Combatting Cyber-Sextortion; Lessons for Sri Lanka from Australia and the United States

Harasgama, K. S., Munasinghe, M.A.P.M.
kushanthi.h@sliit.lk, paramie.m@sliit.lk
School of Law, Faculty of Humanities and Sciences, Sri Lanka Institute of Information Technology

Abstract

With the world rapidly becoming digitalized and the internet being an indispensable part of human life, incidents of cyber harassment including cyber-sextortion have also increased. Cyber-sextortion often involves a perpetrator threatening to disseminate private sexual images or videos of a victim unless more sexual image/sexual favours, money or other benefit are provided by the victim. This paper analyses the adequacy of current laws in Sri Lanka in comparison with those of Australia and USA in combating cyber-sextortion. The analysis reveals that although Sri Lank lacks specific laws on cyber-sextortion, some of its existing criminal laws such as the Penal Code provisions on extortion, criminal intimidation, sexual harassment and obscene publications relating to children can be used to a certain extent to prosecute cyber-sextortion. Some provisions of the Computer Crime Act of 2007, Prohibition of Ragging and Other Forms of Violence in Educational Institutions Act of 1998 and Obscene Publications Ordinance No. 4 of 1927 too can be used to a certain extent for this purpose. Australia, on the other hand, has targeted laws on cyber-sextortion, both at federal and state levels. At the Commonwealth level, section 474.14A of the Criminal Code of 1995 and several provisions of the Enhancing Online Safety Act 2015 (as amended) provide an apt gateway to combat cyber sextortion, while at states level, New South Wales, Northern Territory, Australian Capital Territory, Western Australia, South Australia and Victoria appear to have more comprehensive cyber sextortion laws in terms of capturing the offence. USA at the federal level does not have specific provisions on cyber-sextortion but has used non-specific provisions such as general extortion, child pornography, hacking and stalking laws for prosecutions on cyber-sextortion while at the state level, some states have introduced quite comprehensive targeted laws on cyber-sextortion, some have provisions that cover only certain types of cyber-sextortion. The paper concludes by proposing adoption of a targeted law on cyber sextortion outlining the key elements of a suitable law for Sri Lanka and until then to rely on non-specific provisions which are already available, in order to prosecute perpetrators of cyber-sextortion.

Keywords: cyber-sextortion, computer crimes, online harassment, criminal law

Introduction

Among the many offences committed in the cyber space today, cyber-sextortion has quickly emerged as a growing online phenomenon worldwide.[1] Defined very simply, cyber-sextortion refers to the conduct of threatening to commit some act, generally but not always threatening to release sexually explicit images of a victim, carried out using digital technologies, unless the victim complies with the demands of the perpetrator.[2] It must be noted that the threat could take different forms ranging from a threat to expose sexual images or personal information of a sexual nature to inflicting physical harm to the victim or someone else. The demand could also take different forms such as a demand for more sexually explicit images/videos, engaging in sexual acts or remaining/getting into a relationship with the perpetrator, monetary or other benefit etc.[3]

Existing research indicates that cyber sextortion is a prevalent and a growing problem worldwide.[4] Research further reveals that cyber-sextortion can have devastating impacts on the physical well-being, social life and mental health of victims including psychological issues such as depression, exposure to unwanted sexual advances and harassment, loss of relationships, having to change schools / jobs / residences etc.[5]

Given its prevalence and the seriousness of its impact on victims, cyber-sextortion is a problem that should be tackled through the legal system of a country. In this context, this paper aims to analyze the adequacy of relevant laws in Sri Lank compared with those of Australia and the United States of America in order to identify any lessons that Sri Lanka can learn from these jurisdictions. Australia and the United States have been selected for this comparison as they can provide useful insights in designing a targeted law on cyber-sextortion but also on how the existing laws can be effectively used to combat this issue in the absence of targeted laws.[6]

This paper consists of five parts. Part One

[1] Roberta Liggett O'Malley and Karen M. Holt, 'Cyber Sextortion: An Exploratory Analysis Of Different Perpetrators Engaging In A Similar Crime' (2020) 1 Journal of Interpersonal Violence.

[2] 'What Is Sextortion? | Federal Bureau Of Investigation' (*Federal Bureau of Investigation*, 2021) <https://www.fbi.gov/video-repository/newss-what-is-sextortion/view> accessed 3 December 2020; US Legal, Inc. is one of the oldest and largest US companies which offers a variety of services including legal information, legal products, legal forms, and document preparation and like services; 'Cyber extortion Law And Legal Definition | Us legal, Inc.' (*Definitions.uslegal.com*) <https://definitions.uslegal.com/c/cyberextortion/> accessed 4 December 2020.

[3] Anna Brown, 'Sextortion Definition, Sextortion Emails and Help - Cyber Investigations' (*Rexxfield Cyber Investigation Services*, 2021) <https://www.rexxfield.com/sextortion-definition-sextortion-emails-and-help/> accessed 5 December 2020.

[4] Anastasia Powell and others, 'Image-Based Sexual Abuse: The Extent, Nature, And Predictors Of Perpetration In A Community Sample Of Australian Residents' (2019) 92 Computers in Human Behavior accessed 3 December 2020; Maya Oppenheim, 'Scammers Carrying Out Sextortion Cybercrimes During Corona virus' (*The Independent*, 2020) <https://www.independent.co.uk/news/uk/home-news/sex-scam-email-fraud-phishing-cyber-crime-coronavirus-lockdown-a9480806.html> accessed 15 January 2021; 'Online Sextortion: A Cybercrime Increasingly Affecting Employees' (Controlrisks.com, 2021) accessed 3 December 2021.

[5] Government Equalities Office, 'Hundreds of Victims of Revenge Porn Seek Support from Helpline' (2015) <https://www.gov.uk/government/news/hundreds-of-victims-of-revenge-porn-seek-support-from-helpline> accessed 17 December 2020; Tonya Howard, 'Sextortion: Psychological Effects Experienced And Seeking Help And Reporting Among Emerging Adults' (PhD, Walden University 2019); Janis Wolak and others, 'Sextortion of Minors: Characteristics And Dynamics' (2018) 62 Journal of Adolescent Health.

