

Combating Cyber Sexual Abuse

A Manual for Advocates

Prepared by:

New York Cyber Sexual Abuse Task Force

Last updated May 7, 2019

This Manual is a collaboration of gender-based violence advocates and other professionals in New York City who have seen an increase in instances of cyber sexual abuse in our practice and who identified a need for a comprehensive manual for advocates. This manual does not constitute legal advice. It is intended to provide an overview of both legal and non-legal ways to advocate for clients who have been victims of cyber sexual abuse. It is important to note that both technology and the law in this area are evolving rapidly and so advocates should use this Manual as a foundation only and should always look for updates in statutory and case law when advocating for victims of cyber sexual abuse.

TABLE OF CONTENTS

INTRODUCTION 6

 I. What is Cyber Sexual Abuse?..... 6

 II. Scope of Manual 6

PART 1- CRIMINAL LEGAL REMEDIES FOR VICTIMS OF CSA 8

 I. New York State and New York City Criminal Law 8

 A. NYC Unlawful Disclosure Law 9

 B. New York State Criminal Law 13

 C. Supporting Victims of Cyber Sexual Abuse Who Report to Law Enforcement 16

 II. Federal Criminal Law 23

 A. Computer Fraud and Abuse Act, 18 U.S.C. § 1030 24

 B. Aggravated Identity Theft, 18 U.S.C. § 1028A 25

 C. Federal Wiretap Act, 18 U.S.C. § 2520 26

 D. Interstate Stalking or Harassment, 18 U.S.C. § 2261A 26

 E. Interstate Threats or Extortion, 18 U.S.C. § 875 28

 F. Obscene or Harassing Telephone Calls in Interstate or Foreign Communications, 47 U.S.C. § 223 29

 G. Video Voyeurism Prevention Act of 2004, 18 U.S.C. § 1801 29

PART 2 - CIVIL LEGAL REMEDIES FOR VICTIMS OF CSA 30

 I. Family Court Orders of Protection 30

 A. Overview of Family Court Civil Orders of Protection 30

 B. Procedure for Obtaining a Civil Order of Protection 31

 II. New York State and New York City Civil Causes of Action..... 33

 III. Federal Civil Causes of Actions 36

 A. Cases Against Governmental Entities 36

 B. Cases Against Non-Governmental Entities 39

PART 3 - DESCRIPTION OF RELEVANT SOCIAL MEDIA/ APPLICATIONS AND ASSOCIATED ABUSE..... 44

 I. Overview 44

 II. Phone and Messaging Platforms 44

 A. WhatsApp 44

 B. Skype 44

 C. WeChat 45

 III. Social Media 47

A.	Facebook.....	47
B.	Instagram	48
C.	Snapchat.....	48
D.	Twitter	49
E.	LinkedIn.....	50
F.	Flickr.....	51
G.	Tumblr	51
H.	YouTube	53
IV.	Pornography Websites	54
V.	Dating Websites	54
A.	Match.com	54
B.	Tinder.....	55
C.	Grindr.....	56
D.	Seeking Arrangement	57
E.	Craigslist.....	58
VI.	Google Search Results	58
VII.	Other	59
A.	Reddit.....	59
VIII.A	Note on Liability for Social Media Providers	60
PART 4 -	EVIDENCE COLLECTION	61
I.	Prior to Litigation: Active Steps Clients Can Take to Preserve Evidence.....	61
II.	Important Considerations During Litigation.....	66
A.	Litigation Hold Requests	66
B.	Organizing Evidence	66
C.	Presenting Evidence at Trial.....	67
D.	Admissibility	68
E.	Authenticity	69
F.	Self-Authentication.....	69
G.	Hearsay Rules/How to Introduce ESI.....	70
PART 5 -	COPYRIGHTING AND REMOVING IMAGES AND VIDEOS FROM THE WEB	72
I.	Understanding the Process	72
A.	Background and Initial Considerations	72
B.	Registering a Copyright with the Copyright Office	72
C.	Benefits of Registration	73

D.	DMCA; DMCA Complaints and Takedown Notices.....	74
E.	Takedowns and Subpoenas.....	75
F.	De-Indexing from Google	76
G.	Impact of Court Orders.....	79
PART 6 -	TECHNOLOGY SAFETY PLANNING AND BEST PRACTICES	80
I.	General Safety Tips: The “Digital Breakup Plan”	80
II.	Securing Cell Phones and Tablets.....	81
III.	Computers, E-mail, and Online Browsing.....	83
IV.	Social Media Accounts	84
V.	Credit Cards and ID Theft.....	85
VI.	Nonconsensual Pornography: Images and Videos.....	86
VII.	Detecting Spyware	86
PART 7 -	RESOURCES.....	89
A.	Directory of Useful Websites.....	89
B.	Directory of Service Organizations	90
PART 8 -	APPENDICES.....	93

INTRODUCTION

I. What is Cyber Sexual Abuse?

Perpetrators of intimate partner violence are increasingly using online platforms or other digital technologies to abuse, exploit, harass, and threaten their victims.¹ This type of abuse includes an array of harassment such as hacking, installation of spyware, stalking, spoofing,² identity theft, impersonation (including deep fakes³), sexual extortion (colloquially known as sextortion), and the nonconsensual distribution or threat of distribution of sexually explicit images and videos (hereinafter referred to as “cyber sexual abuse” or “CSA”).

Cyber sexual abuse, or CSA, is also commonly known as “revenge porn” or “nonconsensual pornography” or “NCP”. Images and videos that become the fodder of cyber sexual abuse may have been obtained consensually within the context of an intimate relationship or without consent (e.g., by using hidden cameras, hacking phones, or recording sexual assaults). The term “revenge porn,” though frequently used, is somewhat misleading. In many cases, perpetrators are not motivated by revenge or by any personal feelings toward the victim. In addition, the term “revenge porn” is victim blaming in that it implies that the victim committed an act that ought to be avenged, or that the victim did something to warrant or deserve the abusive treatment. For these reasons, some advocacy organizations prefer the broader and less problematic terms cyber sexual abuse or nonconsensual pornography.

With the ubiquitous use of social media platforms and growing ease of electronic communication, perpetrators of cyber sexual abuse and other forms of technology abuse are able to inflict major and lasting damage very quickly. The harms caused by cyber sexual abuse are pervasive and persistent and can bleed into every aspect of a victim’s life, seriously impairing a victim’s physical, emotional, and economic well-being. As technology grows more advanced and more accessible, new forms of abuse develop and proliferate rapidly. Unfortunately, technology moves faster than statutes and case law, and often faster than judges and juries as well. Lawyers and advocates must therefore be creative and adaptable in their approach to serving victims.

II. Scope of Manual

This Manual is meant to provide an overview of the various types of technology abuse, including a focus on cyber sexual abuse, and serve as a resource for attorneys and advocates representing victims of these forms of abuse. Given that this area of law is evolving, attorneys and advocates should be sure to always check for updates in the law when assisting victims.

¹ This article will use the terms perpetrator, abuser, and defendant interchangeably.

² “Spoofing” is the disguising of a sender’s identity so that the recipient believes the sender is someone else.

³ The term “deep fake” refers to digital manipulation of sound or images to impersonate another person and make it appear that the impersonated person did something, often of a sexual nature, that the person did not actually do. Deep fakes are perpetrated in a manner that appears so realistic that an unaided observer cannot detect the fake.

The Manual first provides an overview of state and federal criminal law and civil law as they relate to cyber sexual abuse. It then summarizes the platforms on which cyber sexual abuse campaigns are often conducted. Next, it provides overviews of state and federal criminal and civil law as they relate to cyber sexual abuse. It then explores the use of the Digital Millennium Copyright Act (“DMCA”) and other remedies to combat the disclosure of intimate images. Finally, it offers best practices to safeguard survivors’ digital lives.

PART 1- CRIMINAL LEGAL REMEDIES FOR VICTIMS OF CSA

The law governing cyber sexual abuse is an imperfect web of state and federal laws. Unfortunately, there is no federal cyber sexual abuse law. However, both New York City and New York State have passed laws addressing cyber sexual abuse in the last few years. In February 2019, both the New York Senate and Assembly passed a cyber sexual abuse law on the state level; however, as of April 2019, the law has not been signed by the Governor (though it is fully expected to be signed).⁴

New York City, by contrast, was the first city in the country to pass its own nonconsensual disclosure law to protect survivors of cyber sexual abuse, therefore victims within the jurisdiction of New York City have an additional option available to them.

I. New York State and New York City Criminal Law

Only a handful of states have not yet passed a law making it a crime to disseminate sexual images without the depicted person's consent. New York State recently joined the vast majority of states – forty-four states and the District of Columbia – who criminalize this type of cyber sexual abuse in some shape or form.⁵

On February 28, 2019, the New York State Senate and New York State Assembly unanimously passed A. 5981 / S. 01719-C, which criminalizes the non-consensual disclosure of the still or video image of a victim's intimate parts, or the victim engaging in sexual conduct, with the intent to cause harm to the emotional, financial, or physical welfare of the victim. The penalty for a violation of this provision is an A Misdemeanor. The law also amends the Family Court Act to add the family offense of unlawful dissemination or publication of an intimate image. The law further creates a private right of action for victims to seek money damages against perpetrators; victims are also empowered to seek injunctive relief to seek a court order to require any website hosting or transmitting a victim's image to permanently remove these images.⁶

On the City level, New York City is the only city in the nation to have a specific anti-cyber sexual abuse law. On November 16, 2017, the New York City Council unanimously approved legislation criminalizing the nonconsensual disclosure of intimate images (the "NYC Unlawful Disclosure Law"). Criminal penalties went into effect on February 15, 2018.⁷ The legislation also

⁴ Vivian Wang, 'Revenge Porn' Law Finally Passes in New York, N.Y. TIMES (Feb. 28, 2019), <https://www.nytimes.com/2019/02/28/nyregion/revenge-porn-law.html>.

⁵ *44 States + DC Have Revenge Porn Laws*, CYBER CIVIL RIGHTS INITIATIVE <https://www.cybercivilrights.org/revenge-porn-laws/> (last visited May 6, 2019).

