CYBERSECURITY AND GENDER-BASED VIOLENCE: PROPOSALS FOR COMBATTING SEXTORTION

By Adya Kumar[*]

Content Warning[**]

Please be advised that this article addresses incidents of sexual violence, gender-based violence, and exploitation, including sexual assault perpetrated against both minor and adult victims. Content may be difficult for some readers.

[*] Candidate for Juris Doctor, 2022, Northeastern University School of Law. A big thank you to Professor David O'Brien for providing me with the support and resources to develop this concept and write this article!

[**] Many resources are available for victims and survivors of sextortion. *See Five Steps to Take If You're Being Sextorted*, C.A. GOLDBERG, https://www.cagoldberglaw.com/5-steps-for-sextortion-victims/ (last visited July 11, 2021); Resources for Victims of Cyber Abuse, CYBER CIVIL RIGHTS INITIATIVE, https://www.cybercivilrights.org/victim-resources/ (last visited July 11, 2021); STOP SEXTORTION, https://www.stopsextortion.com/ (last visited July 11, 2021); *Sextortion Is an Emerging Form of Online Abuse*, THORN, https://www.thorn.org/sextortion/ (last visited July 11, 2021); MALE SURVIVOR, https://malesurvivor.org/ (last visited July 11, 2021); *Stop Sextortion*, FED. BUREAU INVESTIGATION (Sept. 3, 2019), https://www.fbi.gov/news/stories/stop-sextortion-youth-face-risk-online-090319; *About the National Sexual Assault Online Hotline*, RAPE, ABUSE & INCEST NAT'L NETWORK (RAINN), https://rainn.org/about-national-sexual-assault-online-hotline (last visited July 7, 2021).

I. INTRODUCTION: SEXTORTION AS A CYBERSECURITY THREAT

Society tends to view cybersecurity as an issue primarily for major institutions to grapple with. Phishing, malware, and social engineering were identified as top cybersecurity threats in 2020, and, as a result, companies were required to take steps to protect against cyberattacks that target "ransomware victims such as high-net-worth individuals."[1] Further, technological advancements have led to widely publicized security threats aimed at corporations or governments, as well as the personal data of millions of citizens who trust their crucial information to remain secure online and on their computers.[2] But those most vulnerable to these cybersecurity threats—at risk almost daily—are not major institutions, but individuals, and the perpetrators are not simply seeking to steal personal data, but rather to steal their victims' dignity.[3] Specifically, many women and children have had their sexual safety violated by the same technologies that can harm companies, hospitals, banks, and other institutions. Although it is perhaps not intuitive to picture victims of cybersecurity attacks as victims of sexual assault, the growing prevalence of cybersecurity attacks designed to harm individuals' sexual autonomy increasingly positions cybersecurity as an issue that deeply impacts society at all levels, extending beyond just harms to major institutions.

Sextortion is a cybersecurity crime that employs well-known tactics—phishing, malware, ransomware, Remote Access Trojans (RATs), and social engineering—to commit the more violating and egregious crime of remote sexual assault.[4] The perpetrators themselves need not be technological savants. In fact, there are many devices and tutorials online that make it cheap and easy for someone to learn how to commit sextortion.[5] As perpetrators' means and tactics become more sophisticated, the crime of sextortion becomes more prevalent, leaving thousands of adult and minor victims all over the world vulnerable.[6]

Sextortion is "old-fashioned extortion or blackmail, carried out over a computer network, involving . . . a threat to release sexually-explicit images of the victim—if the victim does not engage in some form of further sexual activity."[7] The most common features of sextortion cases include computer hacking, social media manipulation, interstate or international victimization, and a demand for in-person sexual activity.[8] "[A]t the core of the crime always lies the intersection of cybersecurity and sexual coercion. For the first time in the history of the world, the global connectivity of the internet means you don't have to be in the same country as someone to sexually

---

[1] Michelle Moore, *Top Cybersecurity Threats in 2020*, U. SAN DIEGO, https://onlinedegrees.sandiego.edu/top-cyber-security-threats/ (last visited Aug. 24, 2020).

[2] *Id.*; Scott Matteson, *Why Data Breaches Keep Happening*, TECHREPUBLIC (June 25, 2019), https://www.techrepublic.com/article/why-data-breaches-keep-happening/.

[3] *See* Karen Levy & Bruce Schneier, *Privacy Threats in Intimate Relationships*, 6 J. CYBERSECURITY 1, 1 (2020) ("[A] huge number of threats are much more quotidian, performed by much less powerful and less technically savvy actors with very different motives and resources. These attackers know their victims well, and have much greater access to their information, devices, and lives in general.").

[4] BENJAMIN WITTES ET AL., CTR. FOR TECH. INNOVATION BROOKINGS, SEXTORTION: CYBERSECURITY, TEENAGERS, AND REMOTE SEXUAL ASSAULT 2, 3, 7, 20 (2016), https://www.brookings.edu/wp-content/uploads/2016/05/sextortion1-1.pdf [hereinafter SEXTORTION].

[5] *Id.* at 7.

[6] *Id.* at 14–15.

[7] *Id.* at 11.

[8] *Id.* at 10.

menace that person."[9] This is sexual assault on a global scale, impacting thousands of victims, and yet lawmakers have not been able to tackle this highly sensitive issue with specificity and uniformity at the federal level.[10] The Federal Bureau of Investigation (FBI) addresses sextortion primarily as a children's rights issue, as opposed to as a gender-based violence issue that equally and significantly impacts adult women.[11] Furthermore, the FBI does not keep any sextortion data that is separate from data collected on the crime of extortion, further decentering the gender-based dimension of this crime.[12]

The goal of this article is to bring awareness to the prevalence of sextortion as a crime, provide an overview of the existing laws used to prosecute sextortion cases, expose deficiencies in existing legal frameworks, and outline strategies aimed at achieving justice for victims and survivors of sextortion.