[6] Despite the activism in India relating to online harassment in general including cyber –sextortion, India does not have specific laws on cyber-sextortion and nor

explains the background to and the objectives of the research while Part Two discusses to what extent the existing penal laws in Sri Lanka can be used to prosecute cyber-sextortion. Part Three analyses Australia's laws on cyber-sextortion. Part Four analyses the laws of United States of America on cyber-sextortion. Part Five concludes the paper by making recommendations to Sri Lanka on tackling cyber-sextortion and outlining key elements of a suitable targeted law on cyber-sextortion.

Research Objective and Methodology

The aim of this article is to analyze the adequacy of criminal laws in Sri Lanka in comparison with those of Australia and the United States of America in combating cyber-sextortion and to identify the lessons that Sri Lanka can learn from the said jurisdictions in designing a suitable targeted law on cyber-sextortion. This study is a library-based study involving an analysis of the primary and secondary sources of law in the above-mentioned jurisdictions.

1. Sri Lankan Legislative Framework

Sri Lanka lacks specific laws on cyber-sextortion. In this context, it is pertinent to examine to what extent some of the existing criminal laws in the country can be used to prosecute cyber-sextortionists. On a cursory look, it appears that sections 345, 372, 483 and 286A of the *Penal Code Act* 1883 may be applicable to cyber-sextortion. Section 483 provides that "whoever threatens another with injury to their person, reputation or property etc., with intent to cause alarm or to compel the performance of an illegal act or non-performance of a legal act, commits criminal intimidation". According to section 43 of the Penal Code, the term 'injury' refers to 'any harm whatsoever illegally caused to any person in body, mind, reputation or property'. Since section 483 criminalizes threatening to injure the person, reputation or property of an individual and since cyber-sextortion also involves threatening various harms to a victim including threats to distribute sensitive images, threats to cause physical harms etc., it can be argued that this section is broad enough to cover any type of cyber-sextortion. Although no explicit reference is made to sextortion nor to cyber sextortion, this provision could arguably be applied in cases of cyber sextortion. However, current *mens rea* element of the section may not be broad enough to cover all types of sextortionists as some sextortionists may not have the intentions mentioned in the section but rather just an intent to compel the victim to comply with their demands.

Section 345 on sexual harassment too can be applied to cases of cyber –sextortion. Section 345 provides that whoever by assault or use of criminal force sexually harasses another or by use of words or actions causes sexual annoyance or harassment to such other person commits the offence of sexual harassment. Since cyber sextortion involves using threats to harass a person such as threats of going public with questionable images, etc., it can be argued that cyber sextortion falls within the purview of this section as well. It is

has its existing penal provisions, which are similar to Sri Lanka, have been used to prosecute cyber-sextortion.

notable, however, that when proving a charge under this provision, the prosecution would have to prove that the threats made by the defendant actually caused harassment to the victim. In cyber-sextortion, the act of threatening itself should be sufficient for the commission of an offence irrespective of the impact of such threat on a victim.

Section 372 of the Penal Code which criminalizes extortion can also be used to prosecute cyber–sextortion to a certain extent. It provides that a person is guilty of extortion where he/she puts another in fear of injury and thus induces the other to deliver any property or valuable security or anything signed or sealed which may be converted into a valuable security. This section, arguably, could cover cases of cyber-sextortion which involve a perpetrator threatening to distribute intimate images/videos of a victim or threatening to harm the victim in any other manner unless the latter pays money or provide any property. However, lack of a definition of the term 'property' in the section, casts doubt as to whether intimate images and videos of a victim would constitute property for the purposes of this section. Furthermore, this section would, arguably, not be applicable to certain cases of cyber extortion, namely cases where the demand of a sextortionist comprises of a demand that the victim remains in a relationship with the perpetrator or engages in sexual activities with them.[7]

Section 286A of the Penal Code introduced through the Penal Code (Amendment) Act (No. 22 of 1995) can be regarded as a provision applicable to cyber–sextortion committed against children. The section criminalizes, *inter alia,* persuading, inducing or coercing any child to pose or model for or appear in any obscene or indecent photograph or film, or selling, distributing or having in possession any such photograph or video. The section further provides that a 'child' means a person under the age of 18 years and 'film' includes any form of video recording. Thus, this section can apply to instances of cyber-sextortion where a sextortionist threatens and coerces a child to provide intimate photos or videos of themselves. It can also capture perpetrators who threaten to distribute intimate photos/videos of children as they would have such photos/videos in their possession, and as possession of such items itself is an offence under this section.

In addition to the above, section 4 of the Computer Crime Act No.24 of 2007 which criminalizes unauthorized access to a computer or any information held in a computer knowing or having reason to believe that he has no lawful authority to secure such access and with intention to commit an offence under any law, can also be used in certain cases of cyber-sextortion, i.e., where the sextortionist has obtained victim's images/information through unauthorized access with the intent of committing criminal intimidation, extortion etc. However, the section cannot be used for prosecuting all cases of cyber–sextortion as the conduct criminalized in this section is unauthorized access to information. Similarly, sections 2 and 3 of the Prohibition of Ragging and Other Forms of Violence in Educational

[7] Centre for Policy Alternatives, 'Legal Reform to Combat Sexual and Gender Based Violence' (2020) 25.

Institutions Act No. 20 of 1998 could also be used for prosecution of cyber-sextortion if it involves students and members of staff at educational institutions falling within the scope of this Act. Section 2 of the Obscene Publications Ordinance No. 4 of 1927 which criminalizes, *inter alia*, making, producing or having in possession for trade purpose/for distribution/for public exhibition, obscene writings, drawings, prints, photographs, cinematographs etc. too could arguably be used for prosecuting instances of cyber-sextortion involving threats to distribute sexually explicit images. As the perpetrator in such cases would have sexually explicit/intimate images/videos in their possession for the purpose of distribution or public exhibition, their conduct would fall within the purview of this section.

