UNC SCHOOL OF LAW

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 21 | Issue 3 Article 5

3-1-2020

Sextortion: The Hybrid "Cyber-Sex" Crime

Alessandra Carlton

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 21, ISSUE 3: MARCH 2020

SEXTORTION: THE HYBRID "CYBER-SEX" CRIME

Alessandra Carlton*

Sextortion is an increasingly prevalent internet crime, but it is not well-defined or understood. As new technology makes the challenge of combatting sextortion even more difficult, regulators should consider using a broad definition of sextortion to capture the myriad of ways that criminals are extorting victim with their sexual images. This recent development discusses the pervasiveness and methods of the crime, particularly in the context of technology, and the need for federal government action and legislation to promote public awareness of this disturbingly prevalent cyber-sex crime. This article recommends a sextortion attack plan that would involve: (1) enactment of a federal sextortion crime that properly classifies sextortion as a sex crime, (2) federally regulating and negotiating with internet companies to take greater responsibility for sextortion occurring on internet platforms, (3) establishing a non-profit clearinghouse under the federal statute to collect data and provide resources to both victims and law enforcement, and (4) using information gathered from the clearinghouse to create an effective sextortion awareness campaign.

* J.D. Candidate, University of North Carolina School of Law, 2021. The author would like to thank Professor Joseph E. Kennedy for his insight, as well as Erin Larson from the NC JOLT Board of Advisors and all of the NC JOLT editors and staff, particularly Hannah Petersen and Ashle Page, for their assistance throughout the editorial process.

I. INTRODUCTION

One year before Cassidy Wolf was crowned Miss Teen USA, someone hacked into her computer's webcam.[1] The perpetrator was Jared James Abrahams, a nineteen-year-old computer science student and Wolf's former high school classmate.[2] Unbeknownst to Wolf, Abrahams monitored her through the webcam for months and took numerous photos of her undressing in her bedroom.[3] Abrahams emailed Wolf, threatening to post the photos on the internet, including on all of her social media accounts, unless she either sent him sexually explicit photos and videos, or engaged in sexual acts using Skype.[4] At trial, Abrahams pled guilty to three counts of extortion and one count of unauthorized access of a computer.[5] Abrahams admitted that he had access to as many as 150 electronic

[1] Violet Blue, *The FBI Recommends You Cover Your Laptop's Webcam, for Good Reason*, ENGADGET (Sept. 23, 2016), https://www.engadget.com/2016/09/23/the-fbi-recommends-you-cover-your-laptops-webcam-good-reasons/ [https://perma.cc/ZE39-9KL5].

[2] *Id*.; *Miss Teen USA Hacker Pleads Guilty to 'Sextortion' Threats,* BBC (Nov. 13, 2013), https://www.bbc.com/news/technology-24929916 [https://perma.cc/NWQ6-TK45].

[3] Lauren Weigle, *Jared James Abrahams – Cassidy Wolf's Webcam Computer Hacker*, HEAVY. (Mar. 4, 2015), https://heavy.com/entertainment/2015/03/jared-james-abrahams-twitter-cassidy-wolfs-computer-hacker-stalker-webcam-sextortion/ [https://perma.cc/348Z-NS45].

[4] *Id*.

[5] *Id*.

devices belonging to other people.[6] Although Wolf ignored Abrahams' threats, at least two of his victims complied with the demands.[7] Abrahams was sentenced to eighteen months in prison.[8]

Cassidy Wolf was a victim of sextortion.[9] Sextortion is a cybercrime that occurs when a perpetrator obtains or claims to possess a victim's sensitive material, usually through false pretenses or computer or webcam hacking, and threatens to distribute the material unless the victim "provide[s] them images of a sexual nature, sexual favors, or money."[10] The material used to blackmail victims is personal in nature, typically sexual images or videos of the victim,[11] but the sextortionist may also threaten some other harm to the victim.[12] Perpetrators of sextortion, or "sextortionists," often obtain these through: (1) false pretenses on social media (also known as "catfishing"),[13] (2) hacking the photos stored on the

---

[6] Greg Botelho, *Arrest Made in Miss Teen USA Cassidy Wolf 'Sextortion' Case*, CNN (Sept. 27, 2013), https://www.cnn.com/2013/09/26/justice/miss-teen-usa-sextortion/index.html [https://perma.cc/M2G3-BE3B].

[7] *Miss Teen USA Hacker Pleads Guilty to 'Sextortion' Threats, supra* note 2.

[8] Botelho, *supra* note 6.

[9] Cassidy Wolf has become one of the most famous sextortion victims to date. Her case is repeatedly referenced in sextortion dialogue, and during her time as Miss Teen USA, she used her platform to publicly advocate for sextortion victims. SELLING "SLAVING", DIGITAL CITIZENS ALLIANCE 1, 3, 11 (July 2015), https://media.gractions.com/314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/07027202-8151-4903-9c40-b6a8503743aa.pdf [https://perma.cc/4ML8-UJDU].

[10] *What is Sextortion?*, FED. BUREAU INVESTIGATION, https://www.fbi.gov/video-repository/newss-what-is-sextortion/view [https://perma.cc/DU7Y-4NVS]; Benjamin Wittes et al., *Sextortion: Cybersecurity, Teenagers, and Remote Sexual Assault*, BROOKINGS INST. (May 11, 2016), https://www.brookings.edu/research/sextortion-cybersecurity-teenagers-and-remote-sexual-assault/ [https://perma.cc/E6U4-UKDF].

[11] Wittes et al., *supra* note 10.

[12] *See What is Sextortion?*, *supra* note 10 ("The perpetrator may also threaten to harm your friends or relatives by using information they have obtained from your electronic devices unless you comply with their demands."); *see also* Wittes et al., *supra* note 10 ("One young sextortion victim complied with demands for nude photos because her attacker threatened to 'blow up' her computer if she did not, and the computer was a treasured new Christmas present.").

[13] *See* Dan Whitworth, *Sextortion: Big Rise in Victims With 'Tens of Thousands at Risk'*, BBC (May 24, 2018), https://www.bbc.com/news/newsbeat-43433015 [https://perma.cc/N7AW-D329] (describing a male victim who, thinking the

victim's electronic devices or social media accounts,[14] or (3) remote webcam hacking, like in Wolf's scenario, in which the sextortionist covertly creates the blackmail material.

This article will discuss the pervasiveness of sextortion crimes and the possible inadequacy of legal redress for its victims, as well as the continued technological difficulties of sextortion and the need for social awareness to promote sextortion prevention. Part II will introduce sextortion methods, illustrations, and statistics to show the pervasiveness and profitability of the crime, as well as discuss some societal misunderstandings about sextortion and its victims. Part III will explain existing and proposed laws on sextortion and will discuss the pros and cons of separating sextortion from more general extortion or "revenge porn" crimes in federal law. Part IV will discuss how technology has played a key role in the issues surrounding sextortion and tech companies' possible role in its demise. Part V will examine tactics for prevention and societal awareness.

II. SHEDDING LIGHT ON SEXTORTION

In reality, there is no consensus on the definition of sextortion. There are two popular approaches to defining sextortion: (1) sextortion is when a perpetrator threatens to share a victim's private sexual images in order to extort something from them,[15] or (2) sextortion is when a victim is coerced into sending sexual material to the perpetrator, either through the threat of sharing private sexual images or some other threat of harm.[16] The first view can diverge in scope depending on whether the perpetrator must actually possess

---

sextortionist was a woman romantically interested in him, was tricked into masturbating on webcam, recorded, then threatened with the release of the footage).

[14] *See* Emily J. Sullivan, *Whitney Cummings Responds to Extortion Threat by Posting a Photo of Her Breast*, HOLLYWOOD REP. (Aug. 13, 2019), https://www.hollywoodreporter.com/news/whitney-cummings-posted-a-photo-her-breast-response-extortion-threats-1231319 [https://perma.cc/BB88-QHLP] (describing how Cummings photos that she had personally taken were hacked by a sextortionist).

[15] *See What is Sextortion?*, *supra* note 10.

[16] *See* Wittes et al., *supra* note 10.

the images or merely claim to possess the images.[17] This article has adopted a broad view, combining the two popular approaches. But, throughout the discussion of various fact patterns, a reoccurring issue arises as to how lawmakers differ on willingness to define this crime in order to hold perpetrators accountable.

A. The Crime: Sextortion vs. Revenge Porn

Sextortion and "revenge porn" are sometimes conflated by scholars, media, and the general public; however, while these crimes are often interconnected, they are not interchangeable. Revenge porn, which is less popularly, but more accurately called "nonconsensual porn," is the nonconsensual distribution of a victim's pornographic material.[18] The connection between the two crimes that contributes to their confusion is that sextortion is often a threat to commit revenge porn[19] against a victim, unless that victim complies with something demanded of them. Sextortion and revenge porn are both sex-related internet crimes, but unlike revenge porn, coerced silence is a key player in the success of sextortion.[20] If a sextortionist possesses a victim's private material, the sextortionist will not automatically publish it because the objective is usually to obtain sexual material or money, and the victim's

---

[17] This tends to come up in the mass-produced phishing sextortions. *See generally* Thomas Brewster, *Lying Sextortion Scammers Score $250,000 After Sending Victims Their Own Hacked Passwords*, FORBES (July 31, 2018), https://www.forbes.com/sites/thomasbrewster/2018/07/31/sextortion-scam-with-hacked-passwords-scores-250000-dollars-for-cybercriminals/#41edeff0df16 [https://perma.cc/6L34-HPKC] (describing how scammers use old passwords to trick people into believing their personal material is at risk).

[18] *See* Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1918 (2019); *see also 46 States + DC + One Territory Now Have Revenge Porn Laws*, CYBER CIVIL RIGHTS INITIATIVE (2019), https://www.cybercivilrights.org/revenge-porn-laws/ [https://perma.cc/6HPU-K3HY] ("The term 'revenge porn,' though frequently used, is somewhat misleading. Many perpetrators are not motivated by revenge or by any personal feelings toward the victim. A more accurate term is nonconsensual pornography (NCP), defined as the distribution of sexually graphic images of individuals without their consent.")

[19] As previously discussed, sextortion typically, but does not always, include a threat to disseminate the victim's private sexual images. *See* Wittes et al., *supra* note 10.

[20] *See* Citron, *supra* note 18.

silence and fear of embarrassment is crucial to achieving that goal. In contrast, for revenge porn, the offender's objective is to publish the victim's sexual material, and the victim's silence does not play a major role in achieving this goal. These crimes have been treated distinctly by the law, which will be addressed in more detail below.

