018).

242 *Id*.

243 Criminal Justice and Courts Act 2015, Sections 33-35, *at* http://www.legislation.gov.uk/ukpga/2015/2/contents/enacted (last visited Oct. 4, 2018).

244 *Id*.

245 Lucy Clarke-Billings, *Revenge Porn Laws in Europe, U.S. and Beyond*, NEWSWEEK, Sep. 16, 2016, *at* http://www.newsweek.com/revenge-porn-laws-europe-us-and-beyond-499303 (last visited Oct. 4, 2018). *See*, Abusive Behavior and Sexual Harm (Scotland) Act 2016, *at* http://www.legislation.gov.uk/asp/2016/22/contents/enacted. *See also,* Justice Act (Northern Ireland) 2016, Sections 51-53, *at* https://www.legislation.gov.uk/nia/2016/21/contents (last visited Oct. 4, 2018).

The Americas

Canada enacted its first revenge pornography legislation in 2014, which came into force in March 2015. The Protecting Canadians from Online Crime Act not only prohibits "non-consensual distribution of intimate images"[246] but also authorizes courts to order the removal of nonconsensual pornography from the Internet and social media sites, to prevent a perpetrator from distributing intimate images/videos, and to order a perpetrator to "[reimburse] victims for costs incurred in removing the intimate image [or video] from the Internet."[247] Applying to people of all ages,[248] the Act provides a maximum sentence of imprisonment of five years for revenge pornography perpetrators, with a less severe "summary conviction" sentence set at imprisonment of six months and/or $5,000 in fines.[249] Unfortunately, however, Canada's federal legislation and Provincial laws have not been evenly enforced in the courts; Manitoba, Nova Scotia, and Ontario courts have all rejected civil claims and/or altogether struck down these laws on a myriad of grounds, including "free expression" infringements and other constitutional issues.[250]

According to a report from the Brookings Institution, sentencing for cases of sextortion in the United States has "produced disparate sentences with almost no clear association between prison time meted out and the egregiousness of the crime committed." Further, "the severity of the sentence in a sextortion case" does not appear to be "directly related to either the number of victims or the depravity of the individual crime."

For example, in 2014, Joseph Simone, a 24-year-old Rhode Island man, was sentenced in state court to a year in prison and two years home confinement on 20 counts of indecent solicitation of a child, child sexual abuse material, and extortion and blackmail involving 22 high school boys. Simone, a high school wrestling coach, pretended he was a teenage girl and coerced the boys ages 15-17 years from across the state to send him nude photographs over a chat site named ooVoo. He knew many of his victims as he had coached or refereed their wrestling matches.

In comparison, also in 2014, William T. Koch was sentenced in federal court in Ohio to 20 years in prison and a lifetime of supervised release on federal charges of extortion, exploitation of a minor, and receipt and distribution of child sexual abuse material. From 2010-2013, he posed as a 15-year-old girl on Facebook and coerced and threatened 20 minor males as young as 11 to engage in sexually explicit conduct for the purpose of producing and sharing the content.

Source: Benjamin Wittes, et al., *supra* note 34*; See*, Zachary Malinowski, *Ex-Moses Brown wrestling coach sentenced for child pornography*, PROVIDENCE JOURNAL, Dec. 11, 2014, *at* http://www.providencejournal.com/breaking-news/content/20141211-ex-moses-brown-wrestling-coach-sentenced-for-child-pornography.ece; *See also*, Brad Dicken, *Man pleads guilty to Web sextortion,* THE CHRONICLE, Oct. 31, 2013, *at* http://www.chroniclet.com/cops-and-courts/2013/10/31/Man-pleads-guilty-to-Web-sextortion.html (last visited Oct. 8, 2018).

Despite the increased prevalence of sextortion and revenge pornography in the **United States** – especially against children – there is no federal legislation specifically criminalizing either form of online sexual exploitation.[251] A bipartisan bill was introduced in Congress in July 2016 aiming to federally define and criminalize nonconsensual pornography.[252] The bill, though not passed into law,

---

246 Marc Montgomery, *Canada's cyberbullying and revenge porn law applies to adults too*, RADIO CANADA INTERNATIONAL (RCI), Apr. 30, 2015, *at* http://www.rcinet.ca/en/2015/04/30/canadas-cyberbullying-and-revenge-porn-law-applies-to-adults-too/ (last visited Aug. 25, 2018).

247 *Id*.

248 Even minors who commit revenge pornography by sexting and/or distributing intimate photos of boyfriends/girlfriends will be held liable. *Id*.

249 *Id*.

250 Kirsten Thompson, *Cyberbullying & revenge porn: An update on Canadian law*, LEXOLOGY – CYBERLEX (Blog), Feb. 19, 2017, *at* http://www.canadiancybersecuritylaw.com/2017/02/cyberbullying-revenge-porn-an-update-on-canadian-law/ (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

251 Benjamin Wittes, Cody Poplin, et al., *supra* note 34.

252 Steven Nelson, *Lawmakers Unveil Proposal to Take Nip Out of Revenge Porn*, U.S. NEWS & World Report, Jul. 14, 2016, *at* https://www.usnews.com/news/articles/2016-07-14/lawmakers-lay-bare-proposal-to-take-nip-out-of-revenge-porn (last visited Oct. 5, 2018).

would have resulted in incarceration of up to five years for sharing intimate images without consent.[253] While the United States does not have federal legislation concerning revenge pornography, Washington, D.C. and 40 U.S. states have adopted legislation to outlaw revenge pornography within their individual jurisdictions.[254]

In June 2017, a bill focused on sexual extortion was introduced in the United States in an effort to "bring our laws into the age of smartphones and Snapchat" as the laws currently "governing online behavior were written when phones were plugged into walls and when texting someone required a postage stamp."[255] The bill, though not passed into law, would not only have prohibited using a victim's intimate images or video to extort or coerce them, but also would prohibit forcing victims to produce sexual images.[256] Some U.S. states have convicted sextortionists under existing state laws related to child sexual abuse material, extortion, and solicitation of minors.[257] Only five states, Alabama, Arkansas, California, Texas, and Utah, have enacted criminal sextortion laws to date.[258]

While **Mexico** does not yet have federal legislation in place, in December 2017 the Senate unanimously approved an amendment to the Federal Criminal Code to combat nonconsensual pornography as a form of sexual harassment.[259] Further, in September 2017 the State of Jalisco passed legislation punishing nonconsensual pornography with up to 12 years of imprisonment, and in early 2018 the State of Yucatan passed legislation punishing those who publish or disseminate sexual content without the consent of the other person via social networks, email, or any other means with one to nine years of imprisonment.[260]

Further south, few countries have existing legislation addressing sextortion or revenge pornography as standalone offenses; however, a number of countries address these forms of online child sexual exploitation through related laws against online grooming, the use of social media to pursue sexual encounters with children, and possession of child sexual abuse material with intent of sexual exploitation. For example, **Chile**[261] and **Costa Rica**[262] criminalize online grooming and the use of the computer to seek sexual encounters with minors; **Colombia** utilizes its computer crime law to penalize abusive access to computer systems and violation of personal data[263]; law in **Panama** broadly prohibits

---

253 H.R. 5896 - Intimate Privacy Protection Act of 2016, introduced Jul. 14, 2016, *at* https://www.congress.gov/bill/114th-congress/house-bill/5896 (last visited Oct. 8, 2018).

254 *40 States + DC Have Revenge Porn Laws,* Cyber Civil Rights Initiative (CCRI), *at* https://www.cybercivilrights.org/revenge-porn-laws/ (last visited Oct. 8, 2018).