⁶⁶ See A.0719 Text, NEW YORK STATE ASSEMBLY https://assembly.state.ny.us/leg/?default_fld=&leg_video=&bn=S01719&term=2019&Text=Y (last visited May 6, 2019).

⁷ NYC Administrative Code 10-180.

creates a civil cause of action that allows survivors to sue perpetrators for damages and other relief.⁸ Section A of this Part, below, provides an analysis of the NYC Unlawful Disclosure Law criminal penalty. Section II of Part 2 - Civil Legal Remedies for Victims of CSA summarizes the civil remedy available under the new legislation.

A. NYC Unlawful Disclosure Law

On November 16, 2017, the New York City Council unanimously approved legislation criminalizing the nonconsensual disclosure of intimate images. The legislation is now codified as New York City Administrative Code 10-180.⁹ The NYC Unlawful Disclosure Law makes it unlawful to disclose, or threaten to disclose, intimate images with the intent to cause harm, where the individual depicted is or would be identifiable from the image.¹⁰ Unlawful Disclosure is categorized as a misdemeanor and is punishable by up to one year in jail, a fine of \$1,000, or both.¹¹

1. *Elements of the Law*

There are five elements of the NYC Unlawful Disclosure Law, labeled (a) through (e) below.

(a) Disclose or Threaten to Disclose

Under NYC Admin. Code 10-180, “[i]t is unlawful for a covered recipient to disclose an intimate image, without the depicted individual’s consent” Importantly, it is also unlawful “for a covered recipient to make a threat to disclose intimate images. The inclusion of threats in the New York City law is important because abusers often use the threat of dissemination in order to exert control over their victims.¹² Inclusion of the threat provision helps to ensure that advocates and prosecutors can intervene *before* the disclosure of the material, after which removal of the material may be challenging, if not impossible, if it has been disseminated widely on the Internet.

⁸ See NYC Administrative Code 10-180.

⁹ See Melanie Ehrenkranz, *Revenge Porn is Officially Punishable by Law in New York City*, GIZMODO (Feb. 15, 2018, 2:40 PM), <https://gizmodo.com/revenge-porn-is-officially-punishable-by-law-in-new-yor-1823039186>.

¹⁰ NYC Administrative Code 10-180 §§a.-c. “Unlawful disclosure of an intimate image” was renumbered as 10-180 by Local Law 2018/192, effective 3/1/19. See <https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3464946&GUID=F0FDC8E0-A95E-4888-9407-94B676F79650>.

¹¹ NYC Administrative Code 10-180 §c.

¹² The threat to disseminate sexually explicit images is also treated as an offense equivalent to actual dissemination of such images under the provisions of cyber sexual abuse laws in Texas and West Virginia. See Texas Penal Code Ann. § 21.16(c); West Virginia Code §61-8-28a(b).

The NYC Unlawful Disclosure Law defines “disclose” to mean (i) “disseminate” as it is defined in subdivision 5 of section 250.40 of the New York penal law or (ii) “publish” as it is defined in subdivision 6 of section 250.40 of the New York penal law.¹³ Thus, “disclose” means:

- Disseminate: “To give, provide, lend, deliver, mail, send, forward, transfer or transmit, electronically or otherwise to another person;” or
- Publish: “To (a) disseminate, as defined in subdivision five of this section, with the intent that such image or images be disseminated to ten or more persons; or (b) disseminate with the intent that such images be sold by another person; or (c) post, present, display, exhibit, circulate, advertise or allows access, electronically or otherwise, so as to make an image or images available to the public; or (d) disseminate with the intent that an image or images be posted, presented, displayed, exhibited, circulated, advertised or made accessible, electronically or otherwise and to make such image or images available to the public.”¹⁴

(b) Intimate Image

An intimate image is a “photograph, film, videotape, recording or any other reproduction of an image of a depicted individual.” A depicted individual is “an individual depicted in a photograph, film, videotape, recording or any other reproduction of an image that portrays such individual (i) with fully or partially exposed intimate body parts, (ii) with another individual whose intimate body parts are exposed, as recorded immediately before or after the occurrence of sexual activity between those individuals, or (iii) engaged in sexual activity.” Intimate body parts include “the genitals, pubic area or anus of any person, or the female nipple or areola of a person who is 11 years old or older.”¹⁵

(c) Without Consent

The law applies where a perpetrator discloses or threatens to disclose an image “in a manner in which, or to a person or audience to whom, the depicted individual intended it would not be disclosed, at the time at which the covered recipient gained possession of, or access to, the intimate image.”¹⁶ Essentially, this means that where a depicted individual did not intend for a photo to be disclosed at the time the image was taken or sent (even if the depicted individual consented to the actual taking of the image) the NYC Unlawful Disclosure Law applies.

¹³ NYC Administrative Code 10-180.

¹⁴ N.Y. Penal Law § 250.40.

¹⁵ NYC Administrative Code 10-180.

¹⁶ *Id.*

(d) Intent to Cause Harm

The perpetrator must disclose or threaten to disclose with “intent to cause economic, physical or substantial emotional harm to [the] depicted individual.”¹⁷ This intent may be evinced through contemporaneous messages with the image or video (e.g., a text saying, “I’ll show the whole world you’re a slut” or “I’m gonna get you fired”), statements made by the perpetrator to the victim, or other surrounding circumstances that would show that the perpetrator intended harm. Arguably, the content of the photo or image itself could belie an intent to cause harm, along with its intended audience. Even without statements, sending a naked image to an employer could imply that the perpetrator sought to cause economic harm to the victim by getting them in trouble at work or having them fired.

(e) Identifiability

For the actual disclosure of images, a depicted individual is “identifiable” if the victim “is or would be identifiable to another individual either from the intimate image or from the circumstances under which such image is disclosed.” Importantly, for threatened disclosure of images, the standard is different — a depicted individual is “identifiable where the covered recipient states or implies that such person would be so identifiable.”¹⁸

2. *Exceptions to the law*

There are four primary exceptions to when and where the law applies — three explicit exceptions and one that is not explicit but is included elsewhere in the statute.

(a) Law Enforcement Exception — “Such disclosure or threat of disclosure is made in the course of reporting unlawful activity, in the course of a legal proceeding or by law enforcement personnel in the conduct of their authorized duties.”¹⁹ For example, if an individual is reporting the sending of an intimate image to the police, showing the image to the police or sending the image to the police would not in itself violate NYC Admin. Code 10-180. Similarly, if law enforcement sends the photo internally or collects the photo as a part of their law enforcement duties, this disclosure would not be covered under the law.

(b) Communications Decency Act (CDA) Section 230 Exception — “Such disclosure is made by a provider of an interactive computer service, as defined in paragraph (2) of subsection (f) of section 230 of title 47 of the United States code, with regard to content provided by another information content provider, as defined in paragraph (3) of such subsection.”²⁰ This exception merely restates what is already codified under federal law within the CDA, which limits the liability of Internet service providers for posts made by individuals on content providers’ websites

¹⁷ *Id.*

¹⁸ *Id.*

¹⁹ *Id.*

²⁰ *Id.*

or applications (i.e., Facebook, Grindr, Craigslist, and others). There is no liability for the content provider, only for the individuals posting on the websites or applications.

(c) Matters of Legitimate Public Concern — “Such disclosure or threat of disclosure is made in relation to a matter of legitimate public concern or is otherwise protected by the first amendment of the United States constitution.”²¹ Attorneys and advocates have interpreted this exception to be narrowly referring to intimate images or videos that have important public concern (e.g., the photograph of then nine-year-old Phan Thi Kim Phuc running naked on a road after being severely burned on her back by a napalm attack).²²

(d) Public Place Exception — “An intimate image does not include any image taken in a public place as defined in section 240.00 of the New York penal law, except if, at the time the image was recorded, an individual in the depicted individual’s position would reasonably have believed that no one other than the covered recipient could view the applicable intimate body parts or sexual activity while such body parts were exposed or such activity was occurring.”²³ An image or video is not protected under the statute if it was taken in a public place unless the victim knew or reasonably should have known that no one other than the perpetrator could see their body parts or sexual activity. Unfortunately, this applies even if an image or video was taken as a result of coercion, under duress, or even in conjunction with a sexual assault.

3. Challenges

The “intent to cause harm” element of the NY Unlawful Disclosure Law may pose challenges in proving charges of unlawful disclosure of an intimate image, as it creates an additional layer of *mens rea* requiring that the perpetrator must have intended to cause harm to the victim in order to be guilty of the offense.²⁴ Such an intent standard may be difficult for prosecutors to prove and simple for perpetrators to evade. Perpetrators can be driven by, or claim to be driven by, a number of motivations, including a desire for financial gain, for laughs, for “likes” or “retweets,” to show off to friends, for entertainment, for sexual gratification, or for no particular reason at all.²⁵

²¹ *Id.*

²² *100 Photos*, TIME, <http://100photos.time.com/photos/nick-ut-terror-war> (last accessed Aug. 1, 2018).

²³ *Id.*

²⁴ To be clear, an “intent to cause harm” *mens rea* requirement is separate and apart from the general *mens rea* required to undertake the disclosure/distribution/publication act required for the crime. By way of example, the Utah law has both: “An actor commits the offense of distribution of intimate images if the actor, with the intent to cause emotional distress or harm [the “intent to harm” provision], knowingly or intentionally [the general *mens rea* provision] distributes to any third party any intimate image of an individual . . .” Utah Criminal Code § 76-5b-203 (emphasis added). A general *mens rea* requirement of knowledge or reckless disregard is preferred for a strong criminal framework.