B. Methods of Sextortion and the Black-Market Business

"Catfishing" is a common method of sextortionists that is used to trick victims into willingly sending sexual material[21] or covertly record the victims as they engage in sexual acts.[22] Victims are targeted through fake profiles on social media sites like Facebook or dating apps like Tinder and OkCupid.[23] In one instance, an unidentified sextortionist, posing as a woman, connected with a male victim on OkCupid and began sending him sexually suggestive messages.[24] Believing the sextortionist was romantically interested, the victim agreed to engage in "cybersex" with her via Skype.[25] The sextortionist covertly recorded sexually explicit videos of the victim, and threatened to send them to his family and place of work.[26] Another sextortionist, Christopher Patrick Gunn, targeted underage girls by using a fake Facebook profile in which he pretended to be a "new kid in town," befriended them, and convinced them to send him nude photos.[27] He also posed as popular singer Justin Bieber on Omegle, a web-based video-chat platform, and tricked young fans into sending him nude photos by promising free concert tickets or backstage passes.[28]

---

[21] Wittes et al., *supra* note 10.

[22] *See* Kari Paul, *'I Was Humiliated' — Online Dating Scammers Hold Nude Photos for Ransom in 'Sextortion'*, MARKETWATCH (Aug. 23, 2019), https://www.marketwatch.com/story/i-was-humiliated-online-dating-scammers-hold-nude-photos-for-ransom-in-sextortion-attacks-2019-03-06 [https://perma.cc/H6SZ-FHB7].

[23] *Id*.

[24] *Id*. (noting the victim did not report the crime and the actual identity of his sextortionist is unknown).

[25] *Id*.

[26] *Id*.

[27] Wittes et al., *supra* note 10.

[28] *Id*.

Email phishing schemes and malware are common ways for sextortionists to hack a victim's webcam, computer files, or social media accounts. A recipient of a phishing email is either deceived into unveiling personal information, such as account numbers or passwords, or unknowingly downloading infectious malware, which gives the sender access to personal files.[29] One sextortionist created a phishing scheme in which he posed as an employee of Google to obtain passwords from his victims, which he then used to hack their accounts and steal sensitive photos and other personal information.[30] Another sextortionist, Luis Mijangos, tricked "scores" of young women and girls into downloading a malware that granted him access to all of the files on their computers, as well as access to webcams and microphones.[31] In particular, many sextortionists use malware known as a Remote Access Trojan ("RAT").[32] RAT malware enables sextortionists like Mijangos to take control of an unsuspecting victim's computer in a practice referred to as "slaving."[33]

Although many victims comply with sextortionists' demands in order to prevent public disclosure of their intimate material, compliance does not necessarily stop offenders from profiting off of this invasion of privacy.[34] Hackers like Mijangos, often called

---

[29] *How to Recognize and Avoid Phishing Scams*, FED. TRADE COMM'N (May 2019), https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams [https://perma.cc/UDX3-7JP6].

[30] Wittes et al., *supra* note 10 ("Ford had successfully hacked into 450 computers and threatened 75 victims at the time of his arrest.").

[31] *Id*. Luis Mijangos watched, listened, and recorded his victims; he was able to track when they had viewed his threatening messages and see everything they typed on their keyboards. *Id*. Mijangos kept detailed logs of his victims' personal information, and "investigators found more than 15,000 webcam-video captures, 900 audio recordings, and 13,000 screen captures on his computers." *Id*.

[32] SELLING "SLAVING", *supra* note 9 (Cassidy Wolf's sextortionist was also a ratter, and he slaved the devices of 150 victims.).

[33] *Id*. at 6 ("Perhaps the simplest and most popular slaving tool is a RAT. One of the six kinds of Trojans, RATs are malicious code that can be disguised as documents, photographs, videos, and songs to trick targets into downloading the malware onto a device. Whether it is using the device's functions or sifting through files the user has stored—whatever [the device's owner] can do, the ratter can do.").

[34] *See generally* SELLING "SLAVING", *supra* note 9.

"ratters," are able to quickly gain access to hundreds of devices and then either sell access to the "slaved" devices, or make a profit on the material itself.[35] Female exploitation can be more profitable on the black market.[36] One ratter interviewed by BBC claimed that the running price for access to a female camera was listed at one dollar, but one dollar could also purchase access to 100 male cameras.[37] Similarly, but less extreme, another hacker advertised in a forum access to female cameras for five dollars and access to male cameras for one dollar.[38] Some ratters take deeply private videos from these slaved computers and post them on YouTube where the illicit webcam footage gains traction from "peeping toms."[39] Sometimes, this webcam footage gains so many views that YouTube places advertisements on the illicit videos, giving the hacker part of the profits.[40] In recent years, ratters have had a significant market on YouTube for RAT tutorial videos, in which roughly 38% of these tutorials receive advertising revenue from Google.[41] The broad availability of these online tutorials perpetuates privacy issues and emphasizes how easy it is for a layperson to commit sextortion crimes. Although, this past year, YouTube made it clear that "instructional hacking and phishing" videos that "show[] users how to bypass secure computer systems or steal user credentials and personal data" are banned from its platform, the "massive volume" of these videos suggest that that YouTube cannot catch everything.[42] One major takeaway is that victims should never comply with a sextortionist's demands because it is possible that their private content will be posted, despite the sextortionist's promise to delete

---

[35] *Id.* at 4.

[36] *Id*. at 9; s*ee also* Andrew Silke, *Webcams Taken Over by Hackers, Charity Warns*, BBC (June 20, 2013), https://www.bbc.com/news/uk-22967622 [https://perma.cc/B76X-SSSC].

[37] Silke, *supra* note 36.

[38] SELLING "SLAVING", *supra* note 9, at 9.

[39] *Id*. at 7.

[40] *Id*.

[41] *Id*. at 4.

[42] *See* Adi Robertson, *YouTube's 'Instructional Hacking' Ban Threatens Computer Security Teachers*, VERGE (July 3, 2019), https://www.theverge.com/2019/7/3/20681586/youtube-ban-instructional-hacking-phishing-videos-cyber-weapons-lab-strike [https://perma.cc/RW67-T6MP].

it after receiving a ransom. In an ideal world, victims would ignore demands, but many are uninformed of the consequences of compliance and feel pressured to comply believing it will stop the perpetrator's threats.[43]

In a relatively newer sextortionist strategy, mass-produced sextortion emails have become popular for cybercriminals. Using phishing schemes, scammers access victims' old account passwords through data breaches and use that information as leverage to extort victims by claiming access to the victim's computer and personal files.[44] Although the scammer, like a sextortionist, threatens to release the victim's sensitive images or information, the email is typically only a scare tactic, and the scammer does not have any sensitive information aside from the old password.[45]

The mass production of these phishing schemes can be credited to botnets and botnet services.[46] Botnets are global computer networks that are infected with malware and used to send spam through remote commands.[47] Sextortionists can hire services that utilize botnets to reach millions of email accounts with threatening spam messages.[48] In conjunction with sextortionists' ability to

---

[43] In a survey of 13 to 25-year-old sextortion victims, 53% of victims complied to stop the threats, but out of those who complied, only 37% of the sextortionists actually stopped. Janis Wolnak & David Finkelhor, *Sextortion: Findings from a Survey of 1,631 Victims*, U. OF N.H. 1, 37 (June 2016), https://www.thorn.org/wp-content/uploads/2016/08/Sextortion_Report.pdf [https://perma.cc/GFX9-S7N4].

[44] Christopher Boyd, *Sextortion Bitcoin scam makes unwelcome return*, MALWAREBYTES LABS (Feb. 11, 2019), https://blog.malwarebytes.com/cybercrime/2019/02/sextortion-bitcoin-scam-makes-unwelcome-return/ [https://perma.cc/8VRW-4UNH].

[45] *Id*.

[46] Dariusz Sankowski, *The anatomy of a sextortion spam campaign*, MIT TECH. REV. (Aug. 19, 2019), https://www.technologyreview.com/s/614177/the-anatomy-of-a-sextortion-spam-campaign/ [https://perma.cc/RC2E-Q32P].

[47] *Id*.

[48] *Id*.; *see also* Davey Winder, *Inside One Of The Biggest Sextortion Scams: 450,000 Machines Send 30,000 Emails An Hour*, FORBES (Oct. 16, 2019), https://www.forbes.com/sites/daveywinder/2019/10/16/have-you-sent-15000-sextortion-emails-today/#4e1ae2eb195e [https://perma.cc/XYJ5-3NL4] (explaining that researchers who spent five months monitoring one botnet operation found that it was capable of sending 30,000 emails an hour through the

obtain personal information through massive data breaches, sextortionists not only have the tools to reach millions of people, but the information to instill real fear in their victims.[49] Normally, botnet services have a small margin for return rates, but experts predict that sextortionists are likely seeing greater returns.[50] The threatening nature of sextortion campaigns frightens users into directly sending sextortionists money, cutting back the expenses that scammers usually incur through hosting deceptive websites or procuring fraudulent goods.[51] According to a security researcher from the Netherlands, these blackmails are successful[52] for three reasons: (1) many people view pornography on their computers, (2) some people are aware that it is possible for their webcams to be hacked, and (3) old passwords make it easier to manipulate people into believing their computer has actually been hacked.[53]

Sextortion is a lucrative business that will continue to grow as technology advances.[54] For example, if a sextortionist is demanding money from a victim, they will sometimes request payment through cryptocurrency, like Bitcoin.[55] This is a recent phenomenon, closely tied to the mass-produced sextortion emails.[56] The first known

---

use of 450,000 infected machines, and each spam campaign was capable of reaching up to 27 million potential victims).

[49] *See* Sankowski, *supra* note 46 ("Curiously, scammers do not charge more for emails that contain the victim's password or phone number.").

[50] *Id*.

[51] *See id*.

[52] Although actual success rates are mostly unknown, a study of one "sextortion group" revealed that "more than 150 people have coughed up $250,000 in Bitcoin for fear of their private Web browsing habits being exposed." Thomas Brewster, *Lying Sextortion Scammers Score $250,000 After Sending Victims Their Own Hacked Passwords*, FORBES (July, 31, 2018), https://www.forbes.com/sites/thomasbrewster/2018/07/31/sextortion-scam-with-hacked-passwords-scores-250000-dollars-for-cybercriminals/#41edeff0df16 [https://perma.cc/6L34-HPKC].

[53] *Id*.

[54] *See* Sankowski, *supra* note 46.