II. SEXTORTION: A BACKGROUND

Sextortion allows hackers to, in essence, break into the homes of a large number of remote victims over great distances—even across international borders—and demand sexual acts from victims by threatening to release private images of the victims if they do not comply.[13]

Perpetrators can gain access to a victim's computer via social engineering, which is "the art of exploiting human psychology."[14] By "[u]sing a variety of media, including phone calls and social media, these attackers trick people into offering them access to sensitive information."[15] Hackers who commit sextortion aim their attacks disproportionately at women and teenage girls[16] through methods such as catfishing—a method of deceit used to lure another person into a relationship by adopting a fake online identity—in order to gain the victim's trust. An adult hacker named Lucas Michael Chansler once targeted about 350 young girls by pretending to be a teenage boy who wanted to make new friends.[17] Chansler would video call with the victims and ask them to strip on camera while he secretly recorded them.[18] In another case, hackers Christopher Patrick Gunn and Jeremy Brendan Sears pretended to be celebrities whose fan bases consisted mainly of

---

[9] *Id.* at 3.

[10] *See, e.g.*, Stopping Harmful Image Exploitation and Limiting Distribution (SHIELD) Act of 2019, H.R. 2896, 116th Cong. (2019) (establishing a new federal criminal offense related to sextortion, which was only recently introduced in 2019).

[11] *Sextortion*, FED. BUREAU INVESTIGATION, https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/sextortion (last visited Dec. 17, 2020).

[12] Kate Fazzini, *Email Sextortion Scams Are on the Rise and They're Scary – Here's What to Do if You Get One*, CNBC NEWS (June 17, 2019), https://www.cnbc.com/2019/06/17/email-sextortion-scams-on-the-rise-says-fbi.html.

[13] *See* WITTES ET AL., SEXTORTION, *supra* note 4, at 3, 13 (finding eighty cases involving sextortion, affecting more than 3,000 victims, with 63% involving interstate elements and 21% involving international victimization. "It used to be impossible to sexually assault someone in a different country. That is no longer true.").

[14] Josh Fruhlinger, *Social Engineering Explained: How Criminals Exploit Human Behavior*, CSO ONLINE (Sept. 25, 2019), https://www.csoonline.com/article/2124681/what-is-social-engineering.html.

[15] Moore, *supra* note 1 (citing David Bisson, *5 Social Engineering Attacks to Watch Out For*, TRIPWIRE (Nov. 5, 2019), https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/).

[16] *See* WITTES ET AL., SEXTORTION, *supra* note 4, at 4 (finding that a disproportionate number of sextortion victims are women, while almost all sextortion perpetrators are men).

[17] *Id.* at 18.

[18] *Id.*

teenage girls.[19] Gunn and Sears were also members of an online hacking group that "trolled"[20] girls' internet fan-pages for celebrities such as Justin Bieber and One Direction.[21] They would harass the young owners of these fan-pages and spam their pages in order to extort the girls into sending them explicit images and videos.[22]

In addition to social engineering, hackers also manipulate women and teenage girls into downloading malware onto their computers.[23] Malware is shorthand for "malicious software," which can include viruses, ransomware, and spyware.[24] Younger internet users are more vulnerable to hackers as they can be easily induced to visit a website, click on an ad, or download a computer program that contains malware.[25] This malware is designed to be "undetectable to antivirus programs."[26] Hackers Ivory Dickerson and Patrick Connolly, for example, jointly reached out to victims in order to trick them into downloading malware, then blackmailed the victims with photos that they secretly took on their webcams.[27] Connolly would threaten to physically harm his victims or their families if they did not provide further images.[28] In another case, Luis Mijangos used the computers he controlled to spread malware even further by sending it to his victims' friends via their address books, making it appear as though the software was coming from the victims.[29] Some hackers employ technology referred to as keyloggers within their malware, enabling them to see everything that the victim types on their computer.[30] Keyloggers "leverage algorithms that monitor keyboard strokes through pattern recognition and other techniques."[31]

Another popular and more insidious malware device is called a Remote Access Trojan (RAT). Unlike a keylogger, which allows perpetrators to view what a victim types on their computer, RATs give perpetrators total dominion over the computer.[32] Because RATs provide a way for the hacker to gain control over the target computer invisibly, perpetrators are able to manually turn on a victim's camera and access private images.[33] When perpetrators employ both

---

[19] *Id.* at 20.

[20] *See Troll*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/troll (last visited Oct. 27, 2021) (defining the verb "troll" as "to antagonize (others) online by deliberately posting inflammatory, irrelevant, or offensive comments or other disruptive content").

[21] WITTES ET AL., SEXTORTION, *supra* note 4, at 20.

[22] *Id.*

[23] *Id.* at 2.

[24] *See What Is Malware?*, FORCEPOINT, https://www.forcepoint.com/cyber-edu/malware (last visited Aug. 24, 2020) ("[M]alware typically consists of code developed by cyberattackers, designed to cause extensive damage to data and systems or to gain unauthorized access to a network. Malware is typically delivered in the form of a link or file over email and requires the user to click on the link or open the file to execute the malware.").

[25] DIG. CITIZENS ALL., SELLING "SLAVING": OUTING THE PRINCIPAL ENABLERS THAT PROFIT FROM PUSHING MALWARE AND PUT YOUR PRIVACY AT RISK 3 (2015), https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/selling-slavery.pdf.

[26] WITTES ET AL., SEXTORTION, *supra* note 4, at 2.

[27] *Id.* at 19.

[28] *Id.*

[29] *Id.* at 2.

[30] *Id.* at 2, 17.

[31] Dan Swinhoe, *What Is a Keylogger? How Attackers Can Monitor Everything You Type*, CSO ONLINE (Dec. 11, 2018), https://www.csoonline.com/article/3326304/what-is-a-keylogger-how-attackers-can-monitor-everything-you-type.html.

[32] DIG. CITIZENS ALL., *supra* note 25, at 4.