²⁵ See Carrie Goldberg, *Seven Reasons Illinois is Leading the Fight Against Revenge Porn*, CCRI (Dec. 31, 2014), <https://www.cybercivilrights.org/seven-reasons-illinois-leading-fight-revenge-porn/>; see also DR. ASIA A. EATON, DR. HOLLY JACOBS & YANET RUVALCABA, CCRI, 2017 NATIONWIDE ONLINE STUDY OF NONCONSENSUAL PORN VICTIMIZATION AND PERPETRATION: A SUMMARY REPORT 24 (June 2017), <https://www.cybercivilrights.org/wp->

Additionally, attorneys and advocates expect that perpetrators will utilize the broad “legitimate public concern” exception to attempt to deflect unlawful disclosure charges and claim First Amendment defenses under the law. Finally, attorneys and advocates will need to find additional venues to seek justice for victims who were recorded in a public place, as the current law exempts protection for these victims.

B. New York State Criminal Law

New York State Senate and Assembly recently passed legislation criminalizing cyber sexual abuse on a state level; as of the writing of this Manual in April 2019, however, the bill has not yet been signed by the Governor.

Since New York State’s new cyber sexual abuse law has not yet been signed into law, prosecutors currently deploy a mixture of criminal laws to address behavior like stalking, coercion, witness tampering and harassment in the context of cyber sexual abuse. For example, in 2013, a 29-year-old man from Brooklyn posted naked photographs of his ex-girlfriend on his Twitter account and sent these photos to her employer and her sister. In the absence of a statute prohibiting cyber sexual abuse, the District Attorney’s office combined charges consisting of three misdemeanors: aggravated harassment, dissemination of unlawful surveillance and public display of offensive sexual material. Considering a motion to dismiss the charges, the judge described the perpetrator’s conduct “reprehensible.” But, constrained by the laws on the books, the judge felt compelled to find that the perpetrator’s conduct did not technically violate any of the criminal statutes under which he was charged: the perpetrator had not directly communicated with the victim, as required for harassment; he had not obtained the pictures unlawfully, as required by unlawful surveillance; and, according to the Court, he had not publicly displayed offensive sexual material, because Twitter did not amount to public display, and nudity alone did not constitute “offensive sexual material.”²⁶ The case was dismissed.

The below listed sections of the New York Penal Code could potentially address cyber sexual abuse. These are some of the more common penal law provisions that may be utilized to address cyber sexual abuse. There may be others depending on the specific facts of the case.

1. Unlawful surveillance — N.Y. Penal Law §§ 250.45, 250.50
2. Dissemination of an unlawful surveillance image — N.Y. Penal Law §§ 250.55, 250.60
3. Harassment in the second degree — N.Y. Penal Law § 240.26
4. Coercion — N.Y. Penal Law §§ 135.60, 135.65

content/uploads/2017/06/CCRI-2017-Research-Report.pdf (describing a survey finding that the most commonly reported reason for having shared intimate images of another person without consent was “I was just sharing the image(s) with my friends and didn’t intend to hurt the person”).

²⁶ *People v. Barber*, 992 N.Y.S.2d 159 (N.Y.C. Crim. Ct. N.Y. Cty. 2014).

5. Stalking — N.Y. Penal Law §§ 120.45, 120.50, 120.55, and 120.60
 6. Sexual offenses, including sexual misconduct, forcible touching, sexual abuse in the third degree, sexual abuse in the second degree, sexual abuse in the first degree — N.Y. Penal Law §§ 130.20, 130.52, 130.55, 130.60, and 130.65
 7. Witness tampering and intimidation — N.Y. Penal Law §§ 215.10–.17
 8. Criminal contempt — N.Y. Penal Law §§ 215.50–.52
1. *Unlawful Surveillance and Dissemination of an Unlawful Surveillance Image* — N.Y. Penal Law §§ 250.45, 250.50, 250.55, 250.60

“Unlawful surveillance” may be applicable where a victim was recorded, without his or her knowledge or consent, while undressing or otherwise showing his or her intimate or sexual parts, in a location where he or she had a reasonable expectation of privacy.²⁷ However, there are specific intent elements that must be proven for this crime depending on the section of the statute under which the conduct falls, including “for [the abuser’s] own, or another person’s amusement, entertainment, or profit, or for the purpose of degrading or abusing a person” or “for [the abuser’s] own, or another person’s sexual arousal or sexual gratification.”²⁸ Dissemination of an unlawful surveillance image applies where an individual intentionally disseminates images that were obtained through unlawful surveillance.

It is important to note that for either crime to be applicable, the victim must have been recorded *without his or her knowledge or consent*, which excludes a large number of victims who were aware of the recording or photo imaging but did not consent, or who had consented to sending images or videos of themselves. In practice, due to the various elements that must be satisfied for an unlawful surveillance, it can be difficult to have successful prosecutions under either section of the penal code.

2. *Harassment in the Second Degree* — N.Y. Penal Law § 240.26

The elements of harassment in the second degree include a perpetrator evincing an intent to harass, annoy or alarm another person while engaging in a course of conduct or repeatedly committing acts which alarm or seriously annoy such other person and which serve no legitimate purpose. Where an abuser has repeatedly threatened to disseminate, or actually disseminated, images, video, or other media of cyber sexual abuse, the abuser may be liable under harassment in the second degree.

However, harassment in the second degree requires a pattern of conduct, not just one devastating post, which means that stand-alone incidents of cyber sexual abuse would likely not fall under this section of the penal code.

²⁷ N.Y. Penal Law § 250.45.

²⁸ *Id.*

3. Coercion — *N.Y. Penal Law §§ 135.60, 135.65*

A person is guilty of coercion in the second degree when the person either: (a) “compels or induces [the victim] to engage in conduct which [the victim] has a legal right to abstain from engaging in,” (b) “compels or induces [the victim] to abstain from engaging in conduct in which he or she has a legal right to engage,” or (c) “compels or induces [the victim] to join a group, organization or criminal enterprise which [the] person has a right to abstain from joining”²⁹ Additionally, the defendant must compel or induce the victim “by means of instilling in [the victim] a fear that, if the demand is not complied with, the actor or another will” engage in certain conduct, such as committing a crime, “[e]xpos[ing] a secret or publiciz[ing] an asserted fact, whether true or false, tending to subject some person to hatred, contempt or ridicule,” or “[p]erform[ing] any other act which would not in itself materially benefit the actor but which is calculated to harm another person materially with respect to his or her health, safety, business, calling, career, financial condition, reputation or personal relationships.”³⁰

Coercion may be applicable where an abuser threatens to disseminate intimate images or video to a victim’s employer, family, or friends if the victim does not remain in a relationship with the abuser, does not come back to the abuser, or does not give the abuser custody of their shared child. Unlike harassment or stalking, there is no course of conduct needed for coercion—one incident would likely be sufficient.

4. Stalking — *N.Y. Penal Law §§ 120.45, 120.50, 120.55, and 120.60*

A person is guilty of stalking when he intentionally and for no legitimate purpose, engages in a “course of conduct” directed at a person that he knows or reasonably should know “causes material harm to the mental or emotional health of such person, where such conduct consists of following, telephoning, initiating communication . . . with such person . . . or a third party with whom such person is acquainted.”³¹ For purposes of the statute, a “course of conduct [is] a pattern of conduct composed of a series of acts over a period of time, however short, evidencing a continuity of purpose.”³² While the “course of conduct” must be directed at harming the victim, such conduct can include harmful communications made to third parties.³³

Where an abuser has engaged in repeated acts of threats to post or release intimate images, stalking may be applicable. Cyber sexual abuse may also fall under section 120.45(3), which

²⁹ N.Y. Penal Law § 135.60.

³⁰ N.Y. Penal Law §§ 135.60. Additionally, a person is guilty of coercion in the first degree under New York Penal Law §§ 135.65 when he or she commits coercion in the second degree and either “commits such crime by instilling in the victim a fear that he or she will cause physical injury to a person or cause damage to property;” or “compels or induces the victim to: (a) [c]ommit or attempt to commit a felony;” “(b) [c]ause or attempts to cause physical injury to a person; or (c) violate his or her duty as a public servant.”

³¹ N.Y. Penal Law § 120.45(2).

³² *People v. Payton*, 161 Misc. 2d 170 (N.Y.C. Crim. Ct. Kings Cty. 1994).

³³ See N.Y. Penal Law § 120.45(2).

proscribes certain conduct that “is likely to cause such person to reasonably fear that his or her employment, business or career is threatened” (e.g., where an abuser threatens to send intimate images or videos to employers, businesses, schools, or post intimate images or videos online to hurt a victim’s standing in the community).

5. *Sexual Offenses, including Sexual Misconduct, Forcible Touching, Sexual Abuse in the Third Degree, Sexual Abuse in the Second Degree, Sexual Abuse in the First Degree – N.Y. Penal Law §§ 130.20, 130.52, 130.55, 130.60, and 130.65*

Where an intimate image or video depicts a nonconsensual sexual encounter, the perpetrator could be separately liable under penal code provisions for sexual offenses. Although these provisions do not punish the recording or dissemination of an image or video itself, they can be used where other penal codes are not applicable.

6. *Witness Tampering and Intimidation - N.Y. Penal Law §§ 215.10–.17*

Witness tampering may be applicable where an abuser is intimidating a victim to not testify against the abuser, or to falsely testify, by threatening to release intimate images of the victim.

7. *Criminal Contempt – N.Y. Penal Law §§ 215.50–.52*

Criminal contempt may be applicable where there are provisions included in Orders of Protection or Orders of Custody that prohibit abusers from posting or disseminating intimate images, and the abuser violates these orders by posting or disseminating these images. In that instance, the abuser could be arrested on the violation of the order.

C. Supporting Victims of Cyber Sexual Abuse Who Report to Law Enforcement

Victims of cyber sexual abuse who turn to law enforcement for help have faced challenges in achieving justice, including having the abuser arrested, prosecuted, and/or found liable, whether criminally or civilly. These challenges should not discourage victims from reporting, but they do indicate the importance of having advocates and attorneys support victims throughout the reporting process. This section explores ways that advocates and attorneys can support victims of cyber sexual abuse who are considering reporting and/or who actually report their abuse to law enforcement.