2. Australian Legal Framework

Unlike Sri Lanka, Australia, both at federal and at state level has laws which are applicable to cyber-sextortion.[8] At Commonwealth level, there are several legislative provisions which criminalize several types of conduct that amount to crimes taking place in virtual platforms. Accordingly, the Commonwealth Criminal Code of 1995[9] criminalizes several types of conduct which can be interpreted to cover instances of cyber-sextortion. Section 474 (17) provides that a person is guilty of an offence if the person uses a carriage service[10] and he or she does so in a way that reasonable persons would regard as being, menacing, harassing or offensive. As cyber–sextortion can be regarded as using the digital technologies in a menacing way, this section can apply to cyber-sextortion as well. In a recent case, a 29-year-old from New South Wales was charged for using a carriage service to menace, harass or cause offence.[11] He was also charged for distributing/threatening to distribute intimate images under the relevant New South Wales legislative provisions (see below). The offender in this case had allegedly created a fake Facebook and Instagram account on which he posted images of his former partner. He also allegedly made threats to the woman that he would distribute her nude images on social media, and demanded money from her to remove the images.[12]

In 2018, the Enhancing Online Safety Act 2015 (as amended by the Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Act 2018), further developed the said provision by inserting a new section 474.17A on aggravated offences involving private sexual material using a carriage service to menace, harass or cause offence. Unlike section 474.17, the new section explicitly refers to dealing with "private sexual material" which is interpreted to include material that depicts a person (who is 18 years of age or older) who is engaged in a sexual pose/sexual

[8] See for instance sec 41DB of the Summary Offences Act of 1966 (VIC), section 91R (2) of the Crimes Act 1900 (NSW), section 208AC of the Criminal Code Act 1983(NT), section 72E of the Crimes Act 1900 (ACT), section 26DA of the Summary Offences Act 1953(SA) and section 338A of the Criminal Code Act Compilation Act 1913 (WA).

[9] Janis Wolak and others, 'Sextortion of Minors: Characteristics and Dynamics' (2018) 62 Journal of Adolescent Health.

[10] In the federal Criminal Code Act a 'carriage service' is given the same meaning it has in the Telecommunications Act 1997 and means 'a service for carrying communications by means of guided and/or unguided electromagnetic energy.'

[11] Nicola Henry, Asher Flynn and Anastasia Powell, 'Responding To 'Revenge Pornography': Prevalence, Nature And Impacts' (2019).

[12] ibid.

activity or material of dominant character which is a depiction of a sexual organ/region of such person, under such circumstances that reasonable persons would regard as giving rise to an expectation of privacy.[13] Accordingly, a person commits an offence against section 474.17A where he or she commits an offence against section 474.17(1) which involves the transmission, making available, publication, distribution, advertisement or promotion of private sexual material. In a more recent case in March 2019, a 25-year-old man was sentenced to one year and 25 days' imprisonment by the District Court of South Australia for distributing intimate videos and images of a former partner and threatening to send the intimate content to her family and post it on social media and pornographic websites. In this case the charges were made under section 474.17of the Criminal Code Act 1995 (Cth) for using a carriage service to menace, harass or cause offence and under section 474.17A of the Code for aggravated use of a carriage service to menace, harass or cause offence involving the distribution of private sexual material.[14]

Moreover, subdivisions D and F of section 474 under the Criminal Code of 1995 criminalize offences relating to the use of carriage service for child pornography/abuse material[15] and offences relating to use of carriage service involving sexual activity with a person under 16.[16] Thus, in cyber-sextortion cases where a minor is involved the above provisions could be utilized since coercing or threatening a minor to perform sexual favours or withholding such material to compel the performance of some other favour can be regarded as a form of using carriage service for child abuse/pornography material or that involving a sexual activity. E.g.: -In 2020, 24-year-old Kurtis Whaley, was sentenced to a maximum nine years and six months in jail, by the NSW District Court for online sextortion of 49 children. The offender was charged for: using a carriage service to solicit child pornography material contrary to section 474.19(1) of the Criminal Code; using a carriage service to transmit child pornography material contrary to section 474.19(1); and using a carriage service to engage in sexual activity with a person under 16 years old contrary to section 474.25A(1) of the Code.[17]

In addition, the Enhancing Online Safety Act of 2015 (as amended by the Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Act 2018) has created a civil penalty scheme to address image based abuses including threats of distributing intimate images. Accordingly, sec 44B of Act provides that a person must not post or make a threat to post an intimate image of another person on a social media service etc.,and stipulates 500 penalty units as punishment for such conduct. This Act also allows a victim of image abuse to make a complaint to the eSafety commissioner and get the abusive image or video

[13] Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Act 2018, schedule 2.

[14] "Adelaide Resident Jailed for International 'Sextortion' Offences." Australian Federal Police, 16 Mar. 2021, www.afp.gov.au/news-media/media-releases/adelaide-resident-jailed-international-'sextortion'-offences.

[15] Criminal Code of 1995 (Cth), ss. 474.19, 474.20, 474.22 & 474.23.

[16] ibid. ss 474.25A-474.27A.

[17] "Adelaide Resident Jailed for International 'Sextortion' Offences." Australian Federal Police, 16 Mar. 2021, www.afp.gov.au/news-media/media-releases/adelaide-resident-jailed-international-'sextortion'-offences.

removed. Turning to state laws, it can be seen that many of the states have laws which are explicit and are directly applicable to cyber–sextortion. Out of the different state laws, this paper examines in detail the provisions of New South Wales, Northern Territory, Australian Capital Territory, Western Australia, South Australia and Victoria as they appear to be relatively clearer and more comprehensive in terms of capturing cyber-sextortion than those of other states.

New South Wales (hereinafter referred to as NSW), Northern Territory (hereinafter referred to as NT) and Australian Capital Territory (hereinafter referred to as ACT) have almost identical provisions on cyber-sextortion contained respectively in section 91R (2) of the Crimes Act 1900 (NSW)[18], section 208AC of the Criminal Code Act 1983 (NT)[19] and section 72E of the Crimes Act 1900 (ACT).[20] The essence of these provisions is that a person who threatens to distribute an intimate image of another person without the consent of the other person, with intention to cause that other person to fear that the threat will be carried out, is guilty of an offence. Existence of the image for real and actual fear that the threat would be carried out is immaterial for the commission of the offence. The threat may be made by any conduct, and may be explicit or implicit, and conditional or unconditional. The term "distribute" is defined to include sending, supplying, exhibiting, transmitting or communicating to another person or making available for viewing or access by another person, whether in person or by electronic, digital or any other means.[21] These provisions can clearly capture cyber-sextortionists who threaten to distribute intimate images of a person irrespective of what they demand from the victim. However, cyber-sextortionists who threaten other harms to victims such as physical harms may not fall within the purview of these provisions.

In terms of the requisite *mens rea*, NSW and the NT require intention to cause fear that the threat would be carried out while in ACT the mental element can either be intention or recklessness. Thus, in ACT the offence is broader in scope and is capable of capturing even those sextortionists who may have an intent to gain a benefit or intent to compel compliance by the victims and be indifferent as to whether any fear is caused in the victim.