255 Josh Saul, *Online Crimes Like Sextortion, Swatting and Doxing Could Soon Be Outlawed Federally,* NEWSWEEK, Jun. 27, 2017, *at* https://www.newsweek.com/sextortion-new-bill-laws-doxxing-swatting-congress-federal-fbi-629478 (last visited Sep. 17, 2018) (on file with the International Centre for Missing & Exploited Children). *See also,* H.R. 3067 – Online Safety Modernization Act of 2017, 115th Congress (2017-2018), *at* https://www.congress.gov/bill/115th-congress/house-bill/3067/actions (last visited Sep. 17, 2018) (on file with the International Centre for Missing & Exploited Children).

256 *Id.*

257 *State of Rhode Island v. Joseph Simone*, No. P2-2012-0684A (Providence County Superior Court); *Press Releases: Former Moses Brown Wrestling Coach Sentenced for Child Pornography, Indecent Solicitation of a Minor, and Extortion*, Department of the Attorney General, RI.Gov, Dec. 11, 2014, *at* http://www.ri.gov/press/view/23553 (last visited Oct. 8, 2018).

258 Ellen Wulfhorst, *Flood of sexual harassment claims seen boosting efforts to outlaw sextortion,* REUTERS, Oct. 17, 2017, *at* https://www.reuters.com/article/us-women-sexcrimes-sextortion/flood-of-sexual-harassment-claims-seen-boosting-efforts-to-outlaw-sextortion-idUSKBN1CM3B7 (last visited Sep. 17, 2018) (on file with the International Centre for Missing & Exploited Children).

259 *Senate approves reform to sanction revenge porn,* Senate of the Republic, Dec. 15, 2017, *at* http://comunicacion.senado.gob.mx/index.php/informacion/boletines/39808-aprueba-senado-reforma-para-sancionar-la-porno-venganza.html (last visited Oct. 8, 2018).

260 Carlos Salazar, *Pornovenganza could be penalized to up to 9 years in Yucatan*, REPORTE INDIGO, May 30, 2018, *at* https://www.reporteindigo.com/reporte/pornovenganza-en-yucatan/; *see also*, Miguel Velazquez, *Yucatan, The First Entity Where Pornovenganza is a Crime*, EL FINANCIERO, May 25, 2018, *at* http://www.elfinanciero.com.mx/nacional/yucatan-primera-entidad-donde-la-pornovenganza-es-delito (last visited Oct. 8, 2018).

261 Chilean Penal Code, amended in 2018, Article 366, *at* https://www.leychile.cl/Navegar?idNorma=1984&idParte=0 (last visited Oct. 8, 2018).

262 Costa Rican Penal Code, Article 167, *at* https://www.ministeriodesalud.go.cr/gestores_en_salud/derechos%20humanos/leyes/leyexplotsexual.pdf (last visited Oct. 8, 2018).

263 Colombian Penal Code of 2000, Article 269F – Violation of Personal Data, *at* http://leyes.co/codigo_penal/269F.htm (last visited Oct. 8, 2018). *See also*, Miguel Angel Lopez, *"Revenge porn", an evil of the digital age,* EL COLOMBIANO, Sep. 22, 2016, *at* http://www.elcolombiano.com/redes-sociales/porno-venganza-un-mal-de-la-era-digital-DB5030894 (last visited Oct. 8, 2018).

the use of ICTs as a vehicle to contact minors for sexually-related purposes or to "simulate sexual intercourse."[264]

In an effort to more directly address nonconsensual pornography, several countries in South America have introduced law reform initiatives and draft legislation. In 2016, for instance, a bill was introduced in **Argentina** to amend the Criminal Code by adding Article 155bis criminalizing the nonconsensual dissemination of intimate images.[265] As of November 2017, the bill was still under review.[266] Several other law projects and bills have been introduced in **Brazil**,[267] **Chile**,[268] **and Peru**[269] to amend existing laws to specifically address dissemination of intimate images without consent.[270]

Uruguay took a positive step in December 2017 when its Parliament passed the Law on Violence towards Women based on Gender.[271] Article 92 of this law penalizes the disclosure of images or recordings with intimate content without the other person's authorization.[272] The law states, "in no case will the authorization granted by a person under 18 years of age be considered valid" and if the victim is under 18 years of age it is considered an aggravating factor.[273]

Asia Pacific

The **Philippines** was one of the first countries in the world to criminalize revenge pornography by enacting a revenge pornography statute in 2009.[274] With a sentence of up to seven years of imprisonment, the Philippines penalizes offenders who distribute intimate images/videos of another person, regardless of whether the image was consensually obtained.[275] Similarly, **Japan** enacted a revenge pornography statute in 2014, providing a maximum sentence of incarceration of three

---

264 Penal Code of the Republic of Panama of 2008, Article 187, *at* http://www.wipo.int/wipolex/en/text.jsp?file_id=189272 (last visited Oct. 8, 2018).

265 Bill 2119/2016, Modification of the Criminal Code on Penalization of the Publication and/or Diffusion of Images without Consent of Total or Partial Nudity and/or Videos of Sexual or Erotic Content of Persons: Incorporation of Article 155bis, *at* http://www.senado.gov.ar/web/proyectos/verExpe.php?origen=S&nro_comision=&tipo=PL&numexp=2119/16&tConsulta=5 (last visited Oct. 8, 2018).

266 *Id.*

267 In Brazil, two recent bills have been introduced regarding dissemination of intimate images without consent. The first, PLC 18/2017, was introduced and adopted in March 2018 by the Senate and sent on to the Chamber of Deputies. The second, PL 9930/2018, was introduced in April 2018 before the Chamber of Deputies. To date, neither has been passed into law. *See*, House Bill No. 18, 2017, *at* https://www25.senado.leg.br/web/atividade/materias/-/materia/128223; PL 9930/2018, Chamber of Deputies, *at* http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2170680 (last visited Oct. 8, 2018).

268 In Chile, a bill was introduced in July 2018 to modify Article 161-A of the Criminal Code to criminalize nonconsensual dissemination through the Internet or other electronic means of images or content of a sexual nature obtained during the couple's private life. *See*, Bulletin 11923-23, *at* https://www.camara.cl/pley/pley_detalle.aspx?prmID=12444&prmBoletin=11923-25 (last visited Oct. 8, 2018).

269 In Peru, a bill 01669/2016-CR was presented in July 2017 to incorporate Article 154-B in the Penal Code criminalizing the dissemination of intimate material in a nonconsensual manner. A second bill, No. 2460/2017-CR, was introduced in February 2018 to amend Articles 154 and 177 of the Criminal Code to sanction dissemination of intimate images through any means of communication with a particular focus on women and child victims. Both are currently under review by the Commission on Justice and Human Rights. *See,* Bill No. 01669/2016-CR, *at* http://www.congreso.gob.pe/comisiones2016/Justicia/ProyectosLey/; *See also,* Bill No. 2460/2017-CR, *at* http://www.leyes.congreso.gob.pe/Documentos/2016_2021/Proyectos_de_Ley_y_de_Resoluciones_Legislativas/PL01669201707 17.pdf (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

270 Internet Lab, *Enfrentando Disseminação Não Consentida de Imagens Íntimas: uma análise comparada [Facing Nonconsensual Dissemination of Intimate Images: A Comparative Analysis], at* http://www.internetlab.org.br/wp-content/uploads/2018/05/Neris_Ruiz_e_Valente_Enfrentando1.pdf (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children). *See also,* Internet Lab, *How do countries fight the non-consensual dissemination of intimate images?,* May 25, 2018, *at* http://www.internetlab.org.br/en/inequalities-and-identities/how-do-countries-fight-the-non-consensual-dissemination-of-intimate-images/ (last visited Oct. 8, 2018).

271 Law on Violence Towards Women Based on Gender, No. 19580 of 2017, *at* https://www.impo.com.uy/bases/leyes/19580-2017 (last visited Oct. 8, 2018).