1. *Weighing the Advantages and Disadvantages of Reporting Cyber Sexual Abuse to Law Enforcement*

It is important to discuss with your client the pros and cons of reporting cyber sexual abuse to law enforcement. Arming the client with an understanding of the reporting process, as well as an understanding of any civil or non-legal avenues of obtaining protection and relief, will help the client determine whether he or she wishes to pursue a criminal case.

(a) Obtaining a Criminal Order of Protection

Obtaining an order of protection is a key benefit to reporting cyber sexual abuse to the police. The reporting victim—usually referred to in New York State as the “complainant,”

“complaining witness,” or “CW”—is typically granted an order of protection after the perpetrator of the abuse is arrested. An order of protection is an order from a court instructing the perpetrator to refrain from engaging in specified behaviors towards the victim. The relief contained in orders of protection vary depending on the circumstances of each case. They can be “limited orders,” in which the perpetrator is instructed to refrain from committing crimes against the reporting victim, or they could be “full stay away orders,” in which the perpetrator is instructed to stay away from the victim, their home, their work, or other locations delineated in the order. An order of protection can also include other protective provisions depending on the facts of the case. One example of such protective provisions is a “no communication” provision. Additionally, although not yet common in criminal orders of protection, it is possible to request a protective provision that specifically orders the perpetrator to refrain from publishing or disseminating intimate images or videos of the complainant.

While a criminal case is pending, the Court will typically issue a temporary order of protection that renews on each calendar date. In domestic violence cases, temporary orders of protection are usually requested as a matter of policy at arraignment (the defendant’s first court appearance). It is important to explain to a victim in a case that although their order of protection has an expiration date (perhaps only 2-3 months from the date it issued) a new order will be extended on the next date the case is on. If the defendant is ultimately found guilty of the crime charged, or if the defendant enters a plea to the crime charged or a related charge, the Court may issue a final order of protection as part of the disposition of the case. The duration of a final order of protection varies and depends on the severity of the crime for which the perpetrator was ultimately convicted or plead guilty to. If the criminal case is dismissed or the defendant is found not guilty on all charges, then the temporary order of protection is vacated immediately and no final order of protection is issued.

In discussing orders of protection with your client, keep in mind that civil orders of protection are available in Family Court in cases where the parties are related by blood or marriage, are currently or formerly married, have a child in common, or are in or were in an intimate relationship.³⁴ Civil orders of protection are explored in much more detail in Section II of Part 2- Civil Legal Remedies for Victims of CSA. If your client is eligible to seek an order of protection in Family Court, you should discuss which type of order of protection your client would like to pursue, keeping in mind that your client can pursue both types of orders of protection concurrently.³⁵

If the cyber sexual abuse did not occur in the context of an intimate partner or family relationship, then pursuing a criminal case will be your client’s only option to secure an order of protection.

³⁴ See N.Y. Family Court Act § 812.

³⁵ Family court and criminal court have concurrent jurisdiction over crimes that are considered family offenses. See Criminal Procedure Law §530.11, Family Court Act §812. Thus, a victim of intimate partner violence or family violence is able to pursue both a civil order of protection in Family Court and a criminal order of protection in criminal court based on the same set of facts.

Control of the Case

Once your client reports the cyber sexual abuse, the police and the District Attorney's office will decide how to move the case forward, if at all. You can, and should, advocate for the police to make an arrest and for the District Attorney's office to prosecute the case to the fullest extent possible, but your client should understand that law enforcement—not the client—really has control over the decisions made in the case. For example, this means that your client cannot decide to not move forward with the case once the abuse is reported. Clients can always change their minds about whether they want to cooperate with the District Attorney's office, including whether to testify as a witness in the case for the government, but they cannot decide to “drop the charges”—only the District Attorney's office has the ability to make that decision. Policies vary between District Attorney's offices regarding whether to pursue prosecution in cases where the victim does not wish to cooperate but sufficient evidence nonetheless exists for prosecuting the perpetrator absent the victim's cooperation. For example, the Brooklyn and Manhattan District Attorney's offices tend to pursue prosecution whenever possible without the victim, at least in order to have a temporary order of protection in place while the case is open and to have time to investigate and further discuss cooperation with the victim.

If a client decides that they do not want to cooperate with an ongoing prosecution and the District Attorney's office determines that it will nonetheless move forward with the prosecution, the Assistant District Attorney (“ADA”) on the case has the ability to subpoena your client, which will compel your client to testify in a grand jury proceeding or at trial. Although rarely compelled in this way, once subpoenaed, your client will be required to appear in court at the appointed date and time and testify truthfully about the events in question under penalty of perjury.

Similarly, if a criminal order of protection has been issued in favor of your client, your client cannot ask the court to vacate the order of protection if the client decides that he or she no longer wishes to pursue prosecution. However, your client can, and should, communicate their wishes regarding the order of protection to the ADA on the case.

Note that all these policies and procedures differ from civil cases in Family Court, where the client is a party in the case—i.e., the Petitioner—and can decide at any time to withdraw his or her petition for an order of protection. In Family Court, as soon as the petition is withdrawn, the civil temporary order of protection is vacated and the case dismissed. This level of control might be more appealing to your client, so be sure to explain how the criminal and civil processes work, including your client's agency in both processes. Additionally, because your client is a party to the civil case (unlike in a criminal case), he or she will have greater involvement in a civil case than in a criminal case. For example, in a criminal case, the reporting victim does not have to come to any court dates until the day they have to testify in court; in a civil case however, the Petitioner must appear at *every* court appearance or their case will be dismissed.

Privacy Concerns

Make sure your client understands that criminal proceedings are public. Documents (such as orders of protection) are publicly available and may contain the victim's name. In felony cases, grand jury proceedings are secret, but trials are public and open to the media, in most cases, with

some potential accommodations to the victim (e.g., no photographs) on a case-by-case basis and at the judge's discretion. Additionally, although grand jury proceedings are secret, the transcript from the Grand Jury will likely be turned over to defense counsel during the pendency of the case. Additionally, ADA's are under obligations under, what is commonly referred to as, their *Brady/Giglio* obligation. This requires ADA's to disclose to the defense counsel any material and/or information that may be favorable to the defendant, which can include information about the victim that is of a sensitive nature. This information can include, but is not limited to, a victim's history of criminal convictions and mental health history (if the victim suffers from an illness or condition that affects their ability to perceive, recollect, or recall). On a case-by-case basis, an ADA may apply for a protective order, which is a court order in which the court determines that certain documents and/or information will not be turned over to the defense counsel (either until a specific point in the case or never at all). In order to obtain a protective order, an ADA must allege specific reasons why the information should not be disclosed.

Reluctance to Work with Law Enforcement

Some clients may be nervous about reporting to law enforcement because of a criminal history, immigration issues, past negative experiences with law enforcement, or concerns about the consequences of facing their abuser.

If your client has any open warrants, he or she will need to clear those prior to reporting or risk being subjected to arrest when reporting. If your client has a criminal history, they should be honest with the ADA prosecuting the case about their history - the ADA will be able to find out this information, and it is better for the client to be up front about their criminal history than risk damaging their credibility with the ADA prosecuting the case. Additionally, your client's background may be subject to cross examination by defense counsel and it will be important for the client to fully disclose their criminal history in order to allow the ADA to adequately prepare. Prosecutors will do their best to protect victims, but are mandated to disclose certain information to the defense, including prior criminal convictions.

If you are working with an undocumented client you should make sure your client understands that law enforcement is *not* required to report him or her to U.S. Immigration and Customs Enforcement ("ICE"). In New York City in particular, neither the NYPD nor the District Attorney's office will report your client to ICE,³⁶ and in fact should not even be asking for your client's immigration status.

Some clients may have had past negative experiences with law enforcement, including instances where they tried to report a crime and were ignored, disbelieved, or made to feel ashamed. You can help these clients overcome their fear of reporting by preparing them to report, acting as an advocate during the reporting process, and accompanying the client to the precinct. The next section provides more information on how to support your client through the reporting process.

³⁶ See *Sanctuary City Policy Wins in New York City*, INSTITUTE FOR POPULAR DEMOCRACY (Dec. 1, 2017), <https://populardemocracy.org/blog/sanctuary-city-policy-wins-new-york-city>.

Finally, some clients may be reluctant to pursue criminal charges against a person they once loved or may still have feelings for, especially if the client and the perpetrator have children in common. As an advocate, it is important for you to make sure that your client understands what will happen after he or she reports the perpetrator's cyber sexual abuse. Clients should understand that reporting the abuse to law enforcement can lead to an arrest of their abuser, which could ultimately lead to a prosecution, and maybe even jail time. If these consequences are not what your client wants, you should discuss whether the civil order of protection option (if applicable) is more desirable under the circumstances.

That being said, it is important for your client to know that an arrest, prosecution, and a criminal order of protection may be the best way for your client to protect him- or herself. These mechanisms can be strong deterrents for abusers who fear jail time and/or a criminal record. At the end of the day, however, it should be and is your client's decision whether to report to law enforcement, so be sure to always present all options and provide advice in a nonjudgmental way, which includes being understanding when clients are hesitant to report and being supportive of their ultimate decisions.

2. Helping Your Client Report Cyber Sexual Abuse

In New York, reports of cyber sexual abuse can be made in the following ways:

a. New York Police Department (“NYPD”)

A crime can be reported by calling 911 in the case of an exigent emergency or by walking into a police precinct. In New York City, a crime may be reported to any NYPD officer or precinct, but will be handled by the local precinct based on where the incident occurred. If there is not an immediate arrest for an ongoing crime (often there is not an immediate arrest in cyber sexual abuse cases), the case will be transferred to the local precinct's designated domestic violence officer (“DVO”) for investigation and possible arrest. If you or your client needs to follow up on a report, call the local precinct handling the case and ask to speak to the DVO.

b. Family Justice Center

Family Justice Centers are located throughout New York City and are staffed with specialized NYPD officers who can take reports of domestic violence and cyber sexual abuse.

c. District Attorney's Office's Special Victims Unit

Some District Attorney's Offices have Special Victims Units that have full-time NYPD officers who investigate complex domestic violence and cyber sexual abuse cases. When a complaint of domestic violence/cyber sexual abuse is made in New York, the law enforcement officer receiving the complaint will have the complainant fill out a Domestic Incident Report (“DIR”) in their own handwriting. The DIR is a sworn statement of fact in the complainant's own words and can be used, in specific ways, in court. For example, should a case go to trial, a complainant could be cross-examined during the trial based on the content of the DIR. You should

prepare your client that they will be asked to fill out a DIR if they self-report the cyber sexual abuse to the NYPD.