[55] *Sextortion 101: What to Know and What to Do*, COFENSE 1, 4 (2019), https://cofense.com/wpcontent/uploads/2019/07/Sextortion-101.pdf?utm_source=Sextortion+Web+Page&utm_medium=website&utm_campaign=2019_Sextortion+Campaign+ [https://perma.cc/LLV2-9QDU].

[56] *See* Sankowski, *supra* note 46.

sextortion scam that demanded cryptocurrency, as opposed to more traditional forms of payment, appeared in 2018.[57] Bitcoin allows anonymous virtual exchanges of money, thus making it more difficult for law enforcement to discover the criminal's identity or track where sextortionists' transfer their ransoms.[58] In a study in which over 7.8 million attempted sextortion phishing emails[59] were analyzed, approximately 17,000 unique Bitcoin wallets were identified in connection to around 1,200 actual transactions or sextortion victims,[60] suggesting that sextortionists take many precautions when depositing their illegally obtained currency. Some researchers worry that sextortion scams are generally more lucrative than conventional phishing scams, and although the economics are not clearly known, the profitability is likely growing.[61]

These illustrated methods of sextortion demonstrate that there are a vast array of fact patterns surrounding sextortion crimes. Because of this, it can be fairly difficult to narrow the definition of sextortion. But, in many cases, the harm to victims is severe and may necessitate a broader reach.

C. The Victims and Harm of Sextortion

If people have heard of this crime at all, adult celebrity victims first come to mind, probably because of the way sextortion typically appears in the news.[62] In reality, most victims of sextortion are minors. The U.S. Department of Justice has indicated that sextortion is "by far the most significantly growing threat to children[.]"[63] In a

---

[57] *Id*.

[58] *Sextortion 101: What to Know and What to Do*, *supra* note 55.

[59] Again, this number represents attempted scams, not the actual number of people who fell victim to the scams, which not clearly known.

[60] *Sextortion 101: What to Know and What to Do*, *supra* note 55.

[61] *See id*.

[62] *See* Colby Walker, *How to Fight Back Against Sextortion – and Avoid Being a Victim,* KSL NEWSRADIO (June 18, 2019), https://kslnewsradio.com/1907066/how-to-fight-back-against-sextortion-and-avoid-being-a-victim/? [https://perma.cc/BZU4-7YWM] (describing how a famous former Disney star was hacked by a sextortionist); *see also* Sullivan, *supra* note 14 (describing how a famous comedian was hacked by a sextortionist).

[63] *The National Strategy for Child Exploitation Prevention and Interdiction*, U.S. DEP'T OF JUSTICE 1, 75 (April 2016), https://www.justice.gov/

study of 78 prosecuted sextortion cases, over 70% of the victims were minors.[64] Although the majority of victims are female,[65] young boys are frequently targeted as well.[66] According to the CyberTipline from the National Center for Missing and Exploited Children ("NCMEC"), in 78% of cases, the sextortionist is seeking more sexual videos or photos of the child.[67] The sextortionist only seeks money or goods from the child 7% of the time, and in the remaining 5% of scenarios, the sextortionist demands sex from the child.[68] The NCMEC hypothesizes that sextortionists sometimes demand sex to make their second demands for sexual images more appealing, increasing the likelihood of the victim's compliance.[69] Although there is no clear data about where the sexual images or videos ultimately end up, the vast quantity of child victims and primary objective of child sextortionists to obtain sexual material suggest that sextortion may be a tactic for broad child pornography consumption and potentially its mass distribution.[70] In the broader

---

psc/file/842411/download [https://perma.cc/7YFQ-4JBW] ("Sextortion offenders typically threaten minors ages 10–17, the typical age range for juvenile Internet users, but increasingly it has been observed when the offender manipulates the victim to abuse younger siblings or friends, extending the threat to even younger and more vulnerable victims.").

[64] Wittes et al., *supra* note 10.

[65] *See Sextortion*, THORN (2017), https://www.thorn.org/wp-content/uploads/2018/10/Sextortion-Infographic-2018-Findings-V2.pdf [https://perma.cc/23UM-MX8R].

[66] Wittes et al., *supra* note 10.

[67] TRENDS IDENTIFIED IN CYBERTIPLINE SEXTORTION REPORTS, NCMEC 1, 4 (2016), https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/sextortionfactsheet.pdf [https://perma.cc/63TF-BACY] (noting that female children are blackmailed for sexual images or videos at a much higher rate (84%) than male children (53%)).

[68] To account for the remaining 13% of these cases, "[i]n 2% of these reports, multiple objectives were indicated; in 11% of reports, the objective could not be determined[.]" *Id*. at 4–5 (noting that male children are blackmailed for money or goods at a much higher rate (32%) than female children (2%), but the difference between sex demands was negligible (3–5%)).

[69] *Id*. at 5.

[70] *See The National Strategy for Child Exploitation Prevention and Interdiction*, *supra* note 63 (remarking that in a recent DOJ investigation, three live-streaming webcam sites with "worldwide registered users" exhibited thousands of sexually explicit webcam sessions of child sextortion victims).

spectrum of crimes against minors, "[s]extortion cases tend to have more minor victims per offender than all other child sexual exploitation offenses."[71] Child victims of sextortion face serious psychological harm from the sexual and emotional abuse of sextortionists,[72] and "[e]ven though they haven't been touched, the trauma level . . . is as severe as hands-on offenses[.]"[73] Additionally,

> [s]extortion victims engage in cutting, have depression, drop out of school or have their grades decline, as well as engage in other forms of self-harm at an alarming rate. In fact, a 2015 FBI analysis of 43 sextortion cases involving child victims revealed at least two victims committed suicide and at least ten more attempted suicide. Thus, at least 28% of these cases had at least one sextortion victim who committed or attempted suicide.[74]

Although children are more often targeted, adults remain vulnerable to sextortion schemes, especially adult women.[75] Unfortunately, however, government agencies have been reluctant to recognize this crime as anything but a child exploitation crime.[76] This is unfortunate because adult victims face serious psychological harm as well. Harassment from sextortionists contributes to a feeling of helplessness or debilitation that can invade into every area of a victim's life.[77] For some victims, even after their sextortionist is in prison, they are fearful of using electronic devices.[78] Moreover, women and marginalized groups suffer from societal stigmatization when their private sexual lives are put on display.[79] This stigmatization can manifest itself by victims' inability to secure or maintain a job, leaving victims financially vulnerable, humiliated, and ashamed.[80] The fear of this reputational harm may lead

---

[71] *Id.* (explaining that commonly, investigations "reveal that a single sextortion offender has been communicating with hundreds of potential victims.").

[72] *Id*.

[73] Wittes et al., *supra* note 10.

[74] *The National Strategy for Child Exploitation Prevention and Interdiction*, *supra* note 63, at 76.

[75] Wittes et al., *supra* note 10.

[76] *See What is Sextortion?*, *supra* note 10; *see also The National Strategy for Child Exploitation Prevention and Interdiction*, *supra* note 63, at 15.

[77] *See* Wittes et al., *supra* note 10.

[78] *See id*.

[79] *See* Citron, *supra* note 18, at 1875.

[80] *Id.*

sextortion victims to comply with perpetrators' demands, contributing to the silence of victims. The violative nature of this privacy invasion can also create trust and intimacy issues for victims in future relationships,[81] and has the power to "reduce" its victims into being defined by a single sexual act or image in the eyes of the public.[82] Victims whose sexual images have been shared struggle to accept that they "will never know for rest of [their lives] when those images will resurface on the internet."[83] Many of these devasting and lasting impacts on sextortion victims parallel the impact of sexual assault on its victims.[84]

III. SEXTORTION LAWS (AND FLAWS)

A. The "Grab Bag" Approach to Prosecuting Sextortion

The current state of federal law is to prosecute sextortion most often as either garden variety extortion or child pornography.[85] Sextortion crimes against adult victims are charged under 18 U.S.C. § 875(d), the federal extortion law, which requires the perpetrator to have the intent to extort "any money or other thing of value" in conjunction with a "threat to injure the property or reputation" of the victim.[86] If sextortionists seek nonconsensual pornography or sexual favors from victims, those requests are considered "thing[s] of value," and a threat to publish exploitative images of someone is considered a reputational threat; so technically speaking, sextortion

---

[81] *Id.* at 1875.

[82] *Id.* at 1886.

[83] Wittes et al., *supra* note 10.

[84] *See A Call to Action: Ending "Sextortion" in the Digital Age*, THOMAS REUTERS FOUND. (July 2016), https://www.trust.org/contentAsset/raw-data/f3b8d35c-27bf-4ba7-9251-abc07d588347/file [https://perma.cc/L8XZ-RAS5] ("Victims of sexual assault suffer a range of debilitating symptoms, including post-traumatic stress disorder, anxiety, depression, nightmares, flashbacks, difficulty concentrating, and unrelenting feelings of self-blame, shame, embarrassment, fear, sadness, vulnerability, isolation, lack of control, and numbness.").

[85] *See* Pam Greenberg, *Fighting Revenge Porn and 'Sextortion*,' NAT'L CONF. OF STATE LEGISLATURES (July 29, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/fighting-revenge-porn-and-sextortion.aspx [https://perma.cc/GY9F-4A5B].

[86] 18 U.S.C. § 875(d) (2018).

falls under the extortion umbrella.[87] Critics, however, suggest that the law is far too lenient on sextortionists. The maximum imprisonment under 18 U.S.C. § 875(d) is two years, and there is no enhanced sentence for sexually exploitative extortions.[88] Thus, the criminal law does not address the violation of the adult victims' sexual privacy.[89] This is especially disturbing since sextortion "[v]ictims often describe feeling powerless, comparing the experience to rape."[90]

In contrast, in cases with victims younger than eighteen, prosecutors rely on child pornography laws, which often carry severe sentences. Depending on the facts, sextortionists with minor victims are often charged under 18 U.S.C. § 2251 for "Sexual Exploitation of Children" (the production of child pornography) or under 18 U.S.C. § 2252 for "[c]ertain activities relating to material involving the sexual exploitation of minors" (the possession, distribution, or receipt of child pornography).[91] These child pornography crimes have varying sentences depending on severity, from five-year minimums to life sentences.[92] This discrepancy is because sentences are often aggravated based on sexual abuse, repeat offenders, and violent or sadistic images.[93]

---

[87] According to the Eighth Circuit, a sexual relationship is also considered a "thing of value." *A Call to Action: Ending "Sextortion" in the Digital Age*, *supra* note 84 (affirming the defendant's extortion conviction in which he covertly filmed his wife in sexual positions and then, after she decided to divorce him, threatened to release the material unless she continued the relationship).