In Western Australia (hereinafter referred to as WA) section 338A of the Criminal Code Compilation Act 1913[22] provides that any person who makes a threat with intent to gain a benefit or to cause a detriment to another or to prevent performance of a legal act or to compel the performance of an illegal act, is guilty of a crime. Sec 338 defines the term 'threat' to include a threat to cause any harm or detriment to any person or property including distribution of intimate images of any person other than the distributor.[23] The term distribute is defined in section 221BC to include a range of ways in which distribution can occur including 'making the image available for access by electronic or other means' such as by posting on social media, uploading to

[18] Crimes Act 1900 (ACT).
[19] Criminal Code Act 1983 (NT).
[20] Crimes Act 1900, s 72E.
[21] Crimes Act 1900, s 91N; Criminal Code Act 1983, s 208AA.
[22] Criminal Code Act Compilation Act 1913 (WA), s 338A.
[23] ibid s 221BA.

websites etc. It is evident that these provisions, read together, can clearly apply to cyber-sextortion cases involving threats of distributing intimate photos as well as threat of other harms. Since the requisite *mens rea* under this section includes intent to gain a benefit it could be argued that this is broad enough to capture all types of cyber-sextortionists as they all would have an intention of gaining some benefit whether in the form of more intimate images, money, sexual favours or otherwise.

Under section 26DA of the Summary Offences Act 1953 of South Australia, it is an offence to threaten to distribute an invasive image/an image obtained by the indecent filming of a person. The requisite mental element can either be intention or recklessness as to the fear of carrying out the threat, which is similar to the standard of *mens rea* required by the Crimes Act 1900 of ACT. Accordingly, the said provision can also be used to prosecute a cyber sextortionist. E.g.: - Where a person demands another (subject) to perform certain sexual acts and threatens to post a sensitive video/image of the subject on his/her Facebook page in the event of failing to comply with the demand, the person commits an offence under this section.

Victoria introduced the offence of sextortion to the Summary Offences Act of 1966 through the Crimes Amendment (Sexual Offences and Other matters) Act of 2014. Accordingly, section 41DB of the Summary Offences Act criminalizes the threat to distribute an intimate image that is "against community standards of acceptable conduct" and imposes a penalty of one-year imprisonment. Furthermore, to be held liable for the offence, the perpetrator must intend the victim to believe that the perpetrator will carry out the threat.[24] The "Community standards of acceptable conduct", in relation to the distribution of an intimate image, is defined to include standards of conduct relating to various factors including: the nature and content of the image; the circumstances in which the image was captured, the circumstances in which the image was distributed; the age, intellectual capacity, vulnerability or other relevant circumstances of a person depicted in the image; and the degree to which the distribution of the image affects the privacy of a person depicted in the image.[25] Moreover, in today's context the term "distribute" is mostly used to cover instances where the distribution was carried out in cyber space. Thus, this provision can be interpreted to cover instances of cyber sextortion effectively

3. Legal Framework Of USA

The Justice Department of United States has labeled sextortion as the most serious and the fastest growing cyber threat to children, with more minor victims per offender than all other sexual exploitation offences and the existing research on the subject has further revealed that the majority of victims of cyber-sextortion are females and are under 18 years of age.[26] Recognizing the prevalence and the grave

[24] Crimes Amendment (Sexual Offences And Other Matters) Act 2014 s.41DB(1)(c) .
[25] ibid s 24.

[26] *Sexual Extortion And Nonconsensual Pornography* (ICMEC 2018) <https://www.icmec.org/wp-content/uploads/2018/10/Sexual-Extortion_Nonconsensual-Pornography_final_10-26-18.pdf> accessed 22 June 2021.

nature of the crime, most states in the USA have enacted legal provisions to protect the victims of cyber-sextortion and prosecute perpetrators. More than twenty states have enacted specific laws on sextortion which encompass both offline and online aspects of the offence. Rest of the states, while recognizing cyber-sextortion as a crime, have chosen to rely on non-specific, general legal provisions in order to prosecute perpetrators.

At the federal level, a number of provisions of Unites States Code (hereinafter referred to as U.S. Code) such as sections 2251, 2252, 2252A and 2422(b) of title 18 of U.S. Code which are related to child pornography and 875(d) of title 18 of U.S. Code on extortion can be identified as the most used provisions in cyber-sextortion cases.[27]

Section 2251 makes it illegal to persuade, induce, entice, or coerce a minor to engage in sexually explicit conduct for purposes of producing visual depictions of that conduct. Section 2252 too creates a range of offences relating to child pornography such as transmission in interstate and foreign commerce visual depictions of minors engaging in sexual activities, reproducing such material which have been transmitted in interstate or foreign commerce etc. Section 2252A prohibits *inter alia* transporting, receiving, distributing, reproducing material constituting or containing child pornography through any means or facility of interstate or foreign commerce such as the internet. Section 2422(b) deals with the coercion or the enticement of a minor to engage in illegal sexual activity such as prostitution or other criminal sexual acts. In the process of committing cyber-sextortion, perpetrators may in certain cases engage in conduct criminalized by these provisions, for instance some cyber-sextortionists may coerce minor victims to produce or appear for sexually explicit images/videos etc, some may create content depicting minors engaging in sexual activities and transmit them interstate. Thus, although these provisions do not directly criminalize the conduct of cyber-sextortion, they have been used in the United States in prosecuting cyber-sextortionists.

In addition to the above, other provisions such as section 223 of chapter 47 of U.S. Code, and section 2261A of title 18 of U.S. Code can be used in order to prosecute cyber-sextortionists. Section 223 of chapter 47 of U.S. Code prohibits the transmission of obscene or child pornographic communications with intent to harass another person. Since cyber-sextortion includes transmission of sexually explicit content of the victim to if the victim does not comply to the perpetrator's demands, this provision can be used. Additionally, this provides room for the prosecution of cyber-sextortionists whose victims are minors. Section 223 of chapter 47 of the U.S. Code which is on stalking can also be applied in prosecuting cyber-sextortionists as cyber-sextortion can often include the stalking of the identified victims.