Preparing to Report

Unfortunately, crimes of cyber sexual abuse are not always treated as seriously as they should be. In some instances, your client may even face pushback about whether an actual crime was committed. It is helpful to go over the facts of your client's cyber sexual abuse with your client before reporting and determine what provisions of the penal code you think were violated. Doing so helps to build a solid complaint, so that if your client receives resistance from the police, they can point them to specific provisions of the penal code that apply. If the cyber sexual abuse happened in the context of an intimate partner (or former intimate partner) relationship, your client will want to report to the DVO. You should call the precinct in advance to ask when the DVO will be on duty so that your client can make sure to go to the precinct when a DVO is on duty.

Beginning a Criminal Case

Generally, most criminal cases begin with an arrest, such as catching someone at the scene of a crime or in the act of committing a crime. However, due to the nature of cyber sexual abuse, these cases are more likely to begin with pre-arrest investigation after a DIR is made. Given the technological complexities and often ongoing nature of cyber sexual abuse, investigation of phone numbers and IP addresses may be necessary to gather sufficient evidence of abuse to permit an arrest. Depending on how the case is reported and the degree of abuse, an ADA may be assigned to the pre-arrest investigation, or a detective or DVO may be your point person. You and your client can assist in the pre-arrest investigation by providing organized evidence to law enforcement and/or the assigned ADA.

Vertical vs. Horizontal Prosecution

In New York, most District Attorney's Offices prosecute crimes of domestic violence (which include cyber sexual abuse crimes) vertically. This means that the same ADA will handle your client's case from beginning to end (unless there is an interruption in the ADA's employment at that office, such as if the ADA transfers, leaves the office, goes on maternity or paternity leave, etc.). A few District Attorney's Offices may still use horizontal prosecution in domestic violence prosecutions, which means that a different ADA will handle each stage of the case: initial complaint drafting, grand jury, trial, etc. Your client should confirm with the first ADA they speak to whether he or she will be the ADA handling their case going forward.

Misdemeanor vs. Felony Cases

Misdemeanors are crimes that can be punishable by up to one year in jail and are usually charged by a document called a complaint. Felonies can start with a complaint or in the grand jury, but usually require an indictment from a grand jury to move forward. Misdemeanors are handled in Criminal Court, while felonies are handled in Supreme Court and are assigned to a court part based on the trial bureau of the assigned ADA. If there is an open family court case involving the same parties, the case may be handled in the Integrated Domestic Violence ("IDV") court part

of the Supreme Court, which will handle the misdemeanor or felony criminal case and the family court case together.

In New York City, there is a specific law addressing cyber sexual abuse which is described in more detail in Part 1-Criminal Legal Remedies for Victims of CSA, Section I.A., and which makes cyber sexual abuse a Class A misdemeanor. Depending on the facts of the case, it may be possible to charge other crimes that could rise to the level of a felony (e.g., unlawful surveillance in the second degree). See Part -Criminal Legal Remedies for Victims of CSA Section I.B. supra.

Contacting the District Attorney's Office

Once an investigation has begun or an arrest is made, an ADA will be assigned to handle your client's case. If you do not know what ADA is assigned to your client's case, you can contact the main number of your specific District Attorney's Office and provide the docket number of the abuser's case to a switchboard operator who should be able to assist you. You can also find the ADA assigned to your client's case by visiting <https://iapps.courts.state.ny.us/webcivil/ecourtsMain> and clicking on the WebCriminal link. You should also reach out to your client in the event he or she has been contacted by the assigned ADA or received paperwork with the ADA's contact information.

ADAs typically handle multiple cases at a time, are in court daily, and may be difficult to reach. Their voicemails may be full or they may take a long time to return your call. Below are some general tips on best contacting an ADA:

- Call during lunch (1:00 to 2:00 pm) when court is in recess and they are more likely to be at their desks.
- If you are able to leave a message, state who your client is, the abuser's docket number and repeat your phone number multiple times. Try not to leave more than one message in a 48-hour period unless the matter is urgent.
- If you are unable to contact the assigned ADA for more than a week or the matter is urgent, call the District Attorney's Office's main number and ask to speak with the ADA's supervisor.
- Send an e-mail — e-mail addresses for ADAs follow a general format, which you can find online for your specific District Attorney's office.
- Send a written letter — District Attorney's Offices maintain websites with contact information for the ADAs.
- If you are leaving a voicemail and/or writing an e-mail/letter, **do not** include any facts about the case in such communications.

There are two main times that you and your client may interact with the ADA: initial investigation (which may include grand jury testimony if the case is a felony) and trial preparation/trial. Do not be surprised if the case "goes quiet" in between these times as it works through the

stages of a case, including sometimes lengthy motion practice. Your client should receive an update from the ADA before and/or after each court date even if nothing major is happening in the case.

In the initial investigation of the case, your client should expect the ADA to want to spend at least an hour with them to discuss the facts of the case, gather evidence, assess their credibility, and discuss possible outcomes. If the case is a misdemeanor, the ADA may ask your client to sign a Supporting Deposition or Corroborating Affidavit (“corrob”) to complete the first step of converting a misdemeanor complaint into an “information” which can move forward in court. This document simply states that what is alleged in the complaint (which is usually written with a law enforcement officer present) is true. The ADA may also rewrite the complaint with your client to help detail the facts alleged.

If the case is a felony, the ADA will have a similar initial meeting with your client, but will also discuss the possibility of grand jury proceedings. If the case is to move forward as a felony and the defendant is incarcerated, the grand jury must return an indictment within five days of the arrest or the defendant will be released—this stage may therefore move very quickly.

Trial preparation will be similar to the initial meeting, but in much greater detail and may occur over several meetings. The ADA will likely go over the questions they are planning to ask your client, and you should discuss with your client his or her feelings about testifying and answer any questions he or she may have.

You will need to assess your client, the assigned ADA, and your client’s case to determine whether your presence at every meeting will be supportive and productive. ADAs have different preferences and might be more or less tolerant of your active participation in meetings.

II. Federal Criminal Law

On the federal level, there is no single, comprehensive law that addresses cyber sexual abuse. In November 2017, a bipartisan group of lawmakers introduced a bill, the “Ending Nonconsensual Online User Graphic Harassment (ENOUGH) Act of 2017,” in the House and the Senate that would make the nonconsensual circulation of private, graphic imagery a federal criminal offense.³⁷ In order for the dissemination of the image to qualify as a federal crime under the ENOUGH Act, the individual involved in circulating the image would have to be aware of a substantial risk that the victim expected the image would remain private and that the sharing could cause harm to the victim. The Senate and House bills were respectively referred to the Senate Committee on the Judiciary and the House Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, where they remain pending as of January 2019.³⁸

³⁷ S.2162 - ENOUGH Act; H.R.4472- ENOUGH Act

³⁸ See All Actions: S.2162-115th Congress (2017-2018), <https://www.congress.gov/bill/115th-congress/senate-bill/2162/all-actions?overview=closed#tabs>

In an effort to fill the current gap in federal and state law, victims of cyber sexual abuse have availed themselves of an array of existing federal laws, including copyright, civil rights, computer fraud, wire tap, and cyberstalking statutes. Below, we discuss civil and criminal legal laws that could potentially be used to combat cyber sexual abuse at the federal level.

A. Computer Fraud and Abuse Act, 18 U.S.C. § 1030

The Computer Fraud and Abuse Act (CFAA) criminalizes intentionally accessing a protected computer without authorization, or exceeding the scope of the authorized access. Greater punishment applies if the offense was committed in furtherance of any criminal or tortious act.³⁹ While it may seem obvious that computers connected to the Internet are “used in or affecting interstate or foreign commerce or communication,”⁴⁰ this jurisdictional element still needs to be established by the evidence.

In *United States v. Ledgard*, 583 F. App’x 654 (9th Cir. 2014), the defendant and the victim worked together and began dating. During the relationship, the victim allowed the defendant to take nude photos of her, including photos in which she and the defendant were engaged in sexual activity. A few days later, the victim asked the defendant to delete those photographs from his computer hard drive, and he purportedly did so in front of her. The defendant knew that the victim’s family and Armenian culture would make distribution of those photographs to her family and friends particularly upsetting. When the relationship began to deteriorate, the defendant revealed that he had not actually deleted the photos and threatened to distribute them. The victim delayed breaking up with the defendant, in part because of his threats, but eventually took a new job and broke up with him. After the breakup, the defendant hacked into the victim’s bank, e-mail, and Amazon accounts; made purchases and issued checks in her name; and sent e-mails to her family and others attaching the sexually explicit photographs.

After a bench trial, the defendant was convicted of three counts of violating the Computer Fraud and Abuse Act (CFAA) through unauthorized access to the computer of a financial institution, two counts of violating the CFAA through unauthorized access to a protected computer and three counts of aggravated identity theft. All convictions were affirmed on appeal. In its opinion, the Ninth Circuit found that there was sufficient evidence to support the CFAA convictions because the defendant had accessed the victim’s Amazon, Hotmail, and bank accounts via the Internet and without authorization. The Court also noted that the use of the Internet is intimately related to interstate commerce. The Ninth Circuit further held that there was sufficient evidence to find that the defendant’s conduct had been committed “in furtherance of a tortious act,” because the defendant’s actions constituted intentional infliction of emotional distress.

In *United States v. Wadford*, 331 F. App’x 198 (4th Cir. 2009), a defendant gave the victim, his coworker, a date rape drug while they were on an interstate business trip, then took photographs of her naked from the waist down while she was unconscious. Over a year later, the defendant was fired when an anonymous person reported that he had been sexually harassing employees.