272 *Id.* at Article 92 – Disclosure of images or recordings with intimate content.

273 *Id.; see also* Article 93 – Special Aggravating Circumstances.

274 Republic Act No. 9995, An Act Defining and Penalizing the Crime of Photo and Video Voyeurism, Prescribing Penalties Therefor, and For Other Purposes, *at* https://www.lawphil.net/statutes/repacts/ra2010/ra_9995_2010.html (last visited Oct. 8, 2018).

275 *Id.*

years.[276] **New Zealand** also introduced a revenge pornography law in 2015, penalizing nonconsensual dissemination of sexual images.[277]

In 2014, INTERPOL launched an operation specifically targeting organized sextortion rings in the Philippines. Dubbed Operation Strikeback, the effort included coordinated information sharing between the INTERPOL Digital Crime Centre, the Philippines National Police, and law enforcement agencies in Singapore and Hong Kong. The two-day raid led to the arrest of 58 individuals, the seizure of over 250 pieces of electronic equipment, and the identification of over 190 individuals associated with organized crime in the Philippines. Three of the men arrested had harassed and sexually extorted a 17-year-old Scottish teenager, Daniel Perry, who later committed suicide.

Source: INTERPOL, *INTERPOL-coordinated operation strikes back at 'sextortion' networks*, 2014, *at* https://www.interpol.int/News-and-media/News/2014/N2014-075 (last visited Oct. 7, 2018).

Australia passed new legislation criminalizing nonconsensual pornography in August 2018. The new Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Bill 2018 not only imposes civil penalties against the individual who posted the intimate images, but also against the internet or email service provider and social media company on which the image was posted, if it fails to remove the images within 48 hours of receiving a removal notice.[278] In addition, the Bill amends the Criminal Code Act of 1995, introducing criminal penalties for nonconsensual pornography and considering it an aggravated offense if the image is of a child under the age of 16 years.[279] This legislation comes in response to an increasing number of cases in Australia as one in 10 Australians have either been threatened with the sharing of a sexual photo of themselves, or have had such a photo shared without consent.[280]

Some Australian states have undertaken initiatives to prosecute offenders by developing legislation criminalizing revenge pornography and sextortion. In 2014, Victoria became the first Australian state to specifically criminalize revenge pornography by making it a criminal offense to "maliciously distribute intimate images [of a person] without the person's consent."[281] Although created to proscribe revenge pornography, Victoria's law also could be used to convict sextortionists who carry out their threat of posting photos or videos of the victim online. In 2019, Western Australia's government announced plans to follow Victoria's example by introducing a bill that would criminalize revenge pornography as an amendment to its existing domestic violence legislation[282]; the Northern Territory has followed suit.[283] In August 2017, revenge pornography became a crime in New South Wales, as offenses were added to the Crimes Act 1900 criminalizing the recording and distributing of

---

276 Act No. 166 of 2006 Heisei 16, Act on Prevention of Damages by Providing Private Sexual Image Recording, *at* http://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=426AC1000000126 (last visited Oct. 8, 2018).

277 Nicola Henry and Anastasia Powell, *Sexual violence in the digital age: the scope and limits of criminal law*, SOCIAL & LEGAL STUDIES JOURNAL, Jan. 12, 2016. DOI: 10.1177/0964663915624273 (on file with the International Centre for Missing & Exploited Children).

278 Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Bill 2018, *at* http://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/s1113_third-senate/toc_pdf/1727820.pdf;fileType=application%2Fpdf (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children). *See also,* Corinne Reichert, *Australia passes 'revenge porn' legislation,* ZD NET, Aug. 16, 2018, *at* https://www.zdnet.com/article/australia-passes-revenge-porn-legislation/ (last visited Oct. 8, 2018).

279 *Id.*

280 Rachel Peters, *The Terrible Cousins: Sextortion and Revenge Porn*, VILLAINESSE, Oct. 13, 2015, *at* http://www.villainesse.com/think/terrible-cousins-sextortion-and-revenge-porn (last visited Oct. 8, 2018).

281 Dr. Nicola Henry, *Factbox: Revenge porn laws in Australia and beyond*, SBS NEWS, Jul. 13, 2015, *at* http://www.sbs.com.au/news/dateline/article/2015/07/13/factbox-revenge-porn-laws-australia-and-beyond (last visited Oct. 8, 2018).

282 *Revenge porn to be criminalized in Western Australia domestic violence law*, THE GUARDIAN, Sep. 10, 2016, *at* https://www.theguardian.com/society/2016/sep/11/revenge-porn-to-be-criminalised-in-western-australia-domestic-violence-law (last visited Oct. 8, 2018).

283 *Report on the Non-Consensual Sharing of Intimate Images*, Report No. 43, Nov. 2016, Northern Territory Law Reform Committee (Australia), *at* https://justice.nt.gov.au/__data/assets/pdf_file/0011/425666/Northern-Territory-Law-Reform-Committee-Report-on-the-Non-Consensual-S....pdf (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

intimate images of a person without consent.[284] Also in 2017, Australian Capital Territory made it a crime to publish or threaten to publish intimate images and photos of a young person with the Intimate Image Abuse Amendment Act.[285]

Similar to other regions, while national legislation specifically focused on sextortion or nonconsensual pornography may not exist, some countries are utilizing existing laws to combat these crimes. **Malaysia**, for instance, does not have specific legislation criminalizing sextortion; however, charges have been brought under Section 383 of the Penal Code (extortion) as well as the Personal Data Protection Act[286] as an invasion of privacy.[287] **Indonesia** does not have legislation specific to sextortion or revenge pornography, though revenge pornography is reportedly on the rise.[288] In recent cases, Indonesia has used Law No. 44 of 2008 (anti-pornography law),[289] Law No. 19 of 2016 on Electronic Information and Transactions,[290] and Article 369 (extortion) of the Penal Code[291] to prosecute these crimes. [292] In **India,** cases have been brought under Penal Code provisions including criminal intimidation, sexual harassment, and defamation as well as under the Information Technology Act for publishing obscene or lascivious content.[293] In **Singapore**, law does not specifically address sextortion, but criminalizes extortion generally under Section 383 of the Penal Code.[294] Accordingly, extortion is punished with imprisonment of not less than two years and not more than seven years.[295] Further, Singapore also criminalizes criminal intimidation under Section 503 of the Penal Code.[296]

Cases of revenge pornography have been on the rise in **Myanmar**.[297] Recently, activists in Myanmar have called for the nation's law enforcement agencies to improve security and privacy law in order to strengthen penalties for online sexual exploitation.[298] Section 66(d) of Myanmar's Telecommunication Law makes "extortion, threatening, or defaming someone 'by using any telecommunications network'" a criminal offense punishable by imprisonment of three years.[299]

---

284 *Revenge porn is a crime*, NSW Government, Aug. 25, 2017, *at* https://www.nsw.gov.au/news-and-events/news/revenge-porn-is-a-crime/ (last visited Oct. 8, 2018).

285 Crimes (Intimate Image Abuse) Amendment Act 2017, Section 72D – Intimate Image Abuse, *at* http://www.legislation.act.gov.au/a/2017-22/20170830-67084/pdf/2017-22.pdf (last visited Oct. 8, 2018).

286 Personal Data Protection Act 2010 (amended 2016), *at* http://ilo.org/dyn/natlex/docs/ELECTRONIC/89542/102901/F1991107148/MYS89542%202016.pdf (last visited Oct. 8, 2018).

287 Sextortion and revenge porn: what does our law say, *at* https://www.nst.com.my/opinion/columnists/2017/05/238156/sextortion-and-revenge-porn-what-does-our-law-say (last visited Oct. 8, 2018).