The federal statutes governing hacking or appropriation of social media accounts have also been used to prosecute sextortion

[27] Benjamin Wittes, Cody Poplin and Clara Spera, 'Sextortion: Cybersecurity, Teenagers, And Remote Sexual Assault' (*Brookings*, 2016) <https://www.brookings.edu/research/sextortion-cybersecurity-teenagers-and-remote-sexual-assault/> accessed 15 June 2021.

activities.[28] These are the federal identity theft and aggravated identity theft provisions recognized under sections 1028 and 1028A of Title 18 of the U.S. Code. These have become relevant as perpetrators of cyber-sextortion use fake names and fake social media accounts, sometimes pretending to be someone else who is popular and known to the victim, in order to build a connection with the victim. Computer Fraud and Abuse Act (18 U.S.C. section 1030) can be used in instances where the perpetrator accesses the victim's computer in an unauthorized manner and makes a threat to damage such computer or the data protected in it, in return for money or something of value.

Section 875(d) of Title 18, U.S. Code[29] being the federal interstate extortion statute, is the most used legal provision concerning cyber-sextortion cases of adult victims.[30] This section criminalizes transmission (in interstate or in foreign commerce) of any communication containing a threat of injury to the property or reputation of another person or the reputation of a deceased person, or a threat to accuse another person of a crime, with intent to extort. As this provision criminalizes transmitting threats of injury to property or reputation with intent to extort, and as it also does not specify what the extortionist has to demand from the victims, the section is quite broad in its scope. Thus, it can encompass any type of cyber-sextortion including cases involving threats of distributing sensitive images of a victim and threats of causing physical injuries to the victim.

In the U.S. these provisions have been effectively used in combination with each other to prosecute cyber-sextortionists. For example, in *United States v Killen,*[31] Patrick Killen Jr. coerced teenage boys via different internet chat applications to send him sexually explicit images and later blackmailed them to send additional sexually explicit images. He also traded images and videos thus obtained with other individuals. He was convicted of production of child pornography in violation of section 2251(a), distribution of child pornography in violation of section 2252(a)(2), possession of child pornography in violation of section 2252(a)(4) and transmission of interstate threats in violation of section 875(d).[32]

In the infamous case of *United States v Jared James Abrahams*[33] which concerned the former Miss Teen USA, Cassidy Wolf and a group of other young women, the perpetrator used malware and other computer tools to hack and operate the victims' webcams without their consent. He made threats of publicly posting the photos or videos to the victims' social media accounts unless they sent more nude photos and videos. He was charged with computer hacking under section 1030 of Title 18 of

[28] (*Hg.org*) <https://www.hg.org/legal-articles/sextortion-should-it-be-a-federal-crime-53756> accessed 15 June 2021.

[29] "Whoever, with intent to extort from any person, firm, association, or corporation, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to injure the property or reputation of the addressee or of another or the reputation of a deceased person or any threat to accuse the addressee or any other person of a crime, shall be fined under this title or imprisoned not more than two years, or both."

[30] Benjamin Wittes and others (n 26).

[31] (1:15-cr20106) (2018).

[32] 'South Florida Man Who Engaged In "Sextortion" Sentenced To 139 Years In Prison' (*Justice.gov*, 2015) <https://www.justice.gov/usao-sdfl/pr/south-florida-man-who-engaged-sextortion-sentenced-139-years-prison> accessed 23 June 2021.

[33] (8:13-cr-00199) (2013).

the U.S. Code for unauthorized access of protected computers and extortion under section 875(d).

In *United States v Lucas Michael Chansler*,[34] another sextortion case, Chansler victimized hundreds of children in a grooming and sextortion scheme. He gained the trust of the victims through social networking websites such as Facebook and Myspace by being friends with them using different online screen names. While engaging in live chats he coerced the victims to expose themselves which he secretly recorded. He then threatened to send such images and videos to their family and friends if they did not comply with additional demands for sexually explicit content. Chansler was charged under section 875(d) as he knowingly and willfully transmitted threats to injure the reputation of the addressee with the intent to extort things of value. As he coerced the minors to engage in sexually explicit conduct for the purpose of producing such visual depictions and transported them via the internet, he was charged under section 2251(a) and (e) and section 2252.

In *United States v Richard Leon Finkbiner*[35] the defendant used websites like omegle.com[36] to engage in video chats sessions. The perpetrator coerced the minors to engage in sexually explicit conduct and recorded videos of them doing so using screen capture software. He then threatened to post them and the victims' identities on pornography platforms unless they performed sexual acts for him via the webcam. He sextorted thousands of images and videos from a number of minors and adults from around the country for over a year. He was charged with sexual exploitation of children under section 2251, producing child pornography under section 2252, possession of child pornography under section 2252 and interstate extortion under section 875(d).

In a recent case in the state of Minnesota,[37] Mitchell James Ottinger had created and used multiple internet accounts to encourage and direct minors and an adult to create sexually explicit images and videos of themselves. He had also posed as a young female in order to obtain the said images and videos. He had thereafter threatened to publish sexually explicit images of the victims to others unless additional demands for sexually explicit images were not met. Ottinger was charged with production and attempted production of child pornography under section 2251(a) and (e) of Title 18 of the U.S. Code and making extortionate threats under section 875(d) of Title 18 of the U.S. Code in the federal court.[38]

As evident from these cases, although some of the above-mentioned provisions may not be able to cover all instances of cyber-sextortion on their own, taken together with provisions such as section 875(d) on extortion, they appear to have been quite

[34] (3:10-cr-00100) (2010).
[35] (2:12-cr-00021) (2013).
[36] Omegle is a free online chat website that allows users to socialize with others without the need to register. The service randomly pairs users in one-on-one chat sessions where they chat anonymously using the names 'You' and 'Stranger.'

[37] *United States of America v Mitchell James Ottinger* 21-MJ-340(ECW) (2021).
[38] 'Substitute Teacher Charged In "Sextortion" Case' (*Justice.gov*, 2021) <https://www.justice.gov/usao-mn/pr/substitute-teacher-charged-sextortion-case> accessed 25 June 2021.

effective in brining cyber-sextortionists to justice.

Combatting cyber-sextortion at State Level

Recognizing the necessity of addressing cyber-sextortion through legal provisions, a number of states such as Utah, Arkansas, Pennsylvania and California have enacted targeted laws addressing cyber-sextortion. While these states have enacted specific laws on cyber-sextortion, other states rely on non-specific legal provisions such as those on extortion, blackmail, sexual exploitation, sexual assault and stalking to prosecute perpetrators of cyber-sextortion. This part of the article examines the laws of a few states which have targeted laws on cyber sextortion and how well each state has succeeded in implementing the laws to tackle the offence.