³⁹ See 18 U.S.C. § 1030(c)(2)(B)(ii).

⁴⁰ 18 U.S.C. § 1030(e)(2)(B)

After he was fired, the defendant hacked into his former coworkers' work e-mail accounts to send false, fraudulent, and threatening e-mails to other coworkers. Some of the e-mails attached copies of the photographs he had taken of the victim while she was unconscious. The defendant was convicted by a jury of numerous criminal charges including violations of the CFAA and aggravated identity theft.

On appeal, the defendant argued that he did not access a "protected computer" as required by the CFAA. The Fourth Circuit rejected that argument and held that the computers in question were "protected computers" under the CFAA because they were utilized by employees in South Carolina to communicate with employees in Italy, and utilized by employees in Italy to access electronic data stored in South Carolina, and were therefore "used in or affecting interstate or foreign commerce or communication."⁴¹ The defendant's convictions were affirmed on all counts, except one count of sending threatening e-mails based on an e-mail the defendant sent from one coworker's personal account to other coworkers' work accounts because there was no direct evidence or circumstantial evidence to show this e-mail was sent across a state or national border (such as through an out-of-state server).⁴²

In *United States v. Powers*, No. 8:09-cr-361, 2010 WL 1418172 (D. Neb. Mar. 4, 2010), the victim gave the defendant the password to her e-mail account. The defendant used the password to access her e-mail account, looked through her old e-mails, found photos the victim had previously sent to someone else showing her partially nude and/or engaging in provocative poses, and then sent those photos to several people in her e-mail account address book, including a coworker, as well as several e-mail addresses that the victim did not recognize. The government brought criminal charges under the CFAA. The Court held the indictment properly alleged all necessary elements of the CFAA and that "protected" computers were not limited to computers used by financial or government institutions, but included the servers used to host the victim's e-mail account because those servers can be used in interstate communication. The indictment was eventually dismissed without prejudice on motion of the government.

B. Aggravated Identity Theft, 18 U.S.C. § 1028A

The aggravated identity theft statute, 18 U.S.C. § 1028A, imposes criminal penalties for transferring, possessing, or using the means of identification of another person without lawful authority during and in relation to certain enumerated felony violations (generally related to fraud). It may be useful to victims where the perpetrator has assumed the victim's identity, such as instances where the perpetrator creates a fake social media account assuming the victim's identity or sends e-mails as the victim. Aggravated identity theft is a crime that also requires conviction on an enumerated predicate offense. Under the statute, a defendant convicted of aggravated

⁴¹ 18 U.S.C. § 1030(e)(2)(B).

⁴² See Part 1- Criminal Legal Remedies for Victims of CSA, Section II. E, *infra*, for a discussion of criminal charges related to interstate threats or extortion under 18 U.S.C. § 875.

identity theft will receive a two-year term of imprisonment to run consecutively with the sentence imposed for other offenses.⁴³

In *Ledgard*, discussed *supra* at Part 1-Criminal Legal Remedies for Victims of CSA Section II A in the context of the CFAA, the defendant was convicted of aggravated identity theft where he hacked into his former coworker's Amazon, Hotmail, and bank accounts and then made purchases and issued checks in the victim's name. The lower court found that the defendant had committed predicate felony violations of the CFAA and those convictions were upheld on appeal. In *Wadford*, also discussed *supra* in the context of the CFAA, the defendant was also convicted of aggravated identity theft where he accessed the victim's e-mail account and impersonated her in e-mails to others. This conviction was affirmed on appeal.

C. Federal Wiretap Act, 18 U.S.C. § 2520

As discussed *infra* at Part 2-Civil Legal Remedies for Victims of CSA Section III.B in the civil context, the federal Wiretap Act protects individual privacy in communications with other people by imposing civil and criminal liability for intentionally intercepting communications using a device, unless that interception falls within one of the exceptions in the statute. Criminally, a person convicted of violating the Federal Wiretap Act faces a term of imprisonment of up to five years.⁴⁴

In *United States v. Ronan*, No. NMCCA 200800154, 2009 WL 1154111 (N.M. Ct. Crim. App. Apr. 30, 2009), the defendant, a physician assigned to the United States Naval Academy, participated in the U.S.N.A.'s "sponsor program" whereby midshipmen were invited into sponsors' homes during liberty periods. The defendant granted up to 13 midshipmen access to his home. These midshipmen stayed in bedrooms where, unbeknownst to them, the defendant had hidden "nanny cam" surveillance cameras that recorded midshipmen masturbating and having sex. The defendant used sophisticated audiovisual technology to capture this footage and download it onto DVDs, which he then labeled with the initials of the midshipmen who had been recorded. The DVDs were eventually discovered in his home. At trial, the defendant was convicted of illegal interception of oral communications under the Federal Wiretap Act by a general court-martial. The defendant petitioned for a new trial and was denied.

D. Interstate Stalking or Harassment, 18 U.S.C. § 2261A

Under 18 U.S.C. § 2261A, a person who publishes private, intimate images of another as a means of harassment and uses an interactive computer service to do so may be charged in federal court for interstate stalking or harassment. A person convicted under this statute faces: (1) up to life in prison (if the victim dies), (2) a maximum of 20 years in prison (if the victim suffers permanent disfigurement or life threatening bodily injury), (3) a maximum of 10 years in prison (if the victim suffers serious bodily injury or the offender uses a dangerous weapon during the offense), (4) as provided for applicable conduct under the sexual abuse chapter of the criminal code, or (5) a maximum of five years in prison (under any other circumstances). If the offense

⁴³ 18 U.S.C. § 1030.

⁴⁴ See 18 U.S.C. § 2511(4)(a).

involved a violation of a temporary or permanent civil or criminal injunction, restraining order, no-contact order, or similar court orders, there is a one-year mandatory minimum sentence.⁴⁵

In *United States v. Osinger*, 753 F.3d 939 (9th Cir. 2014), the defendant and the victim were in a romantic relationship for nine months, during which time the victim allowed the defendant to take nude photographs of her. When the victim ended the relationship and moved to a different state, the defendant sent several threatening and sexually explicit text messages, e-mails, and photographs of the victim to the victim, her family, and her friends. He also created a Facebook page with a name similar to the victim's, added her family and friends as Facebook friends, and posted sexually explicit photos and demeaning statements as if they had been posted by the victim. The defendant was convicted under the Interstate Stalking or Harassment statute.

On appeal, the defendant argued that the conviction violated his First Amendment rights. The Court rejected the defendant's facial and as-applied First Amendment challenges, holding that the proscribed acts were tethered to the underlying criminal conduct, not to speech. The Court also found that the defendant's speech was not protected because it was integral to criminal conduct and because it involved sexually explicit publications about a private individual. The Court was also not convinced by the defendant's vagueness challenge because it determined that "harass" and "emotional distress" are not esoteric or complicated terms devoid of common understanding and that the statute's "intent" requirement undermined any argument that the defendant could not know his actions were prohibited by the statute.

In *United States v. Sayer*, 748 F.3d 425 (1st Cir. 2014), the defendant and the victim dated for two years, during which time the defendant took sexually explicit photos of the victim and videos of their consensual sexual acts. When the victim ended the relationship, the defendant stalked her in person, then posted videos of their sexual activity on pornography sites, posted ads on Craigslist, and created several fake social media profiles. Through all of these Internet channels, the defendant used sexually explicit pictures of the victim to direct viewers to the videos on adult pornography sites, and posed as the victim to encourage men online to visit her at her home. Even after the victim moved from Maine to Louisiana and changed her name, men who saw the ads online were able to find her and attempt to visit her in person.

The defendant pled guilty to one count of cyberstalking and was sentenced to the statutory maximum of 60 months in prison. He appealed the district court's denial of his motion to dismiss on constitutional grounds and further contended that his above-Sentencing Guidelines sentence was unreasonable. On appeal, the First Circuit court found "meritless" the defendant's argument that the First Amendment prohibited his conviction because his course of conduct involved speech or online communications, noting that any speech involved in his conduct was not protected by the First Amendment because it was integral to criminal conduct.⁴⁶

In *United States v. Petrovic*, 701 F.3d 849 (8th Cir. 2012), after the victim ended her relationship with the defendant, the defendant threatened to publicize pictures of her in the nude

⁴⁵ See 18 U.S.C. § 2261(b).

⁴⁶ See *id.* at 433–34 ("Speech integral to criminal conduct is now recognized as a long-established category of unprotected speech.").

or engaging in sexual activity, including videos that he had secretly captured during their sexual encounters. When the victim ended the relationship, the defendant sent physical copies of the pictures with derogatory language to her friends, family, and coworkers, and launched a website posting sexually explicit photos and videos, as well as the text messages that she had sent him about her private and intimate thoughts, including her suicidal thoughts and history. The website also included her contact information and the social security numbers of her children. When the victim found the website, she “had a breakdown” and “wanted to die.” The victim’s sister eventually managed to have the website taken down for a few days, but the defendant relaunched with a message offering to take down the site only if the victim provided him with \$100,000 and several items of property.

The defendant was convicted of four counts of interstate stalking and two counts of interstate extortionate threats. He received a 96-month sentence. On appeal, the defendant’s First Amendment challenges were rejected by the appellate court.

E. Interstate Threats or Extortion, 18 U.S.C. § 875

18 U.S.C. § 875 criminalizes communicating threats or extorting value from another person across state lines. A person who publishes or threatens to publish private, intimate photos or videos of another with the intention of extracting money or otherwise forcing the victim into prescribed conduct the victim would not have otherwise engaged in, may be charged with extortion if the perpetrator transmitted the communication to the victim via interstate commerce channels.