288 Kate Walton, *Revenge porn: The rise of a dangerous online phenomenon in Indonesia*, THE SOUTHEAST ASIA GLOBE, Mar. 7, 2018, *at* http://sea-globe.com/revenge-porn/ (last visited Oct. 8, 2018).

289 Law No. 44 of 2008 of Indonesia (Anti-Pornography Law), *at* http://www.bpkp.go.id/uu/filedownload/2/33/151.bpkp (last visited Oct. 8, 2018).

290 Law No. 19 of 2016 of Indonesia on Electronic Information and Transactions, *at* https://badanpendapatan.riau.go.id/home/hukum/8495315769-doc-20170202-wa0015.pdf (last visited Oct. 8, 2018).

291 Indonesian Penal Code, *at* http://humanrightspapua.org/resources/nlaw/175-indonesian-penal-code-kuhp (last visited Oct. 8, 2018).

292 Arya Dipa, *Inmates allegedly target dozens of women in 'sextortion' scam*, THE JAKARTA POST, Apr. 14, 2018, *at* http://www.thejakartapost.com/news/2018/04/14/inmates-allegedly-target-dozens-of-women-in-sextortion-scam.html (last visited Oct. 8, 2018).

293 V. Anirudh Narendra and Samraddhi Shetty, *Of sextortion, laws, and what victims of this crime can do*, HINDU BUSINESSLINE, Apr. 27, 2018, *at* https://www.thehindubusinessline.com/news/national/of-sextortion-laws-and-what-victims-of-this-crime-can-do/article23726557.ece; *See also,* Yashee, *Man getting 5 years in jail for sharing nude video of ex shows India is waking up to revenge porn*, DAILY O, Mar. 12, 2018, *at* https://www.dailyo.in/variety/revenge-porn-midnapore-cyber-crime-crimes-against-women/story/1/22796.html (last visited Oct. 8, 2018).

294 Penal Code of Singapore, Article 383 – Extortion, *at* https://sso.agc.gov.sg/Act/PC1871?ProvIds=P4XVII-P4_383- (last visited Oct. 8, 2018).

295 *Id.*

296 Penal Code of Singapore, Article 503 – Criminal Intimidation, *at* https://sso.agc.gov.sg/Act/PC1871?ProvIds=P4XVII-P4_383- (last visited Oct. 8, 2018).

297 Jaiden Coonan, *Revenge porn on the rise*, FRONTIER MYANMAR, Apr. 21, 2016, *at* https://frontiermyanmar.net/en/revenge-porn-the-rise (last visited Oct. 8, 2018).

298 Ei Cherry Aung, *As tech spreads, Myanmar women become victims of 'revenge porn'*, MYANMAR TIMES, Oct. 5, 2016, *at* http://www.mmtimes.com/index.php/national-news/yangon/22900-as-tech-spreads-myanmar-women-become-victims-of-revenge-porn.html (last visited Oct. 8, 2018).

299 *Id.*

Middle East & North Africa

An increase in "cyber-extortion" cases, particularly in Egypt,[300] Lebanon,[301] and Oman,[302] has been reported. Several countries have attempted to address the issues at hand. **Israel**, in 2014, became the only country in the region[303] to enact a revenge pornography law – setting a maximum sentence of imprisonment of five years for distribution of nonconsensual pornography – and the first country in the world to criminalize revenge pornography as a sex crime by classifying perpetrators as sex offenders.[304] In 2017, **Morocco**'s General Directorate of National Security, the main state police body, addressed its sextortion epidemic by adding five counter-cybercrime centers across the country[305]; 30% of sextortion acts committed worldwide are believed to emanate from Morocco.[306]

Africa

With Internet penetration on the rise around the world, it will not be long before sextortion and revenge pornography reach countries that currently do not have widespread Internet access,[307] including many countries in Africa. Among the African nations that do have widespread Internet access, a number of governments have not yet criminalized online sexual exploitation. While Section 25 of **Zimbabwe**'s Prevention and Combating of Corruption Act might reach both revenge pornography and sextortion by proscribing conduct where someone "in a position of power or authority…demands or imposes sexual favours…as a condition for giving…a right, privilege, or any preferential treatment,"[308] the government of Zimbabwe is considering drafting specific revenge pornography legislation.[309] The draft Computer Crime and Cybercrime Bill, proposed in 2016, is currently under review, and women's rights organizations have urged lawmakers to add revenge pornography to the draft bill.[310] Meanwhile, **South Africa** is revising both the Films and Publications Act to include nonconsensual pornography,[311] and the Cybercrimes and Cybersecurity Bill to add sexual extortion (harmful disclosure of pornography).[312, 313]

---

300 *What's next for 'Revenge Porn:' Will Arabs follow Israel's lead?,* ALBAWABA EDITOR'S CHOICE, Jan. 16, 2014, *at* https://www.albawaba.com/editorchoice/revenge-porn-547677 (last visited Oct. 8, 2018).

301 *Cyber-police crackdown draws sexual extortion out of the Middle East's online shadows*, THE NEW ARAB, Oct. 12, 2017, *at* https://www.alaraby.co.uk/english/blog/2017/10/12/lebanon-cyber-police-arrests-highlight-growing-middle-east-sexual-extortion (last visited Oct. 8, 2018).

302 *Rashidiya: 1479 cases of electronic extortion recorded last year and 362 since the beginning of this year*, OMAN DAILY, *at* http://www.omandaily.om/600976/ (last visited Oct. 8, 2018).

303 Israel is included in the Middle East North African region by the World Bank. It is considered Western Asia by the UN and Near East by the U.S. Department of State.

304 Lucy Clarke-Billings, *supra* note 245.

305 Youssef Igrouane, *Moroccan Police Set Up Laboratories to Fight Sextortion,* MOROCCO WORLD NEWS, Feb. 25, 2017, *at* https://www.moroccoworldnews.com/2017/02/209454/moroccan-police-set-five-laboratories-fight-sextortion/ (last visited Oct. 8, 2018).

306 Ghita Benslimane, *Moroccan City of Oued Zem Named World Capital of Sextortion,* MOROCCO WORLD NEWS, Oct. 29, 2016, *at* https://www.moroccoworldnews.com/2016/10/200096/moroccan-city-oued-zem-named-world-capital-sextortion/ (last visited Oct. 8, 2018).

307 INTERPOL has determined that most sextortion victims are from English-speaking countries, but that as Internet access expands into developing countries around the world, "the number of victims is likely to increase." Rachel Peters, *supra* note 280.

308 The Prevention and Combating of Corruption Act [Principal Legislation] of Tanzania, Section 25: Sexual favour or any other favours, *at* https://www.fiu.go.tz/pcca.pdf (last visited Oct. 8, 2018).

309 *Bill To Ban Leaking of Nudes,* NEWSDZEZIMBABWE, Aug. 12, 2017, *at* http://www.newsdzezimbabwe.co.uk/2017/08/bill-to-ban-leaking-of-nudes.html (last visited Oct. 8, 2018).

310 Make Every Woman County, *ZIMBABWE: Activists Call for Specific Laws to Fight Revenge Porn*, Jun. 28, 2017, *at* http://makeeverywomancount.org/index.php/gender-issues/women-peace-security/10536-zimbabwe-activists-call-for-specific-laws-to-fight-revenge-porn (last visited Oct. 8, 2018).

311 Lloyd Gumbo, *Revenge porn law long overdue,* THE HERALD, Jul. 22, 2016, *at* http://www.herald.co.zw/revenge-porn-law-long-overdue/ (last visited Oct. 8, 2018).

312 Cybercrimes and Cybersecurity Bill 2017, *at* http://www.justice.gov.za/legislation/bills/CyberCrimesBill2017.pdf (last visited Oct. 8, 2018).