[33] *Id.*

keyloggers and RATs, the result is a dangerous combination of surveillance and control. RATs are notorious for being inexpensive and simple to use.[34] In an internet search conducted by the Digital Citizen's Alliance, a group of internet experts focused on educating the public about internet threats, the researchers found a multitude of easily accessible ways to obtain and employ RATs.[35] Researchers were able to access malware tools for purchase, online forums containing hundreds of tutorials on how to use RATs, and thousands of YouTube tutorials on how to "slave," or take control over, another user's device.[36] On one hacker website, Digital Citizen Alliance researchers found an advertisement selling access to computers belonging to girls for five dollars each, with access to boys' computers selling for one dollar each.[37] Researchers also found videos displaying "an individual hacker's exploits, displaying videos of victims from on their own webcams."[38]

Perpetrators of sextortion are almost always men and can have hundreds of victims.[39] Nearly all adult victims, and a significant number of underage victims, are women, although there are a significant number of underage victims who are men.[40] In cases studied by the Center for Technology Innovation at Brookings Institution,[41] "[v]irtually all of the adult victims" were women, indicating that "adult sextortion . . . appears to be a species of violence against women."[42] Many victims of sextortion feel that "they are at the mercy of their hackers."[43] "Victims have described . . . feeling like a 'slave' to hackers during the sextortion scheme."[44] They spend "every moment in fear of the next message demanding more compromising pictures or videos, living in perpetual anxiety from the risk of public exposure."[45] Unlike data breaches, sextortion is a cyberattack that is deeply personal, leaving victims with long-lasting adverse psychological injuries. Additionally, many victims are afraid to report these crimes or come forward.[46]

Unfortunately, few studies have addressed the demographics of sextortion victims, and there is very little data on whether incidents of sextortion occur disproportionately against victims according to race, nationality, socioeconomic status, gender identity, or sexual orientation. In one exceptional (albeit limited) study, researchers at the Society for Adolescent Health and Medicine

---

[34] DIG. CITIZENS ALL., *supra* note 25, at 6.

[35] *Id.* at 4.

[36] *Id.* at 4, 5. In the field of computer software, "master-slave" communications involve "electronic interaction in which one device acts as the controller (the master) and initiates the commands, and the other devices (the slaves) respond accordingly." Encyclopedia Entry for "Master-Slave," PCMAG, https://www.pcmag.com/encyclopedia/term/master-slave (last visited Apr. 1, 2022).

[37] WITTES ET AL., SEXTORTION, *supra* note 4, at 7.

[38] *Id.*

[39] Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1916 (2019).

[40] *Id.*

[41] The Center for Technology Innovation at the Brookings Institution conducts "research that affects public debate and policymaking in the arena of U.S. and global technology innovation." *About the Center for Technology Innovation*, BROOKINGS INST., https://www.brookings.edu/about-the-center-for-technology-innovation/ (last visited Oct. 27, 2021).

[42] WITTES ET AL., SEXTORTION, *supra* note 4, at 4.

[43] *Id.* at 23.

[44] *Id.* at 11, 23 (addressing the "impact of sextortion on victims," while also stressing the importance of "understand[ing] that [this discussion of sextortion is] excluding a variety of closely-related coercive activities that may also warrant more attention than they have received . . . [and that n]one of this is to diminish the horrifying extortions by which, for example, many pimps keep women in forms of sexual slavery").

[45] *Id.* at 23.

[46] *Id.* at 28–29.

partnered with Thorn, a nonprofit supporting research in the fight against the sexual exploitation of children, to study sextortion against minors under the age of 17 and young adults between the ages of 18 and 25.[47] The study solicited survey answers from victims of sextortion, mainly via Facebook.[48] Amongst survey respondents who experienced sextortion, 79.2% identified as white, 14% identified as Hispanic or Latinx, 4% identified as Black or African American, 2.8% identified as Asian, 0.3% identified as Native Hawaiian or Pacific Islander, 2.1% identified as American Indian or Alaska native, and 3.1% identified as mixed race.[49] A separate study, conducted by researchers Justin W. Patchin and Sameer Hinduja, found significant differences in victimization according to gender identity and sexual orientation, although none with respect to race.[50]

The limited scope of these studies underscores the need for greater research into the demographics of sextortion victims.[51] For one, the studies do not provide information regarding the socioeconomic status of victims or other demographic risk factors, if any, that may make some groups more vulnerable to sextortion than others.[52] The studies are further limited to English-speaking participants, which likely excludes many victims.[53] Underreporting may also result in a lack of data. The Patchin-Hinduja study, for example, found that almost half of the respondents felt uncomfortable reporting sextortion due to "feelings of shame, embarrassment, fear of retribution, or a sense that it simply would not do any good."[54] Importantly, victims with historically marginalized identities may be even less likely to report sextortion or participate in relevant studies. A number of sextortion victims who participated in the Patchin-Hinduja study felt that police blamed them for participating in a video chat or posting photos in the first place.[55] Such sentiments could disproportionately discourage reporting of sextortion by people of color, including Black individuals who are already more likely to have negative interactions with law enforcement.[56] Given the lack of meaningful insights at the intersection of sextortion victimization and demographic risk factors, stakeholders—including federal lawmakers, social justice and human rights organizations, and cybersecurity experts—should pursue more nuanced research on victims of sextortion according to race, nationality, socioeconomic status, gender identity, and sexual orientation in order to support victims in a more effective and equitable manner.