Utah and Arkansas: Section 76-5b-204(2) of Utah Criminal Code criminalizes communicating in person or by electronic means a threat to the person, property or reputation of another person or a threat to distribute intimate images/videos of a victim with intent to coerce such victim to engage in sexual contact, in sexually explicit conduct, or in simulated sexually explicit conduct, or to produce, provide, or distribute an image, video, or other recording of any individual naked or engaged in sexually explicit conduct.

The State of Arkansas as well has provisions against sexual extortion in section 113, chapter 14, Title 5 of the Arkansas Code which are quite similar to those of Utah. This provision criminalizes conduct such as communicating a threat to damage the property or reputation of another person or to produce or distribute a recording of the other person engaged in sexually explicit conduct or depicted in a state of nudity with the purpose, *inter alia,* of coercing such person to engage in sexual contact or sexually explicit conduct etc.

These legal provisions of Utah and Arkansas are evidently quite broad and are capable of capturing a range of conduct that falls within the purview of the term cyber-sextortion. The reference to communication 'by electronic means' in section 76-5b-204(2) of Utah Criminal Code, makes clear the applicability of the provision to threats made through cyber space. Even though Arkansas does not specify the online aspect of the crime, the provision provides space to cover both the online and offline aspects. However, these provisions may not be able to capture cases where the demand of the perpetrator does not relate to engaging in sexual/sexually explicit conduct or producing/providing/distributing material containing such content. For instance, a case where a perpetrator threatens to distribute sexually explicit images of a victim unless the victim pays money cannot be captured by these provisions as it may not be possible to prove the requisite mental element.

Pennsylvania: The Pennsylvania Act 100 of 2019 amending Title 18 of the Pennsylvania Consolidated Statutes introduced the offence of sexual extortion in the year 2020. This law makes sexual extortion a third-degree felony,[39] if the

[39] A conviction for a felony in the third degree in Pennsylvania includes from 2.5 to 7 years in prison and a fine of up to $15,000.

victim is under 18 or the perpetrator has shown a pattern of engaging in sexual extortion. The law defines sexual extortion as using a threat of some type to coerce a victim to (i) engage in a sexual conduct, simulate a sexual conduct or a state of nudity or (ii) make / produce / disseminate / transmit or distribute any image / video/ recording depicting the victim engaging in a sexual act/simulation of a sexual act or state of nudity. Section 3133(b) sets out the different means by which the offence of sexual extortion can be committed such as by harming or threatening to harm the property or reputation of the complainant, by threatening to produce / disseminate / distribute sexually explicit / nude images / videos etc. of the complainant, threatening to withhold a service, employment, cause a loss, disadvantage, injury etc. Subsection (c) further provides that sexual extortion is committed where a person solicits/demands money/property/service/something of value to remove sexually explicit/nude material of the complainant from public view or for preventing disclosure of such material, or where a person disseminate/distribute or threatens to disseminate/distribute sexually explicit / nude material of the complainant and demands/solicits money etc. for removal of such content from public view or to prevent dissemination of such content. The definitions provided in the Act state that such transmission of the threat can be either an electronic communication or an actual communication covering both online and offline aspects.

The Pennsylvanian provision by far appears to be the most comprehensive state law in terms of encompassing almost all types of sextortion.

Texas: Section 21.18 of the Texas Penal Code creates the offence of sexual coercion and provides for two aspects of the offence in subsections (b) and (c). Subsection (b) provides that a person commits an offence if he/she intentionally threatens to commit an offence under chapter 43 of the Penal Code to obtain, intimate visual material, or an act involving sexual conduct causing arousal or gratification, or a monetary benefit or other benefit of value. Offences under chapter 43 of the Penal Code includes invasive visual recording, unlawful disclosure or promotion of intimate visual material, voyeurism, sexual assault, aggravated sexual assault etc. Thus, this subsection can clearly capture instances of cyber-sextortion which involve threats of distributing sexually explicit videos/images of victims unless the victim complies with the demands of the perpetrator.

Subsection (c) provides that a person commits an offence if he/she intentionally threatens to commit an offence under chapters 19 or 20 or section 20A.02(a)(1), (2), (5), or (6) in order to obtain, in return for not committing the threatened offence or in connection with the threatened offence, intimate visual material or an act involving sexual conduct causing arousal or gratification. The offences under chapters and sections above mentioned include criminal homicide, kidnapping, unlawful restraint, smuggling of persons and trafficking of persons. This subsection can cover cases of cyber-sextortion not covered by subsection (b), i.e., cases where the threat relates to causing physical harm to the victim or another person.

This provision applies to a threat regardless of how that threat is communicated and therefore covers threats transmitted through

email, websites, social media, chatrooms and other electronic or technological means.[40]

California: The California legislature extended their general extortion provision under section 518 Penal Code, in 2018 to include the elements of sextortion as well. The offence of extortion is defined in section 518(a)[41] to include, among other things, the obtaining of property or other consideration from another, with his or her consent, in order to capture the elements of sextortion, subsection 518(b) provides that "consideration" means anything of value including sexual conduct or an image of an intimate body part. A person charged under sextortion faces the same charge as a person who commits extortion and the punishment for sextortion ranges from two to four years. California exempts persons under the age of eighteen from being charged with sextortion.

Minnesota: State of Minnesota currently does not have specific provisions on sextortion but is in the process of passing a bill which intends to make it a felony to extort sex from someone. Extortion is identified as coercion under section 609.27 of the Penal Code which provides that whoever makes various threats including threats to expose a secret or deformity / publish a defamatory statement/expose a person to disgrace/ridicule, and thereby causes another against their will to do any act or forbear doing a lawful act, commits the offence of coercion.

The above-mentioned bill proposes to introduce a new offence of sexual extortion which criminalizes engaging in sexual contact with another person by causing the other person to submit to such contact through various threats. This section too could be useful in prosecuting cyber-sextortionists who have actually managed to coerce victims to engage in sexual activities with them using threats. However, the section does not appear to cover cyber-sextortion cases where threats are used to obtain intimate images/videos of victims, money from victims etc.