[88] Wittes et al., *supra* note 10. There could be an enhanced sentence under § 875(b) if the sextortionist were to threaten bodily injury to the victim, but this scenario does not match the "prototype" sextortion case.

[89] *But see* Greenburg, *supra* note 85 (explaining that victims may be able to seek civil remedies if actual disclosure occurs, because "[a]bout a dozen state laws currently allow for a private right of action against those who disclose intimate images without consent").

[90] Wittes et al., *supra* note 10. Sextortion, like revenge porn, is sometimes referred to as a "virtual sexual assault." *Id*. However, since it is "virtual" and not "physical," it does not fall under traditional sexual assault crimes. *Id*.

[91] *See id.*

[92] 18 U.S.C. § 2251 (2018); 18 U.S.C. § 2252 (2018).

[93] *See Citizens Guide to U.S. Federal Law on Child Pornography,* U.S. DEP'T OF JUSTICE, https://www.justice.gov/criminal-ceos/citizens-guide-us-federal-law-child-pornography [https://perma.cc/LR6R-STZN].

In addition to extortion and child pornography laws, prosecutors bring "a grab bag of charges" which may include stalking[94] or computer fraud charges.[95] Charges brought by prosecutors, however, are inconsistent, leading to varying degrees of sentencing.[96] This sentencing disparity is especially prevalent when comparing adult victims to minor victims.[97] According to the Brookings Institution's limited study of 78 sextortion cases, the average sentence for cases with adult victims was 3.2 years, whereas the average sentence for cases with minor victims was 31 years.[98] This disparity suggests that the current state of federal law provides inadequate redress to adult victims, and comparing the short sentences of sextortionists to the vast numbers of their victims, both adult and minors, can feel vastly underwhelming. For example, co-conspirators and sextortionists Ivory Dickerson and Patrick Connelly targeted around 3,800 underage girls.[99] After pleading guilty to all charges, including "three counts of producing child pornography, one count of possessing child pornography, and two counts of computer fraud," Dickerson received a 110-year sentence in prison.[100] His co-conspirator Connelly only pled guilty to one count of child pornography out of his 12 charges, and he received a

---

[94] Stalking charges are more typical when the sextortionist has a personal connection to the victim. *See* Wittes et al., *supra* note 10. For example, sextortionist Adam Savadar, who targeted women he knew from high school, was sentenced to 2.5 years in prison on one count of cyberstalking and one count of sextortion. *Id*.

[95] *See* Quinta Jurecic, *A Turning Point for Sextortion*, ATLANTIC (Feb. 11, 2019), https://www.theatlantic.com/ideas/archive/2019/02/turning-point-sextortion/582466/ [https://perma.cc/8K4V-35N7].

[96] Wittes et al., *supra* note 10.

[97] *Id*.

[98] *Id*. ("The reason is that federal child pornography laws carry particularly stiff sentences, far stiffer than those at issue with stalking, extortion, or computer intrusion laws. The result is that of those cases that involved minor victims and did not produce a life sentence, the sentencing range varied from seven months to 139 years imprisonment, with a median of 288 months (24 years) and a mean sentence of 369 months (31 years). Cases that involved only adult victims, by contrast, involved sentencing ranges from one month to 6.5 years imprisonment, a median sentence of only 40 months and a mean sentence of 38 months.").

[99] *Id.*

[100] *Id*.

30-year sentence.[101] In contrast, sextortionist Michael C. Ford targeted mostly adult women, specifically aspiring models and sorority girls.[102] At the time of his arrest, Ford had hacked 450 computers and threatened 75 victims.[103] He had 17 charges against him: "nine counts of cyberstalking, seven counts of computer fraud, and one count of wire fraud[.]"[104] Even though he pled guilty to all charges, he only received a 57-month sentence,[105] which equates to less than five years in prison. Unfortunately, because of investigative and evidentiary issues, many of the charges brought by prosecutors do not land, despite the vast number of victims these sextortionists are believed[106] to have targeted.

B. State Laws and a Revenge Porn Comparison and Statutory Suggestion

In the past, state law has not always been the most effective platform for sextortion prosecution.[107] Fortunately, in the past few years, state legislatures have begun to recognize the existence of this crime. In March 2017, Utah paved the way for sextortion laws in the United States.[108] The Utah "sexual extortion" law reads:

> An individual who is 18 years old or older commits the offense of sexual extortion if the individual:

---

[101] *Id*.
[102] *Id*.
[103] *Id*.
[104] *Id*.
[105] *Id*.
[106] *Id*. ("The disparities between the number of identified victims and the number estimated can be extreme.").
[107] See *A Call to Action: Ending "Sextortion" in the Digital Age*, *supra* note 84 (describing a sextortion case in Wisconsin in which the sextortionist, who threatened a minor victim, was charged with misdemeanors and received one year of probation, but prosecutors had "to become pretty creative in finding statutes that deal with this").
[108] Jean Gazis, *Utah and Arkansas First States to Enact Legislation Criminalizing Cyber-Sexual Extortion ("Sextortion")*, LEGAL MOMENTUM (Mar. 31, 2017), https://www.legalmomentum.org/press/utah-and-arkansas-first-states-enact-legislation-criminalizing-cyber-sexual-extortion- [https://perma.cc/T43N-9VDJ] (recognizing that Arkansas passed its sextortion law just five days after Utah's passed).

> (a) with an intent to coerce a 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, communicates in person or by electronic means a threat:
>
> (i) to the victim's person, property, or reputation; or
>
> (ii) to distribute an intimate image or video of the victim; or
>
> (b) knowingly causes a victim to engage in sexual contact, in sexually explicit conduct, or in simulated sexually explicit conduct, or to produce, provide, or distribute any image, video, or other recording of any individual naked or engaged in sexually explicit conduct by means of a threat:
>
> (i) to the victim's person, property, or reputation; or
>
> (ii) to distribute an intimate image or video of the victim.[109]

As the first sextortion law in the country, the Utah statute has become a model for other states, rightfully so for its emphasis on sextortion as a sex offense. However, the statute is not perfect. For instance, the statute has already faced criticism for its failure to incorporate juvenile offenders.[110] Juvenile sextortionists could still be charged for exploitation of minors in which the victims are children,[111] but this option would be unavailable if the juvenile perpetrator had adult victims.[112] Additionally, under Utah's

---

[109] UTAH CODE § 76-5b-204(2) (2017).

[110] Brittany Johnson, *Does Utah's Sextortion Law Fall Short of Protecting All Victims?*, ABC NEWS (Aug. 15, 2019), https://www.abc4.com/news/does-utahs-sextortion-law-fall-short-of-protecting-all-victims/ [https://perma.cc/PYP2-6WZA] (explaining that, in the case of one juvenile sextortionist with 50 victims, he could not be charged under Utah's sextortion law for most of his victims since he was under 18 the time of the crimes).

[111] *See* Jennifer Gardiner*, Courts: Missionary Sent Home After Police Discover He Had Sexually Exploited Over 50 Teen Girls*, ABC NEWS (July 2, 2019), https://www.abc4.com/ap-state/utah/courts-missionary-sent-home-after-police-discover-he-had-sexually-exploited-over-50-teen-girls/_[https://perma.cc/PC2R-YLE6] (explaining that the juvenile sextortionist in Utah was charged with exploitation of minors since many of his victims were teenage girls).

[112] Sim Gill, the Salt Lake County District Attorney in Utah, prosecutes sextortion cases and believes that it is a "simple fix" to include minors and bring justice to these victims. Johnson, *supra* note 111. The Utah law's sponsor, Senator Curt Bramble, said it was worth considering given that other statutes consider "egregious or aggravating circumstances" to determine if a minor could be tried as an adult. *Id*.

definition of sextortion, a threat to distribute a victim's sexually explicit material would not fall under this statute if the sextortionist was merely seeking money instead of sexual images or favors. Fortunately, now, at least 26 states and Washington D.C. have followed Utah's lead by enacting sextortion laws.[113] This quick momentum in just two years is similar to the momentum of state revenge porn laws, which legislatures began enacting in 2013; now, 46 states have laws for the "nonconsensual dissemination of intimate images."[114]

One possible option for states who have yet to address sextortion could be the modification of current state revenge porn laws to include sextortion. Combining sextortion and revenge porn statutes, which have similar fundamental traits, could promote ease of prosecution. Also, distinguishing the crimes could possibly be served in the sentencing process, for example by creating aggravated sentences for the actual distribution of images, as opposed to the threat to distribute them. Like the general public, prosecutors could potentially have difficulty distinguishing between sextortion and revenge porn. For borderline cases, if the perpetrator were prosecuted under a combined sextortion and revenge porn statute, as opposed to a stand-alone statute, there could be a lesser chance that offenders will walk away due to a technicality.

Consider the following hypothetical: a perpetrator has publicly threatened his victim that he will publish a nude photo he stole from her unless she agrees to cease communicating with a friend of his; when she does not comply with his demands, he posts the photo on

---

[113] Greenberg, *supra* note 85.

[114] *Id.* Significantly, several revenge porn laws have been challenged for violating free speech under the first amendment. *Id.* This development is relevant for cases in which sextortion victims may inevitably become revenge porn victims, and thus turn to dissemination laws if the sextortionists' threats are carried out. But, in all likelihood, as long as the revenge porn laws are narrowly tailored, they should withstand first amendment scrutiny, and this issue may never arise. *See* Nicole Ligon, *Revenge Porn Can Be Outlawed Under The First Amendment*, LAW360 (July 11, 2019), https://www.law360.com/articles/1176991/revenge-porn-can-be-outlawed-under-the-first-amendment [https://perma.cc/99QM-ZH68].

Twitter.[115] Under these facts, the crime began as sextortion, and when the victim did not comply, it evolved into revenge porn. However, if a confused prosecutor charged this perpetrator only under a narrowly tailored sextortion statute, the defendant could argue that he "did not engage in 'sextortion' because [he] never demanded that [the victim] send [him] additional topless photos or any money or property in exchange for refraining from posting her photograph[.]"[116] Seemingly, under a typical sextortion law like Utah's,[117] the defendant would walk free.

But sextortionists should not be able to escape accountability based on ambiguities in this developing area of the law. Combining sextortion and revenge porn laws into one statute, at the state or federal level, could provide clarity. Critics of this method from the Brookings Institution, however, argue that sextortion deserves its own statute, because they believe the crime in sextortion is the "creation or production" of the sexual material, not merely the threat to distribute it.[118] This again depends on how narrowly a legislature decides to define sextortion, as it ignores when existing sexual material is stolen from a victim, and Brookings' approach may trivialize the harm innate to the threat of distribution. Arguably, the menacing threat to release a victim's sexual images accompanied by a coercive demand for money or more material, is just as violative as actual dissemination. Likewise, a sextortionist is just as morally culpable as a perpetrator of revenge porn.