---

[47] Janis Wolak et al., *Sextortion of Minors: Characteristics and Dynamics*, 62 J. ADOLESCENT HEALTH 1, 1, 7 (2017), http://unh.edu/ccrc/CV344-J-Sextortion-JAH-Oct-2017.pdf.
[48] *Id.* at 1–2.
[49] *Id.* at 4.
[50] Justin W. Patchin & Sameer Hinduja, *Sextortion Among Adolescents: Results From a National Survey of U.S. Youth*, 32 SEXUAL ABUSE 30, 30, 38 (2018), https://journals.sagepub.com/doi/pdf/10.1177/1079063218800469.
[51] The cited studies were selected not only because they are some of the few studies in existence that consider the demographics of sextortion victims, but also because they thoroughly define sextortion and explain its impact, address the limitations of existing studies in the field, and utilize evidence-based statistical methods in researching whether sextortion disproportionately impacts victims among marginalized populations.
[52] *See* Wolak et al., *supra* note 47, at 2–3; Patchin & Hinduja, *supra* note 50, at 37 (discussion of study methodologies).
[53] Wolak et al., *supra* note 47, at 7; Patchin & Hinduja, *supra* note 50, at 36.
[54] Patchin & Hinduja, *supra* note 50, at 35.
[55] *Id.*
[56] Hannah Giorgis, *Many Women of Color Don't Go to the Police After Sexual Assault for a Reason*, GUARDIAN (Mar. 25, 2015), https://www.theguardian.com/commentisfree/2015/mar/25/women-of-color-police-sexual-assault-racist-criminal-justice.

III. DEFICIENCIES IN EXISTING LAWS ADDRESSING SEXTORTION

Even though many people who commit sextortion are arrested and convicted, they are not prosecuted for the specific act of sextortion. For example, when Luis Mijangos was arrested in 2010, federal investigators found more than "15,000 web-cam video captures, 900 audio recordings, and 13,000 screen captures on his computers."[57] FBI agents found "files related to approximately 129 different computers, corresponding to approximately 230 users. Of the 230 victims identified, 44 were subsequently determined to be juveniles."[58] The authorities also found "passwords and authentication information, credit card information, and other personal data."[59] Mijangos had gained possession of the victims' data by employing malware that provided him access to files, photos, and videos on the infected computers while allowing him to see everything that was typed onto the computer as well.[60] The malware was disguised as files containing popular songs or videos, which victims then shared with their friends and family, allowing Mijangos to gain access to more computers.[61] The software also gave him the ability to turn on any computer web camera or microphone, allowing Mijangos to both watch and listen to victims without their realizing they were being monitored.[62] Agents found dozens of videos taken from his activation of the victims' web cameras, showing them getting out of the shower, dressing and undressing for the day, and in some cases having sex with a partner.[63]

Mijangos pled guilty to one count of computer hacking in violation of 18 U.S.C. § 1030(a)(2)(C) for intentionally accessing a computer without authorization and obtaining information from a protected computer.[64] He also pled guilty to one count of wiretapping in violation of 18 U.S.C. § 2511(1)(a) for intentionally intercepting electronic communications.[65] He was sentenced to six years imprisonment.[66] It is bizarre, almost counterintuitive, that someone who committed remote sexual assault on such a massive scale received a six-year sentence for crimes related to computer hacking and wiretapping rather than sextortion.

Given the lack of a federal sextortion statute, the most common federal statute used to prosecute perpetrators of sextortion is one that outlaws the sexual exploitation of children.[67] 18 U.S.C. § 2251 states that "[a]ny person who employs, uses, persuades, induces, entices, or coerces any minor to engage in . . . any sexually explicit conduct for the purpose of producing any visual depiction of such conduct" is subject to a mandatory minimum of fifteen years in prison.[68] This

---

[57] WITTES ET AL., SEXTORTION, *supra* note 4, at 2.

[58] Complaint at 10, United States v. Mijangos, No. 10-743-GHK (C.D. Cal. June 17, 2010).

[59] *Id.*

[60] *Id.* at 10–11.

[61] Greg Risling, *Hacker Gets 6-Year Sentence in 'Sextortion' Case*, NBC NEWS (Sept. 1, 2011), http://www.nbcnews.com/id/44364150/ns/technology_and_science-security/t/hacker-gets--year-sentence-sextortion-case/#.XzRdyC2ZPow.

[62] Complaint at 11, United States v. Mijangos, No. 10-743-GHK (C.D. Cal. June 17, 2010).

[63] *Id.*

[64] Judgment and Probation/Commitment Order at 1, United States v. Mijangos, No. 10-743-GHK (C.D. Cal. Mar. 11, 2011).

[65] *Id.*

[66] Risling, *supra* note 61.

[67] WITTES ET AL., SEXTORTION, *supra* note 4, at 15.

[68] 18 U.S.C. § 2251.

statute, and other child pornography and exploitation statutes, have allowed prosecutors to get justice for underage victims.[69]

There is no parallel statute for adult victims of sextortion, however, and these cases are often prosecuted under a "statutory lacuna,"[70] meaning that prosecutors are forced to rely on a patchwork of existing laws that are inadequately tailored to address the crime of sextortion. Federal law concerning aggravated sexual abuse is limited to instances of touching or a threat of force "in the special maritime and territorial jurisdiction of the United States or in a Federal prison."[71] A different statute, the federal interstate extortion law,[72] has been applied in 37% of sextortion cases identified by a Brookings Institution report.[73] The relevant portion of the statute, which addresses the extortion of an individual by threatening to injure their reputation, carries a maximum two-year sentence.[74] In 12% of sextortion cases from the Brookings report,[75] prosecutors relied on the federal stalking law, which carries a maximum sentence of five years.[76] In 15% of the cases from the Brookings report,[77] the federal identity theft law[78] and the Computer Fraud and Abuse Act[79] were used to prosecute sextortion. Some states have their own "video voyeurism laws [that] punish the nonconsensual recording of individuals in a state of undress . . . [or] where they can reasonably expect privacy."[80] In 2017, Arkansas and Utah became the first states to enact state sextortion laws.[81] As of 2019, Alabama is the most recent state to enact a sexual extortion statute.[82] Currently, at least twenty-six states have enacted their own version of a sextortion statute.[83]

The range of existing statutes have been effective in prosecuting some perpetrators, but the punishment for many perpetrators varies depending on the state, the age of the victim, and the circumstances surrounding the crime. This article suggests that there are the three prevailing deficiencies in prosecuting sextortion: (1) lack of a federal sextortion law, (2) failure to hold malware creators accountable, and (3) a misguided understanding of the victims of sextortion.