It is evident from the above discussion that different states of USA have taken different approaches to address the growing problem of cyber-sextortion. When looking at states that have enacted targeted laws, it can be seen that some states such as Pennsylvania have enacted laws that are broad enough to cover all instances of cyber-sextortion. On the other hand, states such as Utah and Arkansas have enacted cyber-sextortion laws which address only specific types of cyber-sextortion. However, some states such as California have seen it fit to simply extend their existing laws on extortion to address both online and offline sextortion.

4. Conclusion and Recommendations

This paper analyzed the adequacy or otherwise of criminal laws in Sri Lanka in comparison of those in Australia and USA in order to combat cyber-sextortion. The analysis revealed that although Sri Lanka

[40] 'Before You Text | Texas School Safety Center' (*Txssc.txstate.edu*) <https://txssc.txstate.edu/tools/courses/before-you-text/module-3-2> accessed 7 July 2021.

[41] " Extortion is the obtaining of property or other consideration from another, with his or her consent, or he obtaining of an official act of a public officer, induced by a wrongful use of force or fear, or under colour of official right. "

lacks targeted laws on cyber sextortion, some of the existing provisions on criminal law, especially, sections 345 (sexual harassment), 372 (extortion),483 (criminal intimidation) and 286A (Obscene publications relating to children) of the Penal Code can be applied in cases of cyber-sextortion to a certain extent. Out of these, section 483 on criminal intimidation appears to be the most comprehensive despite some limitations regarding the *mens rea* element. In addition, it was also seen that certain provisions of the Cyber Crime Act of 2007, Prohibition of Ragging and Other Forms of Violence in Educational Institutions Act of 1998 and Obscene Publications Ordinance No. 4 of 1927 can be applied to cyber-sextortion to a limited extent.

In the case of Australia, it was seen that states have laws which are more explicit and directly relevant to cyber-sextortion. Out of laws in different states, those of New South Wales, Northern Territory, Australian Capital Territory and Western Australia were analyzed in detail. This analysis revealed that the laws of NSW, NT and ACT can apply to cyber sextortion cases involving threats of distributing intimate images, these are incapable of capturing cases involving threats of other harms. Furthermore, it was also seen that the *mens rea* element of the offences of NSW and NT was rather narrow and not capable of capturing certain cyber-sextortionists such as those who are indifferent as to whether any fear was caused in the victim. The relevant law in Western Australia is comprehensive enough to capture cyber-sextortion instances involving not only threats to distribute intimate images/videos but also threats to cause other harms, and the *mens rea* element is also broad enough to capture almost all types of cyber-sextortionists.

The analysis of the laws in the USA revealed that at the federal level, the prosecutions on cyber-sextortion are done relying on general extortion provisions, child pornography laws, hacking and stalking laws. As far as the states are concerned, it was seen that some states such as Utah, Arkansas, Pennsylvania and Texas have enacted targeted laws on cyber-sextortion while some other states have chosen to extend their existing provisions on extortion to cover both online and offline sextortion. A careful observation of the laws of USA both at federal and state levels shows that it is not mandatory to have specific provisions on cyber-sextortion in order to prosecute the perpetrators. In fact, existing laws on extortion, child pornography etc. can, in combination with each other, be successfully used for prosecuting cyber-sextortionists. Child pornography laws are abundantly used as most of the time the victims are minors and sextortion includes the persuasion of such minors to produce pornographic content. Generally, sextortion occurs online as a result of hacking of webcams and computers enabling the use of provisions on hacking and stalking.

Until it enacts a specific law on cyber-sextortion, Sri Lanka too should follow the examples of United States and try to use the existing laws to prosecute cyber sextortionists. For instance, in cyber-sextortion cases involving minors, depending on the specific facts of the case, the prosecution can use section 288A which criminalizes, inter alia, coercing or inducing a child for illicit sexual intercourse or section 360B which

criminalizes threatening or using violence towards a child to procure such child for sexual intercourse or any form of sexual abuse along with section 483 on criminal intimidation. In cyber –sextortion cases involving adults, again a combination of provisions such as the hacking provisions in the Computer Crime Act, sexual harassment provisions in the Penal Code along with the provisions on criminal intimidation or extortion could be used.

If Sri Lanka decides to go for a targeted law on this issue, it should either adopt a specific law on cyber-sextortion which is broad enough to cover all aspects of cyber-sextortion or a criminal provision which targets online harassment in general but is broad enough in scope to capture all types of online harassment including cyber-sextortion. If a targeted law on cyber-sextortion is to be adopted, the drafters of such law are recommended to consider the following points. Firstly, the proposed offence should focus on criminalizing the conduct of making a threat to carry out some act unless the person to whom such threat is directed complies with the demands of the maker of the threat. The threat could include but should not be limited to a threat to distribute intimate images/videos of a victim, to harm the victim or someone related to the victim etc. The demand too could include but should not be limited to demands for sexual favours, for money or a demand to start/remain a relationship with the maker of such threat etc. However, for the conduct to be classified as sextortion, the threat or demand should have a sexual dimension. Secondly, it is recommended to have intention to compel the victim to comply with the demands of the perpetrator as the *mens rea* element of the offence. As was seen in the above discussion, having intention to cause alarm or fear that the threat will be carried out as a *mens rea* element can have the effect of some sextortionists falling outside the purview of the law. One may argue that intent to compel compliance with a demand is synonymous to an intention to cause alarm. However, it must be noted that there is a qualitative difference between the two, and that intent to cause alarm involves an intent to cause fear/distress whereas an intent to compel compliance is more about pressurizing or forcing someone to do a particular act rather than causing fear or distress. A sextortionist may intend to force someone into compliance without having an intention to cause any fear/distress in the victim. Thirdly, since the offence relates to sextortion carried out using digital technologies explicit reference should be made in the law to the involvement of digital technologies either for making the threat or carrying out the threatened act. Finally, the offence should carry a penalty sufficient to act as a deterrent to potential perpetrators.

Acknowledgements

This work was supported by the Accelerating Higher Education Expansion and Development (AHEAD) Operation of the Ministry of Higher Education funded by the World Bank.