C. *A Federal Proposal*

Federal law could soon follow the state legislatures' footsteps by addressing both sextortion and revenge porn. The "Stopping Harmful Image Exploitation and Limiting Distribution"

---

[115] These facts are actually based on a civil matter. *See* Backlund v. Stone, No. B235173, 2012 Cal. App. Unpub. LEXIS 6467, at *1 (Sept. 4, 2012).

[116] Jeff Kosseff, *Cybersecurity of the Person*, 17 FIRST AMEND. L. REV. 343, 349 (2018).

[117] UTAH CODE § 76-5b-204(2) (2017).

[118] Benjamin Wittes et al., *Closing the Sextortion Sentencing Gap: A Legislative Proposal*, BROOKINGS INST. (May 11, 2016), https://www.brookings.edu/research/closing-the-sextortion-sentencing-gap-a-legislative-proposal/ [https://perma.cc/CM9B-73FW].

("SHIELD") Act of 2019, proposed by members of the House of Representatives, offers a solution to the gap in federal law,[119] and may also correct the ambiguities of state sextortion and revenge porn laws. The SHIELD Act combines revenge porn and sextortion into one federal crime, as follows:

> § 1802. Certain activities relating to intimate visual depictions . . .
>
> (b) OFFENSE.—Except as provided in subsection (d), it shall be unlawful to knowingly use any means or facility of interstate or foreign commerce to distribute an intimate visual depiction of an individual—
>
> (1) with knowledge of or reckless disregard for—
>
> (A) the lack of consent of the individual to the distribution; and
>
> (B) the reasonable expectation of the individual that the depiction would remain private; and
>
> (2) without an objectively reasonable belief that such distribution touches upon a matter of public concern. . . .
>
> (e) THREATS.—Any person who intentionally threatens to commit an offense under subsection (b) shall be punished as provided in subsection (c).[120]

Rather than create both a sextortion and a revenge porn law to fill the gap in federal law, this proposal criminalizes sextortion as, essentially, a threat to commit revenge porn. The SHIELD Act does not include sextortion crimes in which the sextortionist threatens a harm other than the distribution of the victims' sexual images. These scenarios are rarer than the typical threat to disseminate images, but they do exist. This merely reflects how this sample of representatives was prepared to define sextortion. Of course, such a crime could still fall under federal extortion or child pornography statutes, so it would not go unpunished, but it would not meet the sextortion elements under the SHIELD Act, either.

Despite compelling reasons for establishing a federal sextortion crime, members of Congress may be reluctant to adopt the SHIELD

---

[119] SHIELD Act, H.R. 2896, 116th Cong. (2019).

[120] *Id*. Notice that the proposal anticipates possible First Amendment issues by allowing for a "public concern" exception to the possible protected speech in nonconsensual dissemination of sexual images. *See generally "Revenge Porn" Law Survives Constitutional Challenge in Vermont*, CYBER C.R. INITIATIVE (Oct. 19, 2018), https://www.cybercivilrights.org/revenge-porn-law-survives-constitutional-challenge-vermont/ [https://perma.cc/E3BK-BUZH].

Act due to "overcriminalization" of conduct. Overcriminalization represents the view that criminal law is "overuse[d]" and "abuse[d]" to address societal issues and mistakes—i.e. there are simply too many crimes hampering the overall quality of and effectiveness of criminal law.[121] There is a general critique that in recent years, the catalogue of federal criminal laws has become too vast, and frequently falls victim to "political opportunism."[122] Critics of overcriminalization believe that instead of creating more crimes when a new type of conduct is condemned, the law should focus on traditional *mala in se* crimes to prosecute the conduct.[123] For sextortion specifically, overcriminalization critics may argue that there is nothing wrong with a "grab bag" approach to criminalize sextortionists' conduct, and the addition of a federal sextortion law would be superfluous or redundant.[124] Even though sextortionists cannot be punished equally, criminal law does not allow them to escape entirely: extortion is a crime and there are many technology-based crimes and interpersonal crimes like stalking and sexual exploitation crimes that are available to punish this conduct.[125] Thus, an overcriminalization critics would argue there is no true "loophole" to their behavior, and it is adequately prohibited by criminal law. Many sextortion victims may not find this particularly satisfying, however, if their sextortionists end up with particularly low sentences.

---

[121] *Overcriminalization*, HERITAGE FOUND. (2019), https://www.heritage.org/crime-and-justice/heritage-explains/overcriminalization [https://perma.cc/7RR5-KPNP].

[122] *Id*.

[123] *See id*.; *see also* MERRIAM-WEBSTER INC., *malum in se*, THE MERRIAM-WEBSTER.COM LEGAL DICTIONARY, https://www.merriam-webster.com/legal/malum%20in%20se [https://perma.cc/52V2-X9BW] (last visited Jan. 10, 2020) ("[A]n offense that is evil or wrong from its own nature irrespective of statute — often used with a preceding noun (as crime or act)").

[124] *See Overcriminalization*, *supra* note 121.

[125] For this argument in the context of revenge porn, *see, e.g.,* Sarah Jeong, *Revenge Porn Is Bad. Criminalizing It Is Worse*, WIRED (Oct. 28, 2013), https://www.wired.com/2013/10/why-criminalizing-revenge-porn-is-a-bad-idea [https://perma.cc/5J3M-PLRR] (arguing that the criminalization of revenge porn is not necessary because "a number of legal remedies against both vengeful exes and website operators already exist").

The SHIELD Act, by combining sextortion and revenge porn into one statute, could serve as a middle-ground between proponents of federal sextortion regulation and critics of overcriminalization. Regardless of how the future federal sextortion law reads, the law should treat perpetrators as sex offenders, and sentencing should be similar to other federal sex crimes.[126] If sextortion was classified as a sex crime under the Federal Sentencing Guidelines, this would create higher sentences for some sextortionists, since "sexual assaults are not 'grouped' as a single pattern of conduct for purposes of sentencing,"[127] and as illustrated above, many sextortionists have more than one victim. For example, if a sextortionist has 50 victims, and his actions are grouped, under the SHIELD Act, his maximum sentence would be five years in prison.[128] Some experts even recommend that the statutory minimum for sextortion should parallel the five-year minimum in 18 U.S.C. § 875(c), which covers extortions involving "any threat to injure the person of another."[129] Overall, the SHIELD Act is a step in the right direction, but it falls short for failing to acknowledge that perpetrators are sex offenders by classifying sextortion as a sex crime under the Federal Sentencing Guidelines, or establish some kind of statutory minimum for this sex offense.

Sextortion laws are the first step to increased sextortion awareness. But, considering the use of technology to commit this crime, the use of technology to defeat it and the increased regulation of tech companies are likely to be practical solutions going forward.

IV. THE "TECHNICAL DIFFICULTIES" OF SEXTORTION

Technology is both the problem and solution to stopping sextortionists. It is indisputable that technology has created a greater avenue for sextortionists, stalkers, sex offenders, and pedophiles, alike. People are more vulnerable than ever to internet crimes in general. Cybercriminals have much to gain from the easy

---

[126] *See* Wittes et al., *supra* note 118.

[127] *Id*.

[128] *See* SHIELD Act § 1802(c).

[129] *Id*. ("[T]he issuance of a threat in order to compel sexual activity is an offense roughly comparable in gravity to a threat—perhaps not carried out—to injure someone physically.").

accessibility, distribution, and profitability of illicit materials and sextortion. Additionally, cybercriminals have a small risk of being caught, due to heavy caseloads for prosecutors, and, for sextortionists in particular, the low likelihood that the crime will be reported at all. This section will discuss how technology might be used to help sextortion victims, but also, how technology might be contributing to the plight of victims, other than its obvious use in the facilitation of these crimes.

To combat users' vulnerability, tech and social media companies, some of which have been accused of being idle in the past,[130] are taking measures to safeguard users. For example, Amazon's latest smart home devices with displays allow users to turn off the device's microphone and camera, as well as cover the camera with a built-in shutter when it is not in use.[131] Amazon's decision to include security measures, rather than expect consumers to proactively protect their own security, sends a message to consumers that they are vulnerable to intrusion and webcam privacy should be taken seriously. Companies like Facebook, Amazon, Microsoft, Google, and Apple are also heavily investing in data security, as well as applying for patents that focus on user privacy, including products to secure login credentials and combat cybercriminals.[132] Although most social media companies have self-

---

[130] *See* Michael H. Keller & Gabriel J.X. Dance, *The Internet is Overrun with Images of Child Sexual Abuse. What Went Wrong?*, N.Y. TIMES (Sept. 28, 2019), https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html?module=inline [https://perma.cc/69QR-DWC5] ("Hany Farid, who worked with Microsoft to develop technology in 2009 for detecting child sexual abuse material, said tech companies had been reluctant for years to dig too deeply . . . 'The companies knew the house was full of roaches, and they were scared to turn the lights on,' he said. 'And then when they did turn the lights on, it was worse than they thought.'").

[131] *See Introducing Echo Show 5 – Compact Smart Display with Alexa – Charcoal*, AMAZON, https://www.amazon.com/Introducing-Echo-Show-Compact-Charcoal/dp/B07HZLHPKP/ref=sr_1_2?crid=32BRFYDR7063S&keywords=amazon+technology&qid=1567562407&s=gateway&sprefix=amazon+tech%2Caps%2C143&sr=8-2 [https://perma.cc/K9FE-DHK2] (last visited Oct. 28, 2019).

[132] *How Big Tech Is Finally Tackling Cybersecurity*, CB INSIGHTS (Mar. 27, 2019), https://www.cbinsights.com/research/facebook-amazon-microsoft-google-apple-cybersecurity/ [https://perma.cc/X7YG-XTXY].

reporting systems in place, Facebook is now attempting to use developments in Artificial Intelligence ("AI") to proactively detect nude images and videos that are shared on its platform before the images are even reported.[133] If successful, a widespread AI initiative on Facebook could be especially effective against sextortion. If AI could take down images before they are even posted, and social media users know this, a sextortionist's threat to publish private material simply would not have the same weight, and victims may not be as easily coerced into complying with threats.