A. Lawmakers Should Enact a Federal Sextortion Statute

While it is true that Mijangos' conduct meets the elements of computer fraud—gaining access to computers without permission—the Computer Fraud and Abuse Act was enacted for a

---

[69] WITTES ET AL., SEXTORTION, *supra* note 4, at 15.

[70] *Id*.

[71] 18 U.S.C. § 2241.

[72] 18 U.S.C. § 875.

[73] *Sextortion – Should It Be a Federal Crime?*, HG.ORG LEGAL RES., https://www.hg.org/legal-articles/sextortion-should-it-be-a-federal-crime-53756 (last visited Aug. 22, 2020).

[74] 18 U.S.C. § 875.

[75] *Sextortion – Should It Be a Federal Crime?*, *supra* note 73; *see also* 18 U.S.C. § 2261A (federal stalking law).

[76] 18 U.S.C. § 2261A.

[77] *Sextortion – Should It Be a Federal Crime?*, *supra* note 73.

[78] 18 U.S.C. § 1028A.

[79] 18 U.S.C. § 1030.

[80] Citron, *supra* note 39, at 1932.

[81] Erik De La Garza, *'Sextortion' Criminalized in Two States*, COURTHOUSE NEWS SERV., (Apr. 5, 2017), https://www.courthousenews.com/sextortion-criminalized-statute-two-states/.

[82] *Sextortion – Should It Be a Federal Crime?*, *supra* note 73.

[83] *See* Pam Greenberg, *Fighting Revenge Porn and 'Sextortion'*, NAT'L CONF. ST. LEG. (July 29, 2019), https://www.ncsl.org/research/telecommunications-and-information-technology/fighting-revenge-porn-and-sextortion.aspx.

completely different purpose than sextortion.[84] This creates a problem for victims of sextortion, whose injuries are markedly different from, for example, a company that loses its information in a data breach. This is not to undermine the harm that occurs from unauthorized hacking of any kind but to emphasize that different injuries need to be addressed differently by statute in order to afford victims proper recourse. The same can be said when prosecutors use the federal extortion law to prosecute sextortion related cases. The federal extortion statute was "designed to cover lower-grade extortions . . . [i]t is clearly aimed at extortions of money, not sex."[85] The two-year sentencing minimum may reflect "the limits of the legislature's imagination," indicating that this particular extortion law was meant to address a crime far less egregious than sextortion.[86]

Congress needs to pass a federal sextortion bill that addresses the elements of the crime in order to protect victims from the distinct harms of sextortion. The consequences of sextortion are unique because they include not only a loss of privacy and security but also a loss of agency, dignity, and personal safety. Victims experience extreme psychological trauma as a result of being forced to do unthinkable acts for their hackers; this affects their ability to succeed in school or maintain a job.[87] The harms that result from sextortion are so egregious that the loss of agency and dominion these victims endure can be compared to real-world sex crimes, such as human trafficking. These severe harms cannot be remedied by existing statutes. Until there is a federal sextortion statute, prosecutors are left to pick and choose from an unsatisfactory menu of state and federal laws that each separately address extortion, sexual assault, child pornography, and hacking.

i. Proposed Elements of a Federal Sextortion Statute

A federal sextortion statute should address both the cybersecurity and gender-based violence dimensions of the crime. For example, a federal statute should recognize that the crime involves the use of a computer to reach victims—via social media, email, or unauthorized hacking—while placing the sexual nature of the crime at its center. The law should specify that the kind of extortion in this crime involves leveraging victims' private images, videos, or materials stolen from spying on them in their homes. These images, videos, and other materials are used as blackmail in exchange for unconsented sexual favors that amount to sexual assault. To that end, the statute should treat the remote nature of the sexual assault as seriously as it would treat a physical-world sex crime.[88] The statute should also acknowledge the vast reach of sextortion both interstate and internationally.

---

[84] *See* Declan McCullagh, *From 'War Games' to Aaron Swartz: How U.S. Anti-hacking Law Went Astray*, CNET, (Mar. 13, 2013), https://www.cnet.com/news/from-wargames-to-aaron-swartz-how-u-s-anti-hacking-law-went-astray/ (highlighting how President Ronald Reagan expanded the Computer Fraud and Abuse Act to protect national defense secrets, and since then, the statute imposing felony penalties has been stretched to cover violations in terms of service and unauthorized access to password protected websites).

[85] BENJAMIN WITTES ET AL., CTR. FOR TECH. INNOVATION BROOKINGS, CLOSING THE SEXTORTION SENTENCING GAP: A LEGISLATIVE PROPOSAL 8 (2016), https://www.brookings.edu/wp-content/uploads/2016/05/sextortion2.pdf.

[86] *Id.*

[87] WITTES ET AL., SEXTORTION, *supra* note 4, at 2 ("[V]ictims reported signs of immense psychological stress, noting that they had 'trouble concentrating, appetite change, increased school and family stress, lack of trust in others, and a desire to be alone.'").

[88] WITTES ET AL., CLOSING THE SEXTORTION SENTENCING GAP, *supra* note 85, at 10 (designing a model federal sextortion statute that extends the definition of "sexual act" to coerced remote sexual acts and carries "sentences

Lastly, and most importantly, a federal statute should not treat the age of the victim as a core element of the crime.[89] While there are important reasons for affording children special protection under the law, it is not necessary that a federal sextortion statute treat age as an aggravating element. Because there are additional federal laws designed to combat various forms of juvenile sexual exploitation, a federal sextortion law should address sextortion equally for victims of any age. Allotting different sentences depending on the age of the victim might undermine the impact of sextortion on adult victims. For example, Anton Martynenko committed acts of sextortion against 155 young boys and received a 38-year sentence for producing child pornography.[90] Michael Ford, on the other hand, hacked into the computers of over a hundred adult women, obtaining images of them "undressing in changing rooms at pools, gyms, and clothing stores" and threatening to release them if they did not comply with his demands.[91] For some victims, Ford actually followed through on his threats, sending the images to the victims' friends and family.[92] Ford received 57 months' imprisonment, over 30 years less than Martynenko.[93]