313 Rorisang Kgosana, *Anti-revenge porn law added to Cybercrimes Bill*, THE CITIZEN, Jan. 20, 2017, *at* https://citizen.co.za/news/south-africa/1402739/anti-revenge-porn-law-added-to-cybercrimes-bill/ (last visited Oct. 8, 2018).

Kenya's Cyber Security and Protection Bill 2016, while still under consideration, includes Article 28 on the wrongful distribution of intimate images.[314] The article addresses some, but not all, of the elements of nonconsensual pornography. Article 28 penalizes the transfer, publishing, or dissemination through a telecommunications network or other communications technology of the intimate image of another person. While the draft law addresses the distribution of the intimate image, it does not speak to the offender's intent, the victim's consent or lack thereof, nor does it consider the age of the victim as an aggravating circumstance.

Cape Verde passed a new Cybercrime Law in 2017 criminalizing revenge pornography. Article 10 states that whoever disseminates through a computer system, photos, videos, or any material of a sexually intimate and private nature, with or without consent, of a person with whom they maintain(ed) an intimate relationship with the purpose of causing moral and psychological harm to the victim will be punished with a penalty of imprisonment of up to two years or a fine.[315]

[314] Cyber Security and Protection Bill, 2016, *at* http://www.parliament.go.ke/the-senate/house-business/senate-bills/item/download/2933_0f7efc708ba1d26afe68a22e44dd27a6 (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

[315] Cybercrime Law 2017 of Cabo Verde, *at* http://www.cnpd.cv/leis/Lei%20de%20Cibercrime.pdf (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

Prevention Initiatives

Policy Guidelines

The development of comprehensive policy guidelines can aid in implementing legislative goals. For example, in 2008 the United Nations took positive steps to modernize international policy on issues of online child safety and to call attention to new online risks in the digital age through the International Telecommunication Union's (ITU) Child Online Protection Initiative.[316] The ITU set forth four Guidelines for Child Online Protection: (1) Guidelines for Children; (2) Guidelines for Parents, Guardians, and Educators; (3) Guidelines for the ICT Industry; and (4) Guidelines for Policy Makers. Although non-binding, the Guidelines for Online Child Protection for Policy Makers[317] openly call for national governments to protect minors "in both the 'real' and 'virtual' worlds," recognizing that "any and every crime that can be committed against a child in the real world can…also be committed on the Internet," thus increasing children's vulnerability to sexual exploitation.[318]

These collective Guidelines underscore the need for both national and international policymaking entities to more closely coordinate with ICT industry leaders, and be cognizant of new risks that technology poses to young people, as "the speed with which the technology can change means that many of the traditional methods of law and policy making no longer fit [their intended] purpose[s]."[319] To this end, the Guidelines recommend two strategies: (1) that States develop specialized forensic computer training programs for law enforcement agencies to assist in better pinpointing online child sexual exploitation and catching new and repeat offenders[320]; and (2) that INTERPOL and other cross-border law enforcement agencies work closely with individual governments to exchange information so that law enforcement bodies can be equipped to catch online child sexual predators, regardless of their location.[321]

The European Commission's Safer Social Networking Principles for the EU (Principles) is an important example of a regional, non-legislative effort to address risks to children's safety online.[322] Created by private social networking companies, working in consultation with the European Commission and NGOs, these Principles are primarily recommendations that encourage providers to adapt their existing procedures to protect young Internet users.[323] The Principles contain numerous suggestions that address many of the underlying causes of child sexual exploitation. Principle 2, for instance, advises social networking companies to take steps to identify and remove under-age users from their platforms and to use cookies to track and ultimately restrict users from trying to re-register under a different age if they have previously been rejected for falling below the minimum user age threshold.[324] Principle 3 proposes that social networking companies default profiles of users under age 18 to private settings, as well as to exclude existing profiles of underage users from search capabilities, thus inhibiting predators using such networks from identifying, grooming, and possibly meeting children.[325] The Principles indicate the European Commission's concern for children's safety online; however, social networking sites and other ICT industry participants are *not* bound by these provisions and must

316 *About the Child Online Protection Initiative*, 2017, International Telecommunications Union, *at* http://www.itu.int/en/cop/Pages/about_cop.aspx (last visited Oct. 8, 2018).
317 International Telecommunication Union, *Guidelines for Policy Makers on Child Online Protection*, 2009, *at* https://www.itu.int/en/cop/Documents/guidelines-policy%20makers-e.pdf (last visited Oct. 8, 2018).
318 *Id.* at 36, 46.
319 *Id*.
320 *Id.* at 24.
321 *Id.* at 25.
322 *Safer Social Networking Principles for the EU,* The European Commission, Feb. 10, 2009, *at* https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/sn_principles.pdf (last visited Oct. 8, 2018).
323 *Id.*
324 *Id*. at 7, Principle 3.
325 *Id*.

choose to implement them for the provisions to be effective.[326] The valuable suggestions outlined in both the Principles and the ITU Guidelines can increase child safety online by reducing the victimization of young people by means of sextortion, nonconsensual pornography, and related acts.

Capacity Building & Cross-Sector Coordination

To fully support legislative and policy efforts, it is crucial that law enforcement and others on the frontline be well-trained and equipped with policies and procedures to respond to reports of sextortion and nonconsensual pornography. While there are many global training initiatives broadly addressing child sexual abuse and exploitation, and more specifically online child sexual abuse and exploitation, there are fewer such initiatives that target sextortion and nonconsensual pornography. As new technologies are created, it is crucial that law enforcement agencies become familiar with these new technologies to help keep children safer online. Establishing specialized training programs for law enforcement will better prepare police networks to investigate child sextortion and revenge pornography cases.

One early example of sextortion training was administered from 2009-2011 by the Tanzania Women Judges Association (TAWJA). The Stopping the Abuse of Power for Purposes of Sexual Exploitation: Naming, Shaming, and Ending Sexual Extortion program,[327] held in collaboration with IAWJ, was funded by the Royal Netherlands Government Ministry of Foreign Affairs, and provided seminars for law enforcement officers, judges, magistrates, magistrate trainees, and non-judicial personnel in the Judiciary to define and combat sextortion among adults, adolescents, and children.[328] Likewise, the Global Judicial Integrity Network, in coordination with the UN Office on Drugs and Crime, held a session in April 2018 titled Sextortion – The Need for New Standards of Judicial Integrity and Accountability to discuss judicial codes of conduct and professional ethics for confronting sextortion.[329] As sexual extortion involves abuse of power, sometimes committed by individuals in positions of authority like judges, government officials, educators, or employers, the session aimed to raise awareness of sextortion and encourage its inclusion in judicial codes of conduct and training programs on judicial ethics.[330]

The U.S. National Criminal Justice Training Center presented the webinar Sexual Violence in Cyberspace – From Abuse Images to Revenge Porn in March 2018 for U.S. law enforcement, prosecutors, educators, and social workers, among others.[331] The training aimed to teach participants about sextortion and revenge pornography, the impact on victims of abusive images online, and to introduce new U.S. state laws and discuss possible constitutional challenges.[332] Likewise, the 30th Annual Crimes Against Children Conference (held in Dallas, Texas, in August 2018), included several workshops for law enforcement and other child protection practitioners on sextortion and revenge pornography.[333]

---

326 *Id.* at 1.