While prioritizing privacy could make users less vulnerable, prioritizing privacy rights could also make it harder to catch sextortionists. For instance, Facebook has made a huge shift in the operation of its platform to prioritize user privacy,[134] beginning by changing its messaging platform, Facebook Messenger, to encrypted messages.[135] But advocates against child exploitation are worried encryption will make it more difficult for authorities to catch online predators.[136] According to the NCMEC, 99% of all child pornography tips on NCMEC's tip line come directly from tech platforms such as Facebook.[137] More specifically, around 33%

---

[133] *Facebook Readies AI Tech to Combat 'Revenge Porn'*, REUTERS (Mar. 15, 2019), https://www.reuters.com/article/us-facebook-content/facebook-readies-ai-tech-to-combat-revenge-porn-idUSKCN1QW1JV [https://perma.cc/PE4K-EPC2] (explaining that under Facebook's new policy, a trained employee would then review the possibly offensive image and take steps to remove the image or disable the account). But, the threat remains that sextortionists will use AI to become more sophisticated as well. *See* Peter Asaro, *What Is an 'Artificial Intelligence Arms Race' Anyway?,* 15 I/S: J.L. & POL'Y FOR INFO. SOC'Y 45, 56 (2019).

[134] Mark Zuckerberg, *A Privacy-Focused Vision for Social Networking*, FACEBOOK (Mar. 6, 2019), https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/ [https://perma.cc/BZ22-743Z].

[135] *How Big Tech Is Finally Tackling Cybersecurity*, *supra* note 132 (Mark Zuckerberg said, "I believe the future of communication will increasingly shift to private, encrypted services where people can be confident what they say to each other stays secure and their messages and content won't stick around forever.").

[136] Casey Newton, *Encrypted Messaging is Becoming More Popular, and Child Advocates are Worried*, VERGE (Sept. 13, 2019), https://www.theverge.com/facebook/2019/9/13/20863489/encryption-stanford-conference-facebook-ncmec-ghq [https://perma.cc/429B-TLUY].

[137] *Id*.

of sextortion crimes against child victims are reported by internet platforms.[138] In 2018, Facebook Messenger was the source for two-thirds of child exploitation reports.[139] Mark Zuckerberg, Facebook's co-founder and CEO, conceded that encryption would create risks for "truly terrible things like child exploitation."[140]

WhatsApp, another instant messaging platform owned by Facebook, encrypted users' messages in 2016, and is currently facing issues with exploitative child images shared on the app.[141] Although WhatsApp bans approximately 250,000 accounts a month for distributing exploitative images of children,[142] WhatsApp employees are limited to monitoring un-encrypted data, such as publicly available group names and group photos.[143] Since children and teenagers are the most vulnerable to sextortionists, these effects are particularly relevant to underage victims of sextortion, but adult victims could feel the adverse effects of Facebook Messenger encryption, as well. For example, adult pornography, if legal, is

---

[138] This is according to a total of 1,428 reports between 2013 and 2016, and NCMEC notes that there has been a measured increase in total reports each year since they began tracking sextortion in 2013. TRENDS IDENTIFIED IN CYBERTIPLINE SEXTORTION REPORTS, *supra* note 67.

[139] Gabriel J.X. Dance & Michael H. Keller, *An Explosion in Online Child Sex Abuse: What You Need to Know*, N.Y. TIMES (Sept. 30, 2019), https://www.nytimes.com/2019/09/29/us/takeaways-child-sex-abuse.html [https://perma.cc/AV7C-PKG3]. *See also* Keller & Dance, *supra* note 130 ("Reports to the authorities typically contain more than one image, and last year encompassed the record 45 million photos and videos, according to the National Center for Missing and Exploited Children.").

[140] Dance & Keller, *supra* note 139 (Mark Zuckerberg said, "Encryption is a powerful tool for privacy . . . but that includes the privacy of people doing bad things.").

[141] Josh Constine, *WhatsApp Has an Encrypted Child Abuse Problem*, TECHCRUNCH (Dec. 20, 2018), https://techcrunch.com/2018/12/20/whatsapp-pornography/ [https://perma.cc/3X4J-WBMH].

[142] Newton, *supra* note 136.

[143] Unfortunately, this has not stopped predators from creating and sharing child exploitative images through the app. Constine, *supra* note 141. If the accounts do not have public names or photos indicating that they share child abuse content, they could still be reported and investigated by WhatsApp employees, but there is the potential for covert pedophilia groups. *Id*. Although WhatsApp does not allow its users to search for groups to join, third party applications have become a resource for predators to find these private groups. *Id*.

allowed on WhatsApp, but it is unclear how WhatsApp employees or AI would know if the adult pornography was nonconsensual unless it was actively reported by a user.[144] Open communication with social media platforms allows non-profit authorities like NCMEC to report predators more easily, thus helping authorities facilitate arrests.[145]

In a continuation of its effort to prioritize privacy, Facebook has also announced that it plans to "reduc[e] permanence" of Facebook messages because users "should not have to worry about what they share coming back to hurt them later."[146] On one hand, this could be great news for sextortion victims who are prey to social media hackings. But on the other hand, it could create a shield for sextortionists. For example, Snap, Inc., the parent company of the popular social media app Snapchat, considers protecting user privacy a "paramount" interest and prides itself on keeping "very little user data."[147] The platform, which operates by "self-destruct[ing]" the messages and images shared through the app,[148] has become notorious for its inability to assist law enforcement in collecting evidence,[149] and has been accused as operating as a "haven" for abusers.[150] Facebook will likely also face these issues when it accomplishes full encryption of Facebook Messenger. Under Facebook's new impermanence proposal, if a sextortionist is threatening someone through Facebook Messenger, the perpetrator could "set individual messages to expire after a few seconds or

---

[144] *See id.* This question may solve itself when FB launches its new nonconsensual-pornography-detecting AI. See *Facebook readies AI tech to combat 'revenge porn'*, *supra* note 133.

[145] Newton, *supra* note 136.

[146] Zuckerberg, *supra* note 134.

[147] Zak Doffman, *Snapchat Has Become A 'Haven For Child Abuse' With Its 'Self-Destructing Messages'*, FORBES (May 26, 2019), https://www.forbes.com/sites/zakdoffman/2019/05/26/snapchats-self-destructing-messages-have-created-a-haven-for-child-abuse/#8366782399a1 [https://perma.cc/869X-6KCY].

[148] *Id*.

[149] Keller & Dance, *supra* note 130 ("According to law enforcement, when requests are made to the company, Snap often replies that it has no additional information.").

[150] Doffman, *supra* note 147.

minutes"[151] effectively erasing the evidence of threats even more quickly than evidence is erased on Snapchat.

Facebook's setbacks for victims of online sex crimes may seem relatively minor, but tech companies are actually in the best position to stop these crimes, and more legal pressure should be placed on them to cooperate with law enforcement. The New York Times recently completed a comprehensive investigation on the internet crisis of exploitative child imagery, including the role of social media companies. The concerns raised in the investigation, although focused primarily on child exploitative imagery, are extremely relevant to sextortion, and not incomparable to concerns of adult nonconsensual pornography.[152] Thus, these findings will be used in depth below to create a discussion on their possible parallel impact on sextortion.

Although tech and social media companies are legally required to report images of child abuse when they discover them, they are not required to look for them.[153] Although it is against many social media sites' policies to post sexual content, adult pornography is protected by law, and the sites are under no obligation to remove lawful images.[154] Social media companies, despite access to immense amounts of useful data and potential criminal evidence, "can take weeks or months to respond to questions from the authorities, if they respond at all."[155] And, even when the companies do report crimes and present data to the police, they often "do not retain essential information about what they find."[156] Despite the federal requirement under 18 U.S.C. § 2258A(h) (2018) that internet companies preserve material about their abusive imagery reports for 90 days, "it is not uncommon for requests from the authorities to

---

[151] Zuckerberg, *supra* note 134.

[152] Unfortunately, it is difficult to find accurate statistics focused on sextortion or exploitative adult imagery. The government does not collect data on the scope or number of sextortion prosecutions, and the Department of Justice and FBI both consider sextortion to be a subset of child exploitation, ignoring the many adult victims. *See, e.g.,* Wittes et al., *supra* note 10; *Citizens Guide to U.S. Federal Law on Child Pornography*, *supra* note 93, at 15; *What is Sextortion?*, *supra* note 10.

[153] Keller & Dance, *supra* note 130.

[154] *See id*.

[155] *Id*.

[156] *Id*.

reach companies too late" given the massive number of reports[157] to authorities.

Unfortunately, cybercriminals who traffic child exploitation imagery are "on the cutting edge of technology," according to a former lawyer at the National Security Agency and current cybersecurity researcher at the Brookings Institution.[158] In general, availability of technology has only made perpetrators of internet crimes more advanced,[159] often leaving law enforcement far behind.[160] Law enforcement's lack of resources[161] have put tech

---

[157] *Id*. (Notwithstanding potential reports of adult abusive imagery, Facebook was credited with supplying "nearly 12 million of the 18.4 million worldwide reports of child sexual abuse material."). There are no statistics about the reports of sexually exploitative adult imagery, but Facebook does provide methods to report them. See *Community Standards*, FACEBOOK (2019), https://www.facebook.com/communitystandards/sexual_exploitation_adults [https://perma.cc/F7U9-HUTC].

[158] *Id*.

[159] *Id*. ("Offenders can cover their tracks by connecting to virtual private networks, which mask their locations; deploying encryption techniques, which can hide their messages and make their hard drives impenetrable; and posting on the dark web, which is inaccessible to conventional browsers.").

[160] FBI cyber agent Scott Aken, talking about hackers and ratters in particular, said, "Law enforcement just isn't equipped at this stage of the game to keep up with this stuff as fast as it's changing. People aren't trained enough. They don't have the manpower to go after the people that want to abuse the technology that was originally meant for good and is now being used for evil." SELLING "SLAVING", *supra* note 9, at 12.

[161] *See* Nick Selby, *Local Police Don't go After Most Cybercriminals. We Need Better Training*, WASH. POST (Apr. 21, 2017), https://www.washingtonpost.com/posteverything/wp/2017/04/21/local-police-dont-go-after-most-cybercriminals-we-need-better-training/ [https://perma.cc/6NLT-Q8BP]. In general, there is not much focus on cybercrimes at the local or state level since cybercrimes have, since 9/11, been viewed as the "feds' problem" by local and state police. *Id*. Because of this, training and teams are not typically created (with exceptions in large urban areas). *Id*. If cybercrime investigators do exist, they typically focus their energy and resources on child exploitation. *Id*. Also, many local cops don't take cybercrimes as seriously, and want to focus on "'real' police work." *Id*. *But see* Wittes et al., *supra* note 10 (arguing these cases may be best handled at the federal level since they are "generally non-local and often require[] complex interjurisdictional machinations and technical forensics" and federal authorities are "better positioned for interstate and international investigations than state or local authorities").

companies in the best position to facilitate catching internet criminals, but many of these companies have consistently failed to cooperate with law enforcement in a timely or helpful manner,[162] and tend to prioritize the privacy of users.