References

Table of Legislation: Australia

Crimes Act No. 40 of 1900 (NSW)

Crimes Act of 1900 (ACT)

Crimes Amendment (Sexual Offences and Other matters) Act No. 74 of 2014

Criminal Code Act Compilation Act No. 28 of 1913 (WA)

Criminal Code Act No. 12 of 1995 (Vic)

Criminal Code Act No. 47 1983 (NT)

Criminal Code Act No. 69 of 1924 (Tas)

Criminal Code Act No. 9 of 1899 (Qld)

Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Act 2018 (Cth)

Summary Offences Act 1953(SA)

Summary Offences Act No. 7405 of 1966 (Vic)

Table of Legislation: Sri Lanka

Computer Crime Act No. 24 of 2007

Penal Code Act No. 2 of 1883

Prohibition of Ragging and Other Forms of Violence in Educational Institutions Act No. 20 of 1998

Table of Legislation: USA

Title 18 of the United States Code of 1948

Tile 76 of Utah Criminal Code of 1973

Title 5 of Arkansas Code of 1987

Pennsylvania Act 100 of 2019

Penal Code of California of 1872

Title 5 of the Texas Penal Code of 1974

Chapter 609 Penal Code of Minnesota of 1999

Case Law

United States v Jared James Abrahams (8:13-cr-00199) (2013)

United States v Lucas Michael Chansler (3:10-cr-00100) (2010)

United States v Richard Leon Finkbiner (2:12-cr-00021) (2013)

United States v Killen (1:15-cr20106) (2018)

United States of America v Mitchell James Ottinger 21-MJ-340(ECW) (2021)

Secondary sources

AP NEWS, '*Pennsylvania creates criminal offense of sexual extortion*.' [2021] Available at: <https://apnews.com/article/df146d9b0b164d45a2391db34bd9439a> accessed 28 May 2021

A Brown, 'Sextortion Definition, Sextortion Emails and Help - Cyber Investigations' (Rexxfield Cyber Investigation Services, 2021) <https://www.rexxfield.com/sextortion- definition-sextortion-emails-and-help/> accessed 5 December 2020

A Powell *et al*, 'Image-Based Sexual Abuse: The Extent, Nature, and Predictors of Perpetration in a Community Sample of Australian Residents' [2019] 92 Computers in

Human Behavior <https://www.sciencedirect.com/science/article/abs/pii/S0747563218305454?vi a%3Di hub> accessed 3 December 2020

Australian Federal Police – Adelaide, *Resident Accused of International 'Sextortion' Offences'* [2019] Available at <https://www.afp.gov.au/news-media/media-releases/adelaide-resident-accused-international-sextortion-offences> accessed 14 March 2021

'Before You Text | Texas School Safety Center' (*Txssc.txstate.edu*) <https://txssc.txstate.edu/tools/courses/before-you-text/module-3-2> accessed 7 July 2021

B Wittes *et al*, 'Sextortion: Cyber security, Teenagers, And Remote Sexual Assault' (The Brookings Institution 2016) <https://www.brookings.edu/research/sextortion-cyber security-teenagers-and-remote-sexual-assault/> accessed 3 December 2020

Centre for Policy Alternatives, 'Legal Reform to Combat Sexual and Gender Based Violence' [2020]

'Cyber extortion Law and Legal Definition | Us legal, Inc.' (Definitions.uslegal.com) <https://definitions.uslegal.com/c/cyberextortion/> accessed 4 December 2020

Government Equalities Office, 'Hundreds of Victims Of Revenge Porn Seek Support From Helpline' (2015) <https://www.gov.uk/government/news/hundreds-of-victims-of-revenge-porn-seek-support-from-helpline> accessed 17 December 2020

(*Hg.org*) <https://www.hg.org/legal-articles/sextortion-should-it-be-a-federal-crime-53756> accessed 15 June 2021

J Kolls, *'Sextortion' bill would make blackmail for sex a crime in Minnesota*. (KSTP, 2021) Available at:<https://kstp.com/news/sextortion-bill-would-make-blackmail-for-sex-a-crime-in- minnesota/ 6020658 /> accessed 28 June 2021

J Wolak *et al*, 'Sextortion of Minors: Characteristics and Dynamics' [2018] 62 Journal of Adolescent Health <https://www.sciencedirect.com/science/article/abs/pii/S1054139X1730 4238> accessed 3 December 2020

J Wolak, D Finkelhor, 'Sextortion: Findings from A Survey Of 1,631 Victims' (Crimes against Children Research Center, University of New Hampshire 2016) <https://zxh.3cb.myftpupload.com/wp-content/uploads/2018/09/ Sextortion_Report.pdf> accessed 4 December 2020

Malley R, and Holt K, 'Cyber Sextortion: An Exploratory Analysis of Different Perpetrators Engaging In A Similar Crime' [2020] 1 Journal of Interpersonal Violence

Oppenheim M, 'Scammers Carrying Out Sextortion Cybercrimes During Corona virus' (The Independent, 2020) <https://www.independent.co.uk/news/uk/home-news/sex-scam-email-fraud-phishing-cyber-crime - coronavirus-lockdown-a9480806.html> accessed 15 January 2021

N Henry, A Flynn, A Powell, 'Responding To 'Revenge Pornography': Prevalence, Nature and Impacts' [2019] <https:// researchmgt. monash.edu/ws/portalfiles/portal/264678641/08_1516_FinalReport.pdf> accessed 7 March 2021

S Agrawal, 'Online Sextortion' [2020] 6(1) Indian Journal of Health, Sexuality and Culture Available at: <https://www.iisb.org./> accessed 27 May 2021

Scholar.valpo.edu. [2021] Available at:<https://scholar.valpo.edu/cgi/viewcontent.cgi?article=2492&context=vulr> accessed 28 May 2021

Sexual Extortion And Nonconsensual Pornography (ICMEC, 2018) <https://www.icmec.org/wp-content/uploads/2018/10/Sexual-Extortion_Nonconsensual-Pornography_final_10-26-18.pdf> accessed 22 June 2021

'South Florida Man Who Engaged In "Sextortion" Sentenced To 139 Years In Prison' (*Justice.gov*, 2015) <https://www.justice.gov/usao-sdfl/pr/south-florida-man-who-engaged-sextortion-sentenced-139-years-prison> accessed 23 June 2021

'Substitute Teacher Charged In "Sextortion" Case' (*Justice.gov*, 2021) <https://www.justice.gov/usao-mn/pr/substitute-teacher-charged-sextortion-case> accessed 25 June 2021

'Sydney Man Jailed for Online Exploitation and Extortion of Children' [2020]

T Howard, 'Sextortion: Psychological Effects Experienced and Seeking Help and Reporting Among Emerging Adults' (PhD, Walden University 2019)