Sextortion should also be treated as a felony rather than as a misdemeanor. Threatening to release personal or damaging information in exchange for money is the very definition of extortion, a felony in all fifty states.[94] Perpetrators of sextortion have a unique ability to control almost every aspect of a victim's life. By infiltrating victims' computers, sextortionists can gain access to victims' address books, emails, and passwords, as well as financial, medical, and personal data. Victims, even though they may never meet their perpetrators face-to-face, are effectively trapped. The forcible exchange of unconsented sexual conduct, images, or videos involved in the crime of sextortion constitutes conduct that is arguably more egregious than felony extortion and other sexual-privacy invasions such as up-skirting, which is treated as a misdemeanor in some states.[95] While sextortion includes the voyeuristic and offensive aspects of up-skirting, sextortion differs due to its longevity, combined with the underlying element of extortion. Victims of sextortion do not know how long they will be extorted by their hackers in a sexually invasive manner. In order to reflect the reprehensible nature of the crime, sextortion should be made a felony under federal law.

B. Creators of Malware Should Be Held Accountable

When Mijangos's lawyer was arguing to mitigate his client's punishment, one of his arguments was that Mijangos was not the one who actually created the virus that infected the

---

commensurate with a sex crime that will not, by its nature, involve serious physical injuries but routinely does involve serious psychological trauma for victims").

[89] WITTES ET AL., SEXTORTION, *supra* note 4, at 26.

[90] Citron, *supra* note 39, at 1917.

[91] *Former U.S. State Department Employee Sentenced to 57 Months in Extensive Computer Hacking, Cyberstalking, and "Sextortion" Scheme*, U.S. DEP'T JUST. (Mar. 21, 2016), https://www.justice.gov/opa/pr/former-us-state-department-employee-sentenced-57-months-extensive-computer-hacking.

[92] Citron, *supra* note 39, at 1917.

[93] *Id.*

[94] *Extortion*, FINDLAW, https://criminal.findlaw.com/criminal-charges/extortion.html (last updated Jan. 22, 2019).

[95] *See* Jessica Ravitz, *'Upskirt' Ban in Massachusetts Signed into Law*, CNN (Mar. 7, 2014), https://www.cnn.com/2014/03/07/justice/massachusetts-upskirt-bill/index.html (discussing that in Massachusetts, up-skirting—the act of photographing or recording a person's intimate parts under their clothing and without their consent—is now a misdemeanor punishable up to two and a half years in jail or a fine up to $5,000).

computers.[96] The defense attorney's argument correctly identified a gap in accountability: creators of the malware used to commit sextortion may face harsher consequences than sextortionists themselves. It is crucial that the actual perpetrators of sextortion are not excused for their actions merely because they did not create the software that helped them commit sextortion.

There does appear to be an opportunity to provide justice for victims by also holding the creators of malware accountable for the enabling role they play in sextortion. For example, one of the most popular RATs, Blackshades, was created for people who do not have hacking expertise.[97] In 2014, the FBI arrested two of the creators of Blackshades, along with 100 hackers using the program, after Cassidy Wolf spoke publicly about her experience as a victim of sextortion on the stage of the Miss Teen USA Pageant.[98] The perpetrator, James Abrahams, a high school classmate of Wolf's, had slaving devices on his computer that controlled the computers of as many as 150 girls and young women around the world.[99] Ultimately, he received an 18-month prison term after pleading guilty to computer hacking and extortion.[100] In contrast, consider Alex Yücel, the owner of Blackshades, who was sentenced to 57 months after the FBI raided the organization.[101] He was charged with computer hacking, conspiring to commit access device fraud, access device fraud, and aggravated identity theft.[102]

This gap in sentencing demonstrates two important points. First, it reinforces the fact that people who commit sextortion receive lower sentences because they are charged with crimes that do not actually address the harms of sextortion, such as Abraham's conviction for computer hacking and extortion. Second, it demonstrates that addressing the crime at its source can remove some harmful software from the internet and potentially deter future creators, as assigning liability to the creator of Blackshades for its role in the offense effectively shut down the operation.[103] Therefore, a federal sextortion statute should not only close the sentencing gap between offenders like Abrahams and creators like Yücel, but it should also assign contributory liability to creators who spread and promote software used to victimize others.[104] Where law enforcement may be unable to prosecute creators for actually committing sextortion, contributory liability can provide

---

[96] Risling, *supra* note 61.

[97] DIG. CITIZENS ALL., *supra* note 25, at 8.

[98] *Id.* at 10–12.

[99] *Id.* at 11.

[100] *Temecula Student Sentenced to Federal Prison in 'Sextortion' Case*, U.S. DEP'T JUST. (March 17, 2017), https://www.justice.gov/usao-cdca/pr/temecula-student-sentenced-federal-prison-sextortion-case.

[101] *Swedish Co-Creator of Blackshades Malware that Enabled Users Around the World to Secretly and Remotely Control Victims' Computers Sentenced to 57 Months in Prison*, FED. BUREAU INVESTIGATION (June 23, 2015), https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/swedish-co-creator-of-blackshades-malware-that-enabled-users-around-the-world-to-secretly-and-remotely-control-victims-computers-sentenced-to-57-months-in-prison [hereinafter *Blackshades Malware*].

[102] *Manhattan U.S. Attorney and FBI Assistant Director-in-Charge Announce Charges in Connection with Blackshades Malicious Software that Enabled Users Around the World to Secretly and Remotely Control Victims' Computers*, U.S. DEP'T JUST. (May 19, 2014), https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-and-fbi-assistant-director-charge-announce-charges-connection.

[103] Jeremy Kirk, *Swedish Man Sentenced for Powerful Blackshades Software*, COMPUTERWORLD (June 23, 2015), https://www.computerworld.com/article/2939955/swedish-man-sentenced-for-powerful-blackshades-malware.html.

[104] *Blackshades Malware*, *supra* note 101 ("Alex Yucel created, marketed, and sold software that was designed to accomplish just one thing—gain control of a computer, and with it, a victim's identity and other important information. This malware victimized thousands of people across the globe and invaded their lives. But Yucel's computer hacking days are now over.").

victims with a way to at least obtain monetary relief from those who enable and profit from sextortion.