Privacy protection is an admirable pursuit, but the irony is that these protections may benefit victims much less than they will benefit perpetrators of violative privacy crimes, like sextortion and child pornography. Part of the companies' reluctance to take a greater stand against these cyber-sex criminals, is the fear that if they collaborate too closely with government entities, they could be viewed as "government actors" which would subject them to "new legal requirements and court challenges when they police their own sites."[163] Because of this fear of losing their "private" status, placing the burden on tech companies to police sextortion independently would be, more than likely, a fruitless enterprise. Due to this reluctance, there is a greater need to federally regulate these tech companies and force them to more closely monitor the illegal activity on their sites. Congress has tried to regulate these companies in the past through attempts to impose secondary liability, but this was poorly received by these influential companies who have extensive lobbying powers, and internet companies continue to fall

---

[162] *See* Keller & Dance, *supra* note 130. In addition to the complaints about Snapchat, Tumblr, which has switched ownership more than once in the past few years, is notoriously the worst offender, and police also complain that Bing's reports "lack[] essential information, making investigations difficult, if not impossible." *Id*.

[163] In 2016, a federal court held that the NCMEC, though private, "qualified legally as a government entity because it performed a number of essential government functions," specifically in investigating child pornography tips. Keller & Dance, *supra* note 130; Tim Cushing, *Court Says Child Porn Clearinghouse Acts as A Government Entity, Cannot Perform 'Private Searches'*, TECHDIRT (Aug. 9, 2016), https://www.techdirt.com/articles/20160809/07551035194/court-says-child-porn-clearinghouse-acts-as-government-entity-cannot-perform-private-searches.shtml [https://perma.cc/6LFB-877D]. Social media companies like Facebook have in the past worked very closely with nonprofits, including NCMEC, when reporting crimes, but this ruling could give tech companies a reason to distance themselves from organizations considered government entities to prevent the same from happening to them. *See* Keller & Dance, *supra* note 130.

back on Section 230 of the Communications Decency Act of 1996 to avoid responsibility for their users' illegal content.[164]

For adult victims of sextortion, there are many forms of more horrific abuse and sexual exploitation to which law enforcement agents must allocate their time. Even among nonconsensual child sexual imagery, authorities are so overworked that they are limited to focusing on the most heinous crimes inflicted on the youngest victims.[165] Therefore, some of the "tamer" imagery of children is left behind. Even with authorities' dedication to child exploitation, investigators prioritize finding and rescuing kidnapped victims,[166] thus investigations of child sextortion victims, in which the victim is not in immediate physical peril, are likely put on the backburner.

Unfortunately, sextortion victims cannot rely on the current state of technology, the advocacy of tech companies, or overworked and under-resourced law enforcement, to protect them. There are still steps users can take to protect themselves, including: (1) covering webcams when not in use, (2) being cautious about whom they connect with online and wary of "phish-y" emails, and (3) establishing password security measures.[167] However, an obvious solution would be to place the burden on tech companies who have the power, skill, and resources to protect users on their platforms. The self-regulation of the tech industry is not working at the same pace as these cybercriminals, and law enforcement simply does not have the same power to correct these platforms.

Federally regulating these tech companies and forcing them to take action is needed, but, unfortunately, it is a difficult task for

---

[164] Alina Selyukh, *Section 230: A Key Legal Shield For Facebook, Google Is About To Change*, NPR (Mar. 21, 2018), https://www.npr.org/sections/alltechconsidered/2018/03/21/591622450/section-230-a-key-legal-shield-for-facebook-google-is-about-to-change [https://perma.cc/32DS-2Z4L]. In general, Section 230 grants immunity for internet platforms when illegal content is posted on the platform by a third party; for an in-depth discussion of Section 230, *see* Claudia Catalano, Annotation, *Validity, Construction, and Application of Immunity Provisions of Communications Decency Act, 47 U.S.C.A. § 230,* 52 A.L.R. Fed. 2d 37 (2011).

[165] Keller & Dance, *supra* note 130.

[166] *See id.*

[167] *Sextortion 101: What to Know and What to Do*, *supra* note 55.

Congress, that would likely require amending Section 230. The key to getting such an amendment passed is for Congress to work closely with internet and tech giants, to assure their support of such a law.[168] It is not an impossible task, because the Internet Association recently supported an amendment to allow state and civil lawsuits against sites for "knowingly assisting, supporting or facilitating" online sex trafficking.[169] A common counterargument is that creating liability for tech companies actually creates an incentive for them to ignore the criminal activity on their sites, but the purpose behind lessening liability for internet companies under Section 230 was to encourage these companies to responsibly police their platforms, and internet giants have stretched this statute beyond its legislative intentions.[170] Perhaps Congress could negotiate a mutual agreement for internet companies to use their resources to create more effective AI or tip lines to automatically report instances of sextortion to a non-profit clearinghouse, as demonstrated below, instead of instituting harsh liability.

V. COMBATTING SEXTORTION WITH AWARENESS

A. Societal Perception

Given that sextortion is not typically viewed as a "sex crime," it is important to consider the effect that victim-blaming has on the general secrecy of the crime. It is not uncommon in the media for the public to victim-blame sextortion victims.[171] A legal approach to this area of law could consider whether the victim "assumes the risk" when storing explicit photos on tech-based platforms that are

---

[168] *See* Selyukh, *supra* note 164.

[169] *Id*.

[170] *Id*.

[171] *See* Abby Webb, *Why Bella Thorne Deserves Support, Not Shame, For Sharing Nudes*, STUDY BREAKS (July 10, 2019), https://studybreaks.com/thoughts/bella-thorne-nudes-support-not-shame/ [https://perma.cc/S7DW-78XX]. In particular, Whoopi Goldberg did not sympathize with Bella Thorne, a celebrity sextortion victim, saying on her talk show, "If you're famous, I don't care how old you are, you don't get to take nude pictures of yourself . . . . Once you take that picture, it goes into the cloud, and it's available to any hacker who wants it, and if you don't know that in 2019 . . . I'm sorry, . . . you don't get to do that." *Id*.

vulnerable to hackers. However, few would argue that by carrying around cash in your wallet, you are assuming the risk that you will be robbed. Although there is some legal rhetoric about the assessment of victim's blameworthiness in criminal cases,[172] the law should stray away from "victim-blaming." Victim-blaming can occur for all kinds of crimes, but notably, victims of sexual crimes are often blamed for sexual expression.[173] Blaming victims of sextortion for taking naked photos of themselves is no different from blaming victims of rape for provocative clothing choices—it is simply "slut-shaming."[174] Although the victims' behavior may be perfectly legal, the trend to blame victims is firmly rooted in American culture and psychology,[175] and changing this perspective is an ongoing uphill battle, especially as it relates to some victims of sextortion, whose fear of societal reprisal may deter them from reporting the crime.

While evolving technology had made it easier for sextortionists to trap vulnerable victims, taking nude photos is not an innovation of the smart phone.[176] Instead of blaming teenagers and adults for

---

[172] *See generally* Aya Gruber, *Victim Wrongs: The Case for a General Criminal Defense Based on Wrongful Victim Behavior in an Era of Victims' Rights*, 76 TEMP. L. REV. 645 (2003) (clarifying some of the stigma around "victim-blaming" and discussing the role of victim liability in criminal law, but rejecting the suggestion that the principles of assumption of risk or contributory negligence should be imported from tort law).

[173] *Id*. This comes up when the victim's personal, sexual photos are unlawfully obtained by the sextortionist, and this method of sextortion appears common among celebrity victims. *See* Webb, *supra* note 171; *see also* Sullivan, *supra* note 14. Both Thorne and Cummings chose to post their own nude photos instead of comply with their sextortionists' demands. *Id*.

[174] *See* Rachel Budde Patton, *Taking the Sting Out of Revenge Porn: Using Criminal Statutes to Safeguard Sexual Autonomy in the Digital Age*, 16 GEO. J. GENDER & L. 407, 419 (2015) (Slut-shaming describes the act of criticizing or denigrating an individual based on her perceived sexual history, behavior, or availability as a sexual partner in a way meant to bring shame to the individual.").

[175] Webb, *supra* note 171 (Sherry Hamby, a psychology professor explains that, "[t]here's just a really strong need to believe that we all deserve our outcomes and consequences . . . . In other cultures, where sometimes because of war or poverty or . . . even just because of a strong thread of fatalism in the culture, it's a lot better recognized that sometimes bad things happen to good people[.]").

[176] The concept of naked imagery as a form of expression is centuries old, stemming from its popularity in various artforms. *See* Maude Bass-Krueger,

their desire to "sext" or take nude photos of themselves, society should embrace that this behavior is inevitable, and provide safeguards by educating people to take precautions about how they communicate with peers online.[177] Taking an "abstinence" stance on sextortion by telling people, "never take nude photos of yourself so that you will never be at risk" is not only unrealistic,[178] but contributes to the stigmatization and silence of victims. While these methods of support apply equally to adult sextortion victims, perhaps focusing on educating young people, the future of society, will foster a culture of victim-supporters, not victim-blamers. For

[NSFW] A Brief History of Nudes, GOOGLE ARTS & CULTURE, https://artsandculture.google.com/theme/XwISmlY5uQWdJQ [perma.cc/3CTF-85KC]. In contrast, sexual blackmail as a crime did not emerge until the 19th century. John Schwartz, The Art of Blackmail, N.Y. TIMES (Oct. 3, 2009), https://www.nytimes.com/2009/10/04/weekinreview/04schwartz.html [https://perma.cc/5YFD-TG78]. The advent of the Polaroid camera in the mid-20th century introduced the general public to shareable nude pictures; for the first time in history, people could develop photos without lab technicians, keeping intimate photos private. Christopher Bonanos, *Before Sexting, There Was Polaroid*, ATLANTIC (Oct. 1, 2012), https://www.theatlantic.com/technology/archive/2012/10/before-sexting-there-was-polaroid/263082/ [https://perma.cc/95WE-5KLX]. Although nude imagery has existed for centuries, many people in society still perceive it as morally offensive, which could be the unspoken reason behind blaming sextortion victims. Expression of sexuality is highly debated, especially among women and feminist communities in which there is not a consensus over whether taking nude photos is empowering or exploitative. *See* Isabelle Khoo, *Women Pose Nude for Female Empowerment*, ATLANTIC (Oct. 2, 2014), https://www.huffingtonpost.ca/2014/10/02/women-pose-nude_n_5922020.html [https://perma.cc/ZS4N-ABX2] (with the view that nude photography promotes body positivity and self-confidence); *see also* Jia Tolentino, *How 'Empowerment' Became Something for Women to Buy,* N.Y. TIMES MAG. (Apr. 12, 2016), https://www.nytimes.com/2016/04/17/magazine/how-empowerment-became-something-for-women-to-buy.html [https://perma.cc/GH3N-EB2X] (with the view that "empowerment" has become merely a marketing tactic targeting women).