For example, in *United States v. Howard*, 759 F.3d 886 (8th Cir. 2014), the defendant met the victim through a gay social networking website. The victim was not open about his sexual orientation in part because the nature of his occupation meant revealing his sexual orientation would likely cause him to lose his job. A couple of months later, the defendant began repeatedly asking for money and referencing the victim’s occupation, which the victim interpreted as being a threat to disclose his sexual orientation. When the victim ran out of money, the defendant mentioned he had nude photographs of the victim and provided proof by sending them via text message. By the time the victim contacted law enforcement, he had sent the defendant a total of \$53,625.25. After the victim contacted law enforcement, he paid the defendant an additional \$100 provided by law enforcement. The defendant then asked the victim to take out a second vehicle title loan in order to send the defendant more money, and threatened to contact the victim’s family, employer, and coworkers directly when the victim refused. To prove he could make good on his threats, the defendant sent a picture of the victim to the victim’s secretary, sent faxes to the victim while the victim was at a work retreat, contacted several people the victim knew, and texted the victim a photo of one of his colleagues. Ultimately, the defendant pleaded guilty to one count of extortion and was sentenced to 21 months in prison.

In *United States v. Kurtz*, No. 08 Cr. 402-01 (RWS), 2009 U.S. Dist. LEXIS 61126 (S.D.N.Y. Apr. 3, 2009), the defendant visited the victim, a 62-year-old woman, after contacting her on a Jewish dating website. While visiting the victim, the defendant photographed her in the shower and in bed without her consent. The victim asked the defendant to give her the camera and film, but the defendant refused. The victim then sent the defendant an e-mail asking for the photos and requesting he destroy all copies. The defendant replied that she owed him money and threatened to send the pictures to her friends, business associates and Rabbi. After criminal

charges were brought, the defendant pleaded guilty to extortion and was sentenced to two years in prison.

Likewise, in *United States v. Petrovic*, 701 F.3d 849 (8th Cir. 2012), discussed *supra* at Criminal Legal Remedies for Victims of CSA Section II E in connection with interstate stalking, the defendant was convicted of interstate extortion given his demand for \$100,000 in exchange for taking down a website with sexually explicit photos of the victim.

F. Obscene or Harassing Telephone Calls in Interstate or Foreign Communications, 47 U.S.C. § 223

A person who publishes intimate photographs or videos of another without his or her consent and who uses a telecommunication device to harass the victim (perhaps by threatening that the intimate material will be published) may be charged under 47 U.S.C. § 223(a)(1)(C).

For example, in *United States v. Cope*, 24 F. App'x 414 (6th Cir. 2001), the defendant harassed his ex-girlfriend, a nationally recognized high school teacher, by sending incriminating e-mails in her name to various people, including the victim's church minister and employer. The e-mails indicated that the victim had been having sexual relationships with her students. Ultimately, the defendant pleaded guilty and nolo contendere on 13 counts of violating 47 U.S.C. § 223(a)(1)(C) and was sentenced to prison.

G. Video Voyeurism Prevention Act of 2004, 18 U.S.C. § 1801

18 U.S.C. § 1801 prohibits recording the private areas of individuals without their consent, but only applies in a limited jurisdiction—the “special maritime and territorial jurisdiction of the United States”—which makes it unlikely that the statute will often be of use. The jurisdiction where this statute applies includes: (1) the high seas, waters within the maritime jurisdiction of the U.S., and vessels on the high seas or Great Lakes; (2) land acquired and used by the United States, or land purchased from a State by the United States for a fort, dockyard, or “other needful building;” (3) islands or rocks (at the discretion of the President); (4) aircraft in flight over the high seas or waters within the admiralty jurisdiction of the U.S., or any spacecraft; (5) any jurisdictionless place or vessel scheduled to travel to the U.S. where an offense against a U.S. national takes place; and (6) U.S. military, diplomatic, or consular bases in foreign nations, or residences in foreign nations used by U.S. personnel on U.S. missions.

Federal law regarding cyber sexual abuse has developed at a slower pace than the technology enabling such abuse has progressed. Nevertheless, while there are no federal laws that directly address cyber sexual abuse, a variety of existing federal laws can be used on behalf of cyber sexual abuse victims, depending on the facts and circumstances of each matter. You should educate your client on which laws are most applicable to the client's case and work with the client, and/or ADA, to explore these possible criminal legal remedies.

PART 2 - CIVIL LEGAL REMEDIES FOR VICTIMS OF CSA

I. Family Court Orders of Protection

A. Overview of Family Court Civil Orders of Protection

Victims of cyber sexual abuse may be able to obtain relief by seeking a civil order of protection in New York Family Court, which can prohibit the abuser from disclosing intimate images of the victim if certain conditions are satisfied.⁴⁷

1. Jurisdiction: “Family” Relationship Must Be Established

In order to proceed in Family Court, the victim and the perpetrator must meet *one* of the following relationship requirements:

- the victim (called the “petitioner”) and abuser (called the “respondent”) are, or were formally, legally married;
- the victim and abuser have a child in common;
- the victim and abuser are blood relatives or related by marriage; or
- the victim and the abuser are, or were formerly, in an intimate relationship:⁴⁸

2. Family Offenses

In order to obtain an order of protection, the victim will need to file a petition alleging at least one family offense. The Family Court Act defines a family offense as “acts which would constitute disorderly conduct, harassment in the first degree, harassment in the second degree, aggravated harassment in the second degree, sexual misconduct, forcible touching, sexual abuse in the third degree, sexual abuse in the second degree . . . , stalking in the first degree, stalking in the second degree, stalking in the third degree, stalking in the fourth degree, criminal mischief, menacing in the second degree, menacing in the third degree, reckless endangerment, criminal obstruction of breathing or blood circulation, strangulation in the second degree, strangulation in the first degree, assault in the second degree, assault in the third degree, an attempted assault, identity theft in the first degree, identity theft in the second degree, identity theft in the third degree, grand larceny in the fourth degree, grand larceny in the third degree or coercion in the second

⁴⁷ A civil protective order may also be obtained in New York Supreme Court as part of a divorce already pending there.

⁴⁸ In determining whether a relationship is an “intimate relationship,” courts consider factors such as the following: the nature or type of relationship, regardless of whether the relationship is sexual in nature; the frequency of interaction between the persons; and the duration of the relationship. Note: Neither a casual acquaintance nor ordinary fraternization between two individuals in business or social contexts shall be deemed to constitute an “intimate relationship.” *See* Family Court Act § 812.

degree”⁴⁹ In other words, the Family Court Act designates certain crimes from the penal code as family offenses, providing a basis for seeking a Family Court Order of Protection.

New York State’s cyber sexual abuse law (awaiting signature by the Governor) establishes “unlawful dissemination or publication of an intimate image” as a family offense. *See infra Part 1, Criminal Legal Remedies for Victims of CSA, Section I.A.* Additionally, depending on the particular facts of the case, cyber sexual abuse may qualify as one or more of other family offenses, such as harassment, coercion, stalking, or a sexual offense. For example, if an abuser repeatedly threatens the victim to disclose intimate images, or actually does post images repeatedly, his or her conduct may constitute harassment. The offense of coercion may be found if the abuser has threatened to disclose the images unless the victim does (or does not) do something, such as get back together with the abuser or seek custody of their children. If the underlying depicted acts were non-consensual, the abuser’s conduct may be found to constitute one or more sexual offenses as well. Additionally, a victim may be able to show the offense of identity theft if the abuser has been impersonating the victim online.

B. Procedure for Obtaining a Civil Order of Protection

1. *Venue*

A victim seeking a Family Court Order of Protection may go to the Family Court in the borough: 1) where the victim lives, 2) where the abuser lives, or 3) where the abuse took place.⁵⁰

2. *First Day in Court: Filing the Petition and Seeking a Temporary Order of Protection*

The victim will go to the petition room of the Family Court and file a Family Offense Petition that alleges at least one family offense.⁵¹ The victim must include as much detail as possible in the petition about the incidents of abuse, including details about the cyber sexual abuse. Upon completing the petition, petitioners will make an *ex parte* appearance before a judge in intake where they will apply for Temporary Orders of Protection, which the judge will grant directly from the bench on the same day if good cause is shown.

3. *Available Relief*

a. Standard Provisions

The relief available on a Temporary Order of Protection is similar to the relief available on a Final Order of Protection. The relief under a Temporary Order of Protection may include standard provisions such as that the abuser:

⁴⁹ N.Y. Fam. Ct. §812(1).

⁵⁰ *See Information by County*, New York City Family Courts, <https://www.nycourts.gov/courts/nyc/family/infobycounty.shtml> (last accessed March 19, 2019).

⁵¹ Victims should try to get to court as early as possible to ensure they will be able to have the case heard before the judge that day.

- stay away from the petitioner, and/or the petitioner’s children;
- stay away from specific locations, such as the petitioner’s place of employment or the children’s day care or schools;
- vacate or be excluded from the home;
- not communicate with the victim by any means;
- refrain from committing any family offenses against the victim.

b. Provisions Prohibiting Cyber Sexual Abuse

In cases where the petition contains allegations of cyber sexual abuse, family court adjudicators are increasingly willing to include provisions in the Order of Protection specifically prohibiting this conduct. Such provisions are often needed, as victims have found that when reporting instances of nonconsensual disclosure of intimate images following the issuance of an Order of Protection with only standard terms, law enforcement officials often do not consider such conduct to be a violation of the Order of Protection, based on the logic that a disclosure made by the abuser to third parties does not equate to the abuser directly contacting the victim.

Therefore, if appropriate, Petitioners and advocates should specifically ask that one or both of the provisions below be included in the terms of the Order of Protection. The request should be made both in writing in the petition and orally at the appearance before the judge.

- **The Respondent is not to post, transmit, or maintain, or cause a third party to post, transmit, or maintain, any images, pictures, or other media, depicting the Petitioner in a naked state or participating in any sexual act OR threaten to do the same.**
- **The Respondent is to refrain from using Petitioner’s likeness or impersonating Petitioner on any social media.**

Sample Orders of Protection including this language are included in this Manual as Appendix E.