327 *Stopping the Abuse of Power for Purposes of Sexual Exploitation: Naming, Shaming, and Ending Sexual Extortion: A Toolkit*, *at* http://www.iawj.org/wp-content/uploads/2017/04/Corruption-and-Sextortion-Resource-1.pdf (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

328 *Id.*

329 Global Judicial Integrity Network & UNODC, *Substantive Breakout Session Report,* Apr. 2018, *at* https://www.unodc.org/documents/ji/session_reports/iawj_launch_report.pdf (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

330 *Id.* The session was part of a larger global programme created following the adoption of the Doha Declaration in 2015. *See,* UNODC, *Doha Declaration Global Programme, at* http://www.unodc.org/dohadeclaration/news/2015/04/13th-un-crime-congress-closes-with-vow-to-implement-doha-declaration-for-crimes-victims.html (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

331 National Criminal Justice Training Center of Fox Valley Technical College, *Sexual Violence in Cyberspace – From Abuse Images to Revenge Porn*, 2018, *at* https://ncjtc.fvtc.edu/training/details/TR00006362/TRI0006363/part-2-sexual-violence-in-cyberspace-from-abuse-images-to-revenge-porn (last visited Aug. 27, 2018).

332 *Id.*

333 30th Annual Crimes Against Children Conference, *Full Agenda*, Aug. 2018, *at* https://www.eventscribe.com/2018/CACC/agenda.asp?h=Full%20Schedule (last visited Aug. 27, 2018) (on file with the International Centre for Missing & Exploited Children).

The UK NCA's Anti Kidnap and Extortion Unit (AKEU) was developed to handle cases of extortion, blackmail, and kidnapping.[334] In addition to investigating such cases, this small, specialized unit provides 24/7 response and conducts training for law enforcement in the United Kingdom and around the world on sextortion including how to recognize the offense, investigative recommendations, and victim support.[335]

Coordination between law enforcement agencies and the technology industry is also very important in the fight against sextortion and nonconsensual pornography. In response to news reports of children as young as age 11 falling victim to revenge pornography on social networking apps and social media sites from sexting with peers, a UK National Society for the Prevention of Cruelty to Children representative noted that this "underlines the urgent need for action by social media sites to improve safety."[336]

While it may not be feasible for all social networking services to incorporate age verification technology into their networks to prevent children from creating social media accounts with false age information[337], they can use image recognition technology (e.g., Microsoft's PhotoDNA[338]) to identify nonconsensual pornography and sextortion photos or videos by creating a database of images and algorithms.[339] Instagram has incorporated photo detection technology into the app to effectively ban all photos depicting intercourse, genitalia, and "close ups of fully-nude buttocks" to remove and prevent revenge pornography against minors as soon as possible after they are reported on the site.[340] Twitter also has successfully used photo detection technology to prevent users from circulating nonconsensual pornography by using databases and algorithms, disabling violators' accounts until the offending material has been removed.[341] Continued use of photo detection technology will help online industries work even more closely with law enforcement by helping identify victims and predators. In addition, it is imperative that companies pledge to increase support for minors by making it easy to report and request the removal of sexually exploitative content and then quickly blocking and removing[342] the reported content from Internet and social media platforms.[343]

---

334 National Crime Agency, *Kidnap and Extortion*, *at* http://www.nationalcrimeagency.gov.uk/crime-threats/kidnap-and-extortion (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

335 *Id.*

336 Peter Sherlock, *supra* note 38.

337 *Memorandum of Montevideo*, *supra* note 216, at 9 paragraph 23.

338 It should be noted that Microsoft's PhotoDNA, although largely effective, does not prevent all exploitative photos of children from being uploaded online. Although a devoted user of PhotoDNA, Facebook has not been able to detect all instances of child pornography. In January 2018, Facebook reached an out-of-court settlement with a 14-year old girl in Northern Ireland who sued Facebook for allowing her abuser to repeatedly post revenge pornography. *See,* Ivana Kottasova, *Facebook faces revenge porn trial over teenager's revenge*, CNN MONEY, Sep. 13, 2016, *at* http://money.cnn.com/2016/09/13/technology/facebook-nude-photo-lawsuit/index.html (last visited Oct. 8, 2018). See also, *Facebook warned over legal action after revenge porn case,* BBC News, Jan. 13, 2018, *at* https://www.bbc.com/news/uk-northern-ireland-42675036 (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

339 Kurt Wagner, *Facebook says it will use image recognition software to fight revenge porn,* Apr. 5, 2017, *at* https://www.recode.net/2017/4/5/15194360/facebook-ai-image-recognition-software-fight-revenge-porn (last visited Sep. 12, 2018) (on file with the International Centre for Missing & Exploited Children).

340 Zach Miners, *Instagram clarifies rules to ban revenge porn,* IDG NEWS SERVICE, PC WORLD, Apr. 16, 2015, *at* http://www.pcworld.com/article/2911232/instagram-clarifies-rules-to-ban-revenge-porn.html (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

341 Jonathan Blake, *Twitter Changes Rules to Ban 'Revenge Porn,* BBC NEWS, Mar. 11, 2015, *at* http://www.bbc.co.uk/newsbeat/article/31843001/twitter-changes-rules-to-ban-revenge-porn (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

342 Jack Smith, *Google is Doing Something About Revenge Porn That it Should Have Done Years Ago*, TECH.MIC, Jun. 22, 2015, *at* https://mic.com/articles/121111/google-is-doing-something-about-revenge-porn-that-it-should-have-done-years-ago#.7Cu7EoaBA (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

343 Jacqueline Beauchere, *Microsoft's 'revenge porn' approach, one year later*, Blogpost, Jul. 22, 2016, *at* http://blogs.microsoft.com/on-the-issues/2016/07/22/microsofts-revenge-porn-approach-one-year-later/#sm.01n7n2861e6qdem10vx2cdgik97la (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

Awareness-Raising Initiatives

It is essential that the public understand the nature of the risks children face online and steps that can be taken to better protect them. Awareness-raising initiatives take many forms, including conferences and training seminars, publications and written materials, and public service announcements and campaigns. Advocacy organizations, such as ICMEC, support governments, law enforcement, educators, healthcare professionals, and other frontline practitioners working directly with child victims and their families to apprise them of current trends, highlight the risks of online abuse like revenge pornography, sextortion, and online grooming, and outline preventive techniques to avoid victimization.

Based on reported incidences in 2015 and 2016, the Canadian Centre for Child Protection (Canadian Centre) noted an 89% increase in online sextortion cases among teenage boys. In response, the Canadian Centre developed Canada's first awareness and prevention campaign for boys, which launched 23 May 2017. The campaign "Don't Get Sextorted, Send a Naked Mole Rat" uses humor to deliver its message by using a naked mole rat character portrayed in various memes that can be sent as an alternative to those asking for nude photos online. The www.dontgetsextorted.ca website offers resources for teens, parents, and educators "to facilitate open conversations about the issue and a link to confidential online help."

Source: Press Release: *Online Sextortion of Teens on the Rise – Canada's first awareness and prevention campaign targeting boys launches in May*, Canadian Centre for Child Protection, May 23, 2017, *at* https://www.protectchildren.ca/en/press-and-media/news-releases/2017/dontgetsextorted_campaign (last visited Oct. 8, 2018).

The NCA, in partnership with the UK National Police Chiefs Association, launched a sextortion awareness campaign in December 2016 in response to the suicides of four young men who were victims of online sextortion.[344] Through video and print materials, the campaign explains the concept of sextortion, gives information about how to report the crime, and provides links to support resources.[345] Similarly, the Australian Federal Police manage the ThinkUKnow cyber-safety campaign to protect children by educating parents, teachers, and school children on inappropriate online behavior including sextortion and online grooming.[346] Europol launched the #SayNo Online Sexual Coercion and Extortion campaign in June 2017, including "a short film, available in all EU languages, which helps people to recognise a potential sextortion approach…and highlights the importance of reporting the crime to the competent national authorities."[347]

Thorn,[348] a U.S.-based NGO, initiated a Stop Sextortion campaign in 2017, utilizing imagery (e.g., memes, videos) and language (e.g., #NoShame, #FriendsFirst) that appeal to young people.[349] The campaign explains sextortion, outlines steps to take in case of sextortion, and makes available tools and resources to report the offense and support victims, including a text helpline.[350] The End Revenge Porn campaign was launched by the Cyber Civil Rights Initiative in August 2012.[351] The Campaign's mission includes providing a telephone helpline and educational resources for victims of revenge

344 National Crime Agency, *Sextortion (webcam blackmail), at* http://www.nationalcrimeagency.gov.uk/crime-threats/kidnap-and-extortion/sextortion (last visited Oct. 8, 2018).