[177] *See* Kelly Muldavin, *Cruel to be Kind: The Societal Response to Technology and Youth Sexual Expression*, 23 LEWIS & CLARK L. REV. 425, 461–62 (2019).

[178] *See* Melissa Davey, *Teens Should be Educated About Safer Sexting Not Just Abstinence, Report Says*, GUARDIAN (Oct. 30, 2016), https://www.theguardian.com/australia-news/2016/oct/31/teens-should-be-educated-about-safer-sexting-not-just-abstinence-report-says [https://perma.cc/VG5G-AC4C]. Also, abstinence only sexual education has failed schools. Muldavin, *supra* note 177, at 462.

16-year-old sextortion victim Tevan Tobler, the fear of his nude video being released led him to commit suicide.[179] After Tobler's parents shared his story, other victims came forward and opened investigations.[180] If more sextortion victims felt supported to come forward, authorities would be more likely to catch perpetrators, prevent further victims, and literally save victims' lives. Basically, sextortion needs its own "#MeToo" movement.

B. Awareness Campaigns

Public awareness campaigns have recently become more prominent, but their effectiveness remains unclear, and Congressional intervention through clearly defining and creating a comprehensive legal process for sextortion victims could help bring these varying efforts into consensus. Public figures are anomalous sextortion victims, because they are "both particularly vulnerable to blackmail and particularly resistant to it[,]"[181] but they could have an important role in public awareness of the pervasiveness of this crime. In one example, Jeff Bezos, the CEO of Amazon, fought back against his sextortionist by exposing the threatening messages in a public blog post.[182] Two other sextortion victims, comedian Whitney Cummings and actress Bella Thorne refused to comply with their sextortionists' demands, and proactively released their own nude

---

[179] Pat Reavy, *Utah Family Sharing Sextortion Suicide Story 'Likely Saved Some Lives,' Police Say,* DESERETNEWS (Apr. 10, 2019), https://www.deseret.com/2019/4/10/20670612/utah-family-sharing-sextortion-suicide-story-likely-saved-some-lives-police-say#davis-county-sheriffs-detective-john-peirce-works-in-his-office-at-the-davis-county-justice-center-in-farmington-on-monday-april-1-2019-peirce-worked-on-the-tevan-tobler-case [https://perma.cc/572N-LZJ4].

[180] *Id.*

[181] Jurecic, *supra* note 95.

[182] "Of course I don't want personal photos published, but I also won't participate in [the National Enquirer's] well-known practice of blackmail, political favors, political attacks, and corruption." Jeff Bezos, *No Thank You, Mr. Pecker*, MEDIUM (Feb. 7, 2019), https://medium.com/@jeffreypbezos/no-thank-you-mr-pecker-146e3922310f [https://perma.cc/5RMP-RVR4] (explaining that AMI, the owner of the National Enquirer, threatened to release intimate images that Bezos took of himself if he failed to make a public statement, that Bezos perceived to be a lie, about the political nature of AMI).

photos on their social media accounts.[183] Not all victims of sextortion possess the power, resources, confidence, or societal acceptance to take the same actions as public figures, but they are creating an important precedent that tells victims they can fight back. If more sextortion victims are inspired by these public figures, they may gain the confidence to, at the very least, tell someone about their sextortion.[184] It is simply not possible for police to catch sextortionists, or prosecutors to bring them to justice, if the crimes remain unspoken and unreported.

Although celebrity involvement has been a recent, informal avenue of promoting public awareness of sextortion, it does not stop there. The FBI recently launched its official "Stop Sextortion" campaign to promote sextortion awareness in schools.[185] The site includes graphics, advice, and a general explanation of sextortion, all catered towards a young audience.[186] The campaign reiterates to victims that they are not "in trouble" and encourages them to reach out to the FBI or a trusted adult if they are being targeted by a sextortionist.[187] The campaign also provides posters for campuses and recommended language for schools to use in their newsletters to students and parents.[188] Thorn,[189] an organization devoted to preventing child sexual abuse, has a similar campaign with a cat-

---

[183] Webb, *supra* note 171; Sullivan, *supra* note 14. But, although some may perceive these celebrity women posting their own nude photos as empowering, the threat of this post is exactly what keeps the average sextortion victim silent.

[184] Victims are in a better position when they can overcome their shame or embarrassment and turn to a third party, often a parent or a friend, who can report the crime to law enforcement. Wittes et al., *supra* note 10. In a survey conducted by Thorn, one in three sextortion victims (ages 13 to 25) never told anyone, but out of the victims who disclosed, 53% told a friend, and only 17% told law enforcement. *Sextortion Infographic*, THORN (2018), https://www.thorn.org/wp-content/uploads/2018/10/Sextortion-Infographic-2018-Findings-V2.pdf [https://perma.cc/D732-BUPL].

[185] *See Stop Sextortion*, FBI (Sept. 3, 2019), https://www.fbi.gov/news/stories/stop-sextortion-youth-face-risk-online-090319 [https://perma.cc/9KQG-PBUE].

[186] *Id.*

[187] *Id.*

[188] *Id.*

[189] Not to be confused with Bella Thorne, who is not affiliated with this organization.

themed website that is friendlier to children.[190] Thorn particularly focuses on the importance of kids talking to friends about sextortion and vocalizing their support.[191]

Overall, these campaigns are an step in the right direction, especially since they are focused on children, who are the most vulnerable to sextortionists. If schools follow similar guidelines to the Thorn or FBI campaigns, this could successfully shift the societal conversation from victim-blaming to victim support. However, the campaigns may create the false impression that sextortion is exclusively a crime against children, and similar campaigns are needed, perhaps workplace campaigns, to promote awareness of adult victims, particularly given the FBI and DOJ's failure to acknowledge adults as possible victims of sextortion.[192]

Private initiatives like Thorn's campaign, government agency initiatives like the FBI's campaign, and informal awareness tactics from outspoken public figures may all be effective tools for promoting sextortion awareness, but the ultimate awareness tactic lies in the hands of Congress. The creation of a federal sextortion crime would finalize this crime's definition, help prosecutors with the efficiency of justice, guide more states to criminalize this behavior, and give victims a remedy for their virtual sexual assault. But, even more broadly, a federal crime would emphasize the reprehensibility of sextortion, and assure victims that the government is taking the threat seriously. To take this suggestion one step further, a cohesive federal awareness program could be launched through the establishment of a non-profit agency to act as a clearinghouse for sextortion crimes. Like the NCMEC,[193] this

---

[190] *Sextortion. Yup. It's a Thing*., THORN (2018), https://www.stopsextortion.com/ [https://perma.cc/GT2H-STQT].

[191] *Id*.

[192] *See supra* citations accompanying note 76.

[193] *See The National Center for Missing & Exploited Children Mission and History*, NAT'L CTR. FOR MISSING & EXPLOITED CHILDREN, https://web.archive.org/web/20121029010231/http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=4362 [https://perma.cc/H7UH-L2BT] "(In 1984, the U.S. Congress passed the Missing Children's Assistance Act which established a National Resource Center and Clearinghouse on Missing and Exploited Children. The National Center for Missing & Exploited Children was designated to fulfill this role.").

agency could collect sextortion statistics, report sextortion crimes, interpret federal sextortion law, and provide a "one-stop-shop" for sextortion victims to seek help and resources.[194] Such an organization would be the best suited to launch a campaign based on victims' needs. For example, through surveying and crime statistics, the non-profit could assess where sextortion crimes are the most concentrated geographically, as well as which populations are the most misinformed about sextortion, in order to launch an effective and financially practical campaign to the populations that most need it. The sextortion clearinghouse could also provide resources and training recommendations to the law enforcement in these jurisdictions. The establishment of this agency should be another addition to Congress's proposed SHIELD Act,[195] including the recommendations previously suggested, that the SHIELD Act should incorporate provisions that classify sextortion as a sex crime with a statutory sentencing minimum.

VI. CONCLUSION

Sextortion is simply not discussed enough. Everyone is at risk, and its violent impact on children is especially severe. Sextortion has the potential to be an extremely profitable internet crime as sextortionists continue to manipulate technological advancements and societal stigma to their advantage. The simple truth is that silent victims cannot rely on law enforcement to catch sextortionists, and sadly, even for victims who have the courage to come forward, prosecutors cannot always adequately punish offenders due to the confusion in this developing area of law. The demise of sextortion depends on a proactive federal government, societal awareness, and

---

[194] Right now, the government does not collect data on sextortion specifically, since data collection is based on violations of federal statutes. *See* Wittes et al., *supra* note 10. The NCMEC is a clearinghouse that provides resources, collects statistics, and acts as a third party to report missing children and exploited children to the FBI through the use of a CyberTipline service. *See About NCMEC*, NAT'L CTR. FOR MISSING & EXPLOITED CHILDREN, http://www.missingkids.com/footer/media/keyfacts [https://perma.cc/2BGF-G5S5].

[195] Since the SHIELD Act incorporates both revenge porn and sextortion under the same statute, this clearinghouse could also perform this same role for revenge porn crimes, killing two birds with one stone.

outreach for victims. Avoiding uncomfortable conversations only empowers the perpetrators of this disturbing cyber-sex-crime hybrid.

To address the issues surrounding sextortion, Congress has followed states' leads by proposing a federal sextortion (and revenge porn) law in the form of the SHIELD Act. While this Act is a step in the right direction, it is deficient for failing to properly categorize sextortion as a sex crime. Moreover, the enactment of a federal law, alone, is not enough to win the battle against sextortionists. Federal regulation of tech companies is needed to further bolster the government's resources and skill in battling this largely internet-based crime. In addition to these steps, the SHIELD Act should be amended to appoint a non-profit clearinghouse to act as a one-stop-shop for interpreting sextortion law, providing resources to victims and law enforcement, and creating an effective awareness campaign. It takes a village to raise a child, and it will take a determined nation to defeat sextortion.