Contributory liability is typically claimed in copyright infringement cases with the goal of holding an individual accountable for inducing or materially contributing to an infringing activity, even when the individual did not actually commit the infringing activity.[105] Liability is not found where the individual's product is widely used for legitimate purposes.[106] A contributory liability clause in a federal sextortion statute would hold creators of malware liable for materially contributing to sextortion. This would be a useful route for victims to obtain civil damages if their lawyer or law enforcement is able to locate the exact tool the hacker used when committing sextortion. Material contribution or inducement can be shown by presenting evidence of discourse in the hacking community surrounding the product or presenting evidence of the way the product is advertised. As a form of malicious software, RATs are created and primarily used to allow unsophisticated internet users to easily victimize hundreds of unsuspecting individuals.[107] While ethical hackers often study and learn how to use RATs in order to prevent the spread of malware, hackers who spread RATs to facilitate illegal activity should not be protected from contributory liability.[108] Including a contributory liability scheme in a federal sextortion statute would provide victims with an alternative route to relief in instances where the actual perpetrators are difficult to locate or prosecute. Moreover, it would both deter hackers from creating malware that easily facilitates sextortion and limit those creators' ability to indirectly profit from the remote sexual assault of so many victims.[109]

C. Changing the Discourse Surrounding Victims of Sextortion

When advocates and scholars were first educating lawmakers on nonconsensual pornography, both lawmakers and the public had to be convinced that nonconsensual pornography was not the fault of victims who entrusted their former partners with nude photos.[110] Similarly,

---

[105] *See Contributory Infringement*, CORNELL L. SCH.: LEGAL INFO. INST., https://www.law.cornell.edu/wex/contributory_infringement (last visited Dec. 27, 2020).

[106] Sony Corporation of America v. Universal City Studios Inc., 464 U.S. 417, 442 (1984).

[107] Akhil Sharma, *Introduction to RAT – Remote Administration Tool*, GEEKSFORGEEKS (June 8, 2020), https://www.geeksforgeeks.org/introduction-to-rat-remote-administration-tool/ ("Hackers use RAT only for illegal activities."); DIG. CITIZENS ALL., *supra* note 25, at 6 ("RATs are an easy to use, inexpensive tool frequently used to spy on women, and then exploit them for money and/or sexual favors. They are also a weapon of war used by enemies of democracy to target and attack their adversaries. RATs are frequently used in corporate espionage missions, allowing hackers to pull off many of the embarrassing and debilitating strikes against U.S. corporations.").

[108] DIG. CITIZENS ALL., *supra* note 25, at 34 ("There are plenty of videos that include ratters talking about getting victims, sharing public IP addresses, and featuring the faces of those whose devices they've slaved.").

[109] Any federal sextortion statute should also protect those caught in the crossfire of pervasive sextortion schemes. In the Mijangos case, for example, the hacker disguised malware used to commit sextortion as popular songs and videos that his victims unintentionally spread to their friends and family. Risling, *supra* note 61. The proposed federal sextortion statute should only hold liable those who either intentionally spread malware in order to facilitate sextortion or otherwise spread malware knowing that it is often used to commit sextortion.

[110] Citron, *supra* note 39, at 1945. This sort of pushback by lawmakers and the general public almost certainly finds its basis in longstanding societal views on sexuality, which often foster negative reactions toward sexual activity amongst "those who do not fall in line with heteronormativity." *Id.* at 1886–87. Unsurprisingly, then, "[s]exual-privacy invasions impact women and individuals from marginalized communities in distinctly damaging ways," effectively "entrenching a sense of subordination" while perpetuating outdated and misogynistic views on sexual privacy. *Id.* at 1876–77, 1891, 1894. Related "[s]ocial attitudes have also stymied reform efforts[, with s]ome contend[ing] that sexual privacy merits no attention because sexual-privacy invasions involve problems of victims'

with sextortion, advocates will need to educate lawmakers that invading computers, stealing private images, and spying on naked bodies and sexual activity is not the fault of victims who have a right to exist freely in the safety of their own homes. A federal sextortion law would educate society about "what behavior is harmful and what behavior is unacceptable" and that "publicly exposing a single aspect of one's intimate life does not mean that all aspects are meant for public consumption."[111]

In arguing for a lenient sentence, Mijangos's defense attorney argued that his client was not the one who actually created the photos used to extort his victims.[112] This argument reflects the tenuous line drawn between ownership, possession, and distribution of private images as well as the meaning of "consensual" and "non-consensual." Mijangos hacked into hundreds of computers, stole private images taken and owned by victims, and used them as ammunition to blackmail victims. His defense's argument that Mijangos did not actually create the images himself reflects a widely held belief in sexual assault culture that the victim is to blame for putting themselves in a vulnerable position to start.

This may explain why there is a severe sentencing disparity between the perpetrators of sexploitation against adults and against children. While the federal government views children as needing special protection from sexual exploitation, adult victims are viewed differently because adult pornography is "constitutionally protected speech."[113] This implies that, because the law protects adult women who consent to creating images or videos depicting sex or nudity, those women assume the risk that a hacker may use those materials to harass, intimidate, or control them.[114] Such attitudes result in the disparate treatment of victims of the same crime.[115] This suggests that in the eyes of the law, because adults have agency in their decisions—whether it is the decision to take a nude photo or click on a link that happens to be malware—they are less deserving of the kind of protection that young victims receive in identical situations. When juveniles are victims of sex crimes, they are taught that it is not their fault, that they are not to be blamed for bad actors who target them as vulnerable. But the prevalence of remote sexual assault indicates that adult women are also vulnerable to improperly regulated online sex crimes regardless of their intelligence or decision-making abilities. It is crucial for victims to know that it is not their fault, and they are not alone.[116]

---

making." *Id.* at 1875–76. Put more bluntly, "[s]aying that victims 'asked for it' is just another way that society has long trivialized harms suffered by people from marginalized communities." *Id.* at 1876.