345 *Id.*

346 Australian Federal Police, *ThinkUKnow*, *at* https://www.thinkuknow.org.au/ (last visited Oct. 8, 2018).

347 Europol, *Online Sexual Coercion and Extortion is a Crime: Public awareness and prevention*, *at* https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/online-sexual-coercion-and-extortion-crime (last visited Oct. 8, 2018). *See also*, Northamptonshire Police, *Campaign to #SayNo as report shows children as young as seven are falling victim to 'webcam blackmailing', at* http://www.northants.police.uk/simple/press-release/campaign-sayno-report-shows-children-young-seven-are-falling-victim-%E2%80%98webcam-blackmailing%E2%80%99 (last visited Oct. 8, 2018).

348 Thorn, *About us, at* https://www.wearethorn.org/about-our-fight-against-sexual-exploitation-of-children/ (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

349 Thorn, *Stop Sextortion campaign, at* https://www.stopsextortion.com/ (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

350 Report sexual extortion by texting "THORN" to 741741. *Id.*

351 Cyber Civil Rights Initiative, *End Revenge Porn Campaign*, *at* https://www.cybercivilrights.org/erp-campaign/ (last visited Oct. 8, 2018).

pornography and sextortion, supporting legislative movement to address these crimes, and developing technological tools to help combat the criminal behavior.[352] Similar campaigns, like the UK government's Be Aware B4 You Share campaign (#NoToRevengePorn),[353] launched in 2015, provides posters, videos, and other materials to inform the public that revenge pornography is a crime and what it entails, and gives redress guidance to victims.[354]

In addition to public awareness campaigns, it is important to incorporate online safety programs into school curricula.[355] Focusing on school safety programs is crucial as cooperation between teachers, parents, and students/peers can prevent online and offline sexual abuse. For instance, Childnet International, in collaboration with the UK Safer Internet Centre, offers materials for teachers to incorporate Internet safety themes across the curriculum and conducts customized in-school interactive presentations for students, teachers, and/or parents.[356] These programs should include discussions about online safety and good digital citizenship.[357] Similarly, ICMEC's *Education Portal* provides vetted and continually updated links to international resources addressing a broad range of child protection topics.[358] These resources provide curriculum support for educators around the world in addition to research-informed and accessible information and tools for students and parents.[359]

Helplines, Hotlines, & Other Reporting Mechanisms

The long-term mental health effects on victims of sextortion and revenge pornography, especially children, include depression, anxiety, panic attacks, and self-blame.[360] Victims may experience life-long emotional distress as "the mere knowledge that images exist and are being circulated causes shame, humiliation and powerlessness… This victimization lasts forever since the pictures can resurface at any time."[361] The impact can be devastating, leading some to contemplate, attempt or commit suicide.[362] Services, including legal and psychological support services, should be made available to help victims deal with the repercussions of the abuse and exploitation caused by sextortion and nonconsensual pornography.

Online victim support and advocacy groups like Digital-Trust,[363] Canada's needhelpnow.ca,[364] and the Crash Override Network[365] offer step-by-step instructions to teach children young victims of online sexual exploitation how to maintain safe online profiles, guide victims through the reporting process, and provide information on how to request the removal of content from social media platforms, if needed.

---

352 *Id.*

353 UK Government, *Be Aware B4 U Share, at* https://www.gov.uk/government/publications/revenge-porn-be-aware-b4-you-share (last visited Oct. 8, 2018).

354 *Id.*

355 Stay Safe Online, Middle & High School, *at* https://staysafeonline.org/teach-online-safety/middle-and-high-school/ (last visited Oct. 8, 2018).

356 Childnet International, *Teachers and Professionals*, *at* https://www.childnet.com/teachers-and-professionals (last visited Oct. 8, 2018).

357 Cosima Marriner, *supra* note 133. Good digital citizenship refers to acting responsibly, being cautious, and thinking critically when interacting in the digital world. For more information, see https://www.commonsensemedia.org/videos/what-is-digital-citizenship.

358 International Centre for Missing & Exploited Children, *Education Portal, at* https://www.icmec.org/education-portal/ (last visited Oct. 8, 2018).

359 *Id.*

360 U.S. Department of Justice, *supra* note 3, at 76.

361 Audrey Rogers, *Child Pornography's Forgotten Victims* 853, 28 Pace L. Rev. 847 (2008), *at* https://digitalcommons.pace.edu/cgi/viewcontent.cgi?article=1539&context=lawfaculty (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

362 U.S. Department of Justice, *supra* note 3, at 76.

363 Digital-Trust, *at* http://www.digital-trust.org/ (last visited Oct. 8, 2018).

364 Founded by the Canadian Centre for Child Protection, Needhelpnow.ca was specifically designed to serve as a resource for 13-17-year-old minors, providing self-help assistance with instructions on how to remove revenge porn or other sexually exploitative material from social media sites, like Facebook. *See,* NeedHelpNow.ca, *About Needhelpnow.ca*, *at* https://needhelpnow.ca/app/en/about (last visited Oct. 8, 2018).

365 Crash Override, *Resource Center, at* http://www.crashoverridenetwork.com/resources.html (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

Helplines, too, can connect victims and their family members with helpful resources to aid in coping with the abuse experienced.

A child abuse expert of Barnardo's Scotland warns that in cases of sextortion, "we are underestimating how real the threat [of suicide] is. We don't understand how embarrassing this can be for young people" and recommends that suicide prevention plans "be automatically put in place for young victims of webcam extortion."[366] Organizations like Lifeline[367] in Australia, Childline[368] and the Samaritans[369] in the United Kingdom, and the National Suicide Prevention Hotline[370] in the United States all provide suicide prevention assistance.

While there are numerous helplines that focus broadly on assisting child victims of sexual abuse such as Child Helpline International[371] and Netsafe,[372] in recent years several helplines have emerged that focus specifically on the issue of nonconsensual sharing of intimate images. The aforementioned Cyber Civil Rights Initiative's End Revenge Porn campaign launched the End Revenge Porn Crisis Line in October 2014 for victims of nonconsensual pornography.[373] Victims residing in the United States can call the toll-free helpline 24 hours a day, 7 days a week at 1-844-878-CCRI (2274).[374] Helpline counselors, victim support specialists, and a team of attorneys provide the urgent support victims need when an incident occurs.[375]

In February 2015, the Revenge Porn Helpline was launched in the United Kingdom by South West Grid for Learning, a nonprofit charitable trust, to assist victims whose intimate images or videos have been distributed online or offline without consent.[376] The Revenge Porn Helpline, funded by the UK government, connects callers with law enforcement and Internet companies to request the removal of content, and explains the available legal resources.[377] Similarly, in Scotland, a website (http://notyourstoshare.scot/) was developed to explain the issue of nonconsensual sharing of intimate images and help victims better understand the national law that criminalizes the act.[378] The site further provides information on how to report to police someone sharing or threatening to share an intimate image without the victim's consent (e.g., calling 101 or in an emergency 999), and links victims to trusted specialist services.[379]

The humiliation and shame that many victims suffer may prevent them from reporting the incidences to law enforcement.[380] As the number of cases of sextortion and revenge pornography increase globally, easily accessible reporting mechanisms may encourage victims to report to law enforcement as well as the technology companies, facilitating a rapid and effective response. In turn, increased reporting will also help generate much-needed data to improve understanding of the prevalence of

---

366 Libby Brooks, *Suicide prevention plan needed for child victims of 'sextortion' expert*, THE GUARDIAN, Nov. 29, 2017, *at* https://www.theguardian.com/society/2017/nov/29/suicide-prevention-plan-needed-for-child-victims-of-sextortion-expert-says (last visited Oct. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

367 Lifeline, *at* https://www.lifeline.org.au/ (last visited Oct. 8, 2018).

368 Childline, *at* https://www.childline.org.uk/ (last visited Oct. 8, 2018).

369 The Samaritans, *at* https://www.samaritans.org/ (last visited Oct. 8, 2018).

370 National Suicide Prevention Hotline, at https://suicidepreventionlifeline.org/ (last visited Oct. 8, 2018).

371 Child Helpline International, *Child Helpline Network*, *at* https://www.childhelplineinternational.org/child-helplines/child-helpline-network/ (last visited Oct. 8, 2018).