[111] *Id.* at 1944–45. While this normative effect would ideally prevent victimization across all demographics, it could offer particular protection for sex workers, whose livelihoods presumably depend on their ability to control their sexual autonomy online.

[112] Risling, *supra* note 61.

[113] WITTES ET AL., SEXTORTION, *supra* note 4, at 26.

[114] As such, the law can be seen as perpetuating a longstanding misogynistic sense of entitlement that men may feel toward women's bodies, particularly as women mature from childhood into adulthood and become subject to increased sexualization. *See supra* note 110 and accompanying text (critique of victim-blaming and underlying issues of subordination as often experienced by women and members of marginalized communities in conjunction with invasions of their sexual privacy).

[115] WITTES ET AL., SEXTORTION, *supra* note 4, at 26.

[116] DIG. CITIZENS ALL., *supra* note 25, at 9 ("There's a lot of shame in it, particularly when it involves compromising videos or images. I think it is important for victims to know how prevalent it is, how even security researchers fall victim to these sorts of attacks. You haven't done anything stupid or shameful; using technology in a completely secure way these days is all but impossible.").

IV. CONCLUSION

The policy proposals that have been put forth in this article are only intended as a starting point for reform, and it is important to recognize that they do not provide the perfect solution for combatting sextortion. This article acknowledges the systemic harm of mass incarceration[117] and cautions that explicitly criminalizing sextortion without putting in place corresponding preventative measures could prove ineffective in eradicating sextortion while also contributing to the United States' growing prison population. Although there is very little data available on whether sextortionists are prosecuted disproportionately across race or socioeconomic lines, the potential for harm to people of color remains pervasive. This inherent tension means that preventative measures, coupled with further research into demographic risk factors, are crucial.

The rapid rise of sextortion, contrasted against the lack of relevant empirical data, suggests a collective failure by lawmakers, cybersecurity experts, and other stakeholders to effectively define, study, and understand the crime with a view toward oversight and prevention.[118] Outreach efforts like comprehensive in-school sexual education programs that educate young people about sexual violence, including online sexual violence such as sextortion, can be helpful. While some sexual education programs already exist and have proven effective, many do not directly address sextortion.[119] Separately, evidence-based intervention and prevention programs might also save victims from the harms of sextortion while reducing the need for incarceration, but such measures must be intersectional and inclusive of race, socioeconomic class, gender identity, and sexual orientation to maximize their effectiveness.

The increasing pervasiveness of sextortion should not have been surprising to lawmakers or law enforcement. It is a byproduct of new technology used to facilitate an age-old crime. The slow response to the crime of sextortion is consistent with how gender-based violence has been viewed and treated over time: cloaked in shame as an incident that the victim could have prevented or even brought upon themselves.[120] The Department of Justice, Federal Bureau of Investigation, and state governments should provide education to stakeholders as well as the average internet user about the intersections between technology and gender-based violence.[121]

Sextortion is a cybersecurity and gender-based violence issue, requiring stakeholders from the legal and cybersecurity world[122] to come together to combat this threat. "The same

---

[117] The United States has 2.3 million people in jail and prison today, with Black and Latino men largely overrepresented in that population. *Mass Incarceration*, ACLU, https://www.aclu.org/issues/smart-justice/mass-incarceration (last visited Jan. 14, 2020).

[118] *See, e.g.*, Wolak et al., *Sextortion of Minors, supra* note 47, at 2 ("Despite concerns about youth vulnerability to sextortion, there is little empirical research about its characteristics and dynamics.").

[119] *Id.* at 7.

[120] *See Rape Culture, Victim Blaming, and the Facts*, SOUTHERN CONN. ST. U.: INSIDE SOUTHERN, https://inside.southernct.edu/sexual-misconduct/facts (last visited Aug. 23, 2020).

[121] *See* ROBERT J. DEIBERT ET AL., CITIZEN LAB, MUNK SCH. GLOB. AFFS., U. TORONTO, SUBMISSION TO THE SPECIAL RAPPORTEUR ON VIOLENCE AGAINST WOMEN 17–18 (2017), https://citizenlab.ca/wp-content/uploads/2017/11/Final-UNSRVAG-CitizenLab.pdf ("Most legal professionals, law enforcement, and frontline workers do not receive basic training on the intersections between technology and violence against women, despite the fact that acts of gender-based violence, harassment and abuse are increasingly likely to have a technological nexus.").

[122] *See id.* at 7–8 (recommending the creation of encryption and anonymity tools to protect women from gender-based violence online). "[W]hile encryption and anonymity tools can be used as shields by perpetrators of harassment, they are also vital to human rights and to members of groups vulnerable to technology facilitated

cybersecurity vulnerabilities that are making our corporations and government agencies ripe for cyber exploitations from foreign intelligence agencies and hackers are making teenagers and young adults ripe for highly-remote sexual exploitations."[123]

Beyond education and visibility, fighting sextortion must become a priority in the criminal justice system. In this regard, the most effective approach for combatting sextortion is to create an interstate federal sextortion law that uniformly protects adults and children from sextortion. This statute would put perpetrators on notice that there are consequences for remote sexual assault, even for those hiding behind a computer. By creating a statutory mechanism to prevent the easy facilitation of sextortion, lawmakers can ensure that victims have access to a criminal justice system committed to protecting them while law enforcement can more effectively seek justice for victims and survivors.

violence, harassment, and abuse, who can use [these] tools to ensure their privacy in the face of harassment." *Id.* at 7 (internal quotations omitted). Although law enforcement "continue[s] to raise [the] alarm about the rise of strong encryption and anonymity tools, arguing that they pose a threat to their ability to conduct investigations online . . . there is no data to support the claim that strong encryption poses an insurmountable barrier in the vast majority of criminal investigations, and an increasingly large range of alternative measures and data sources remain available to law enforcement." *Id.* at 8.

[123] WITTES ET AL., SEXTORTION, *supra* note 4, at 13.