372 Netsafe Helpline, *at* https://www.netsafe.org.nz/nudes/ (last visited Oct. 8, 2018).

373 Cyber Civil Rights Initiative, *CCRI Crisis Helpline, at* https://www.cybercivilrights.org/ccri-crisis-helpline/ (last visited Oct. 8, 2018).

374 *Id.*

375 *Id.*

376 Revenge Porn Helpline, *at* http://www.revengepornhelpline.org.uk/ (last visited Oct. 8, 2018).

377 UK Government Equalities Office, *Revenge Porn Helpline Given Further Funding,* Apr. 8, 2017, *at* https://www.gov.uk/government/news/revenge-porn-helpline-given-further-funding (last visited Oct. 8, 2018).

378 Safer Scotland – Scottish Government, *Not Yours To Share, at* http://notyourstoshare.scot/ (last visited Oct. 8, 2018).

379 Myscot.gov, *Support if someone shares your intimate picture without permission, at* https://www.mygov.scot/intimate-image-victim-support/ (last visited Oct. 8, 2018).

380 Europol, *supra* note 10, at 21.

and trends and motives behind revenge pornography and sextortion, thereby allowing law enforcement to successfully identify and prosecute offenders.

According to INTERPOL, "anyone who believes they are being targeted should immediately cease all contact with the individual and report the matter to their local police and online service provider. If the communication is via a social network, the administrator should also be alerted."[381] Hotlines, like the UK's Revenge Porn Helpline,[382] Australia's CyberReport Hotline,[383] Canada's Cybertip.ca hotline,[384] and the U.S. CyberTipline[385] each provide the public with an online mechanism to report online sexual exploitation, including sextortion and revenge pornography, to law enforcement for investigation.

Reporting can also occur via the service providers and social media applications themselves. For example, Facebook's Help Center contains a form for users to report blackmail, intimate images, or threats to share intimate images.[386] Similarly, Snapchat,[387] Instagram,[388] Twitter,[389] and Skype,[390] give detailed information in their online help centers about how to report this kind of abusive behavior.

---

381 INTERPOL, *supra* note 76.

382 Press Release, Government Equalities Office, *Hundreds of Victims of Revenge Porn Seek Support From Helpline,* Aug. 23, 2015, *at* https://www.gov.uk/government/news/hundreds-of-victims-of-revenge-porn-seek-support-from-helpline (last visited Oct. 8, 2018).

383 Australia office of the eSafety Commissioner, *CyberReport Hotline*, *at* https://www.esafety.gov.au/complaints-and-reporting/offensive-and-illegal-content-complaints/report-offensive-or-illegal-content (last visited Oct. 8, 2018).

384 Canadian Centre for Child Protection, *Cybertip!ca – Report Form*, *at* https://www.cybertip.ca/app/en/report (last visited Oct. 8, 2018).

385 National Center for Missing and Exploited Children (NCMEC), *CyberTipline Report, at* https://report.cybertip.org/ (last visited Oct. 8, 2018).

386 Facebook, Help Center, *Report Blackmail, Intimate Images or Threats to Share Intimate Images*, *at* https://www.facebook.com/help/contact/567360146613371 (last visited Oct. 8, 2018).

387 Snapchat Support, *Report Abuse on Snapchat*, *at* https://support.snapchat.com/en-US/a/report-abuse-in-app (last visited Oct. 8, 2018).

388 Instagram, Help Center, *Report Blackmail on Instagram*, *at* https://help.instagram.com/contact/240773466098227 (last visited Oct. 8, 2018).

389 Twitter, Help Center, *I'm reporting exposed private information, at* https://help.twitter.com/forms/private_information (last visited Oct. 8, 2018).

390 Skype Help, Privacy and Security – Abuse and spam, *What should I do if I see abusive behavior on Skype?, at* https://support.skype.com/en/faq/fa34447/what-should-i-do-if-i-see-abusive-behavior-on-skype (last visited Oct. 8, 2018).

Conclusion

The Internet and related ICTs have led to countless positive developments the world over. However miraculous the Internet may be in some respects, our heavy reliance on it brings new and ever-evolving challenges, most as complex as the Internet itself. While the growth of ICTs has many benefits, it also has introduced new risks, especially for children. ICTs allow for new, developing, and constantly changing forms of online child sexual exploitation, among them sextortion and revenge pornography.

Children are using the Internet, receiving their first cell phones,[391] accessing social media and other messaging platforms, and are tempted to engage in peer-to-peer sexting at younger ages than ever before,[392] unwittingly increasing their risk of online victimization. Opportunities to sexually exploit children have increased with the spread of social media and Internet use. In the past 15 years, a plethora of online platforms have gained in popularity, opening the door for even more opportunities for child sexual exploitation. The ease of acquiring intimate images of children through grooming, manipulation, or hacking highlights the sensitivity and care that must be taken to reduce and combat online child exploitation.

While sextortion and revenge pornography fall under the broad umbrella of threats to children's safety under existing international and regional child protection initiatives, neither international nor regional legal instruments afford adequate attention to new and developing forms of online sexual exploitation necessary to fully protect children from potential offenders.

As the Brookings Institution report aptly explained, it is important to name the crimes, in order that they are understood as distinct from similar or related crimes like cyberbullying and stalking, and so legal responses can be properly formulated.[393] There is a need for targeted legislative provisions that encompass the elements specific to sextortion and nonconsensual pornography, with consistent terminology and definitions, penalties that better match the crime committed, and aggravating circumstances that consider at a minimum the age of the victim, the number of victims, the severity of the crime, and repeat offenses.[394]

Amid the benefits conferred by ICTs, the widespread dangers that sextortion and revenge pornography pose to children demonstrate that policymakers must take the appropriate steps to ensure that children are better protected and that the necessary resources are available for victims. The creation of accessible reporting mechanisms, collection of data, provision of training for law enforcement and other child protection practitioners, and facilitation of industry engagement can further respond to the growing threat of online child sexual exploitation and help make the world's children safer.

---

391 Study Finds Average Age of Kids When They Get First Cell Phone Is Six, *supra* note 16.

392 Erin Gabriel, *1 in 4 young people has been sexted, study finds,* CNN, Mar. 1, 2018, *at* https://www.cnn.com/2018/02/26/health/youth-sexting-prevalence-study/index.html (last visited Oct. 8, 2018); *See also,* Jessica Ringrose, et al., *A qualitative study of children, young people and 'sexting',* NSPCC, May 2012, *at* https://www.nspcc.org.uk/globalassets/documents/research-reports/qualitative-study-children-young-people-sexting-report.pdf (last visited Oct. 8, 2018).) (on file with the International Centre for Missing & Exploited Children).

393 Benjamin Wittes, Cody Poplin, et al., *supra* note 34.

394 *Id.*

ICMEC.org | Information@ICMEC.org
+1 703 837 6313 | 2318 Mill Rd Suite 1010, Alexandria, VA 22314