To the extent a judge is unfamiliar with this language or resistant to including it, the advocate or victim should be prepared to argue why its inclusion is appropriate under the Family Court Act. Section 842(c) of the Family Court Act allows the Court to enter an Order of Protection ordering a respondent to “refrain from harassing, intimidating or threatening” conduct, which includes behavior beyond the delineated family offenses listed in the Family Court Act. Furthermore, Section 842(k) of the Family Court Act states that the Court may require a respondent “to observe such other conditions as are necessary to further the purposes of protection.”⁵² Based

⁵² N.Y. Family Ct. Act 842(k). See also N.Y. Comp. Codes R. & Regs. tit. 22, § 205.74(c)(6) (“An order of protection entered in accordance with section 841(d) of the Family Court Act may, in addition to the terms and conditions enumerated in sections 842 and 842-a of the Family Court Act, require the petitioner, respondent or both . . . to: . . . comply with such other reasonable terms and conditions as the court may deem necessary and appropriate

on this authority, numerous family court judges have been willing to include the above CSA-specific provisions in both temporary and final orders of protection.

If the adjudicator nevertheless refuses to include these provisions, the advocate or victim can offer to provide additional briefing on this issue. (See Appendix C for Legal Memo on this subject).

4. Continuing the Case

Following the initial *ex parte* appearance, the Judge will generally issue a summons for the abuser to appear in court on a specific date. The abuser must be served with the summons, petition, and Temporary Order of Protection at least 24 hours before the set court date.⁵³

On the set court date—called the adjourn date or return of process—various scenarios may arise depending on whether the abuser has been served and appears in court. If the abuser comes to court and does not consent to a final Order of Protection, both parties will have the opportunity to obtain a lawyer or be appointed a free one by the court if they cannot afford one. Additional court dates will be set, and ultimately the case will either settle (for example, if the abuser consents to a final Order of Protection without admission of wrongdoing), or proceed to trial, where the victim will need to prove that the family law offense occurred by a preponderance of the evidence. If the court finds in favor of the victim, the court will issue a final Order of Protection, which typically has a duration of two years, or up to five years if certain aggravating circumstances are shown.⁵⁴

Due to the delays that routinely occur in family court, you should advise your client that the trial may not take place for as long as six months or more after the petition is filed. Therefore, collecting and preserving evidence of cyber sexual abuse from the beginning is crucial. (See Part 4- Evidence Collection).

II. New York State and New York City Civil Causes of Action

As discussed *supra* at Criminal Legal Remedies for Victims of CSA Section I A, in 2018, New York City enacted legislation criminalizing the nonconsensual disclosure of intimate images (the “NYC Unlawful Disclosure Law”). At the same time, New York City also created a civil cause of action allowing victims to sue perpetrators of cyber sexual abuse for damages and other

to ameliorate the acts or omissions which gave rise to the filing of the petition.”); *see also Miriam M. v. Warren M.*, 859 N.Y.S.2d 66, 67-68 (1st Dep’t 2008) (“The Family Court has the authority to impose reasonable conditions when they are likely to be helpful in eradicating the root of family disturbance.”)

⁵³ When the respondent’s address is known, usually the court will send these papers directly to the Sherriff, who will serve the Respondent without a fee.

⁵⁴ Under Family Court Act §827, aggravating circumstances include: 1) physical injury or serious physical injury to the petitioner caused by the respondent; 2) the use of a dangerous instrument against the petitioner; 3) a violation of prior order(s) of protection; 4) prior convictions for crimes against the petitioner; 5) exposure of any family or household member to physical injury by respondent; or 6) other “like incidents,” behaviors, and occurrences which, in the court’s opinion, constitute an immediate and ongoing danger to the petitioner or any member of the petitioner’s household. Family Court Act §827.

relief, including compensatory and punitive damages, injunctive and declaratory relief, attorney’s fees and costs, and “such other relief as a court may deem appropriate.”⁵⁵ A civil suit under this section does not preclude the victim from also seeking criminal justice remedies for the same behavior.⁵⁶

The first lawsuit under this new civil claim was filed in April 2018. It remains to be seen how this cause of action will develop in New York City. Remember that if there is no nexus to New York City, then this cause of action is not available to victims, though other local jurisdictions in the State are starting to pass similar laws that create specific causes of action for cyber sexual abuse victims.⁵⁷

Other potential causes of action against a perpetrator who discloses intimate images without consent are the torts of intentional infliction of emotional distress (“IIED”) and negligent infliction of emotional distress (“NIED”). An overview of each claim is laid out below.

1. Intentional Infliction of Emotional Distress (“IIED”)

To successfully bring an IIED as a cause of action, each of the following elements must be established:

- a. extreme and outrageous conduct;
- b. intent to cause, or disregard of a substantial probability of causing, severe emotional distress;
- c. a causal connection between the conduct and injury; and
- d. severe emotional distress.

The Second Department has recognized that a cause of action for the intentional infliction of emotional distress may exist where an “intimate photograph depicting an unclothed portion” of a petitioner’s body is “widely disseminated” with no legitimate purpose, and the petitioner “did, in fact, suffer severe emotional distress as a result of the dissemination”.⁵⁸ Note, however, that it

⁵⁵ NYC Administrative Code 10-180 §d.

⁵⁶ *See id.*

⁵⁷ *See* Lisa Finn, *Crackdown on Revenge Porn: New Suffolk County Legislation Signed*, PATCH (Dec. 17, 2018, 8:31 PM), <https://patch.com/new-york/easthampton/crackdown-revenge-porn-new-suffolk-county-legislation-signed>.

⁵⁸ *Leff v. Our Lady of Mercy Acad.*, 55 N.Y.S.3d 392, 395 (App. Div. 2d Dep’t 2017) (rejecting argument that disseminating unclothed photo of high school student, when the student was an infant, failed to meet “extreme and outrageous” element needed to state a cause of action).

can be challenging to ultimately succeed on an IIED claim, as liability is generally only found “where the conduct has been so outrageous in character, and so extreme in degree, as to go beyond all possible bounds of decency, and to be regarded as atrocious, and utterly intolerable in a civilized community.”⁵⁹ Moreover, IIED is unavailable where damages resulting from the conduct at issue are available via another recognized tort.⁶⁰

2. Negligent Infliction of Emotional Distress (“NIED”)

The New York Court of Appeals has recognized the right to recover for negligently caused emotional distress. To successfully bring negligent infliction of emotional distress as a cause of action, the following elements must be established:

- a. breach of the duty of care; and
- b. breach of the duty of care results directly in the emotional harm.

Unlike IIED, NIED does not require “extreme and outrageous” conduct.⁶¹ However, like IIED, a claim of NIED can be difficult to win. A claim of NIED “must generally be premised upon a breach of a duty owed directly to the plaintiff which either endangered the plaintiff’s physical safety or caused the plaintiff fear for his or her own physical safety.”⁶² Identifying a duty that was breached appears to be the biggest hurdle in bringing an NIED claim in cyber sexual abuse cases, as there is no common-law right to privacy in New York.⁶³ However, an NIED claim may be premised on a statutory duty.⁶⁴ In *Dana v. Oak Park Marina, Inc.*, for example, the Fourth Department found that a claim for NIED could proceed against the owner of a boat marina who secretly videotaped women changing in the marina restrooms.⁶⁵ The court found that the owner

⁵⁹ *Id.* (quoting *Murphy v. Am. Home Prods. Corp.*, 58 N.Y.2d 293, 303, 461 N.Y.S.2d 232, 448 N.E.2d 86 (1983)), quoting RESTATEMENT (SECOND) OF TORTS § 46 cmt. d).

⁶⁰ See *Xiaokang Xu v. Xiaoling Shirley He*, 147 A.D.3d 1223, 48 N.Y.S.3d 530 (3d Dep’t 2017); accord *Fischer v. Maloney*, 43 N.Y.2d 553, 558, 402 N.Y.S.2d 991, 373 N.E.2d 1215 (1978) (IIED should not be entertained “where the conduct complained of falls well within the ambit of other traditional tort liability”).

⁶¹ *Taggart v. Costabile*, 14 N.Y.S.3d 388, 398 (App. Div. 2d Dep’t 2015) (clarifying that, “notwithstanding case law to the contrary, extreme and outrageous conduct is not an essential element of a cause of action to recover damages for negligent infliction of emotional distress”).

⁶² *Id.*

⁶³ See *Dana v. Oak Park Marina, Inc.*, 660 N.Y.S.2d 906, 909 (App. Div. 4th Dep’t 1997) (holding corporation owed no common-law duty to protect plaintiff’s privacy in New York, “the right to privacy is governed exclusively by sections 50 and 51 of the Civil Rights Law”).

⁶⁴ See *id.*

⁶⁵ See *id.*

had a statutory duty under New York’s General Business Law, which prohibits certain businesses from installing video cameras in private areas such as restrooms.⁶⁶

New York courts have carved out a few exceptions where recovery under NIED was permitted without proof that defendant owed a general duty to plaintiff. Exceptions include situations involving mishandling a relative’s corpse, a hospital falsely advising a daughter her mother died, and a medical examiner concealing that a child died of natural causes, resulting in an improper homicide investigation. It is unclear how likely courts would be to carve out an exception for instances of cyber sexual abuse.

III. Federal Civil Causes of Actions

A. Cases Against Governmental Entities

1. Federal Civil Rights Statutes: Title VII and Title IX

The federal Civil Rights Act of 1964 outlaws discrimination based on race, color, religion, sex, or national origin.⁶⁷ Sexual harassment is encompassed within its prohibition of discrimination on the basis of sex.⁶⁸ Because Congress wished to encourage enforcement of these statutes by “private attorneys general,” federal courts may award attorney’s fees to a plaintiff who prevails on claims brought under the Civil Rights Act.⁶⁹ Title VII of the Act prohibits sexual harassment or other forms of discrimination at work.⁷⁰ Title IX of the Education Amendments Act of 1972 prohibits discrimination in an education program that receives funding from the federal government.⁷¹ Title VII and Title IX do not provide plaintiffs with a cause of action against individuals, only against employers and educational institutions.

Title VII (Employment Setting)

Under Title VII, it is an unlawful employment practice for an employer to “(1) fail or refuse to hire or to discharge any individual, or otherwise to discriminate against any individual with respect to his compensation, terms, conditions, or privileges of employment because of such individual’s race, color, religion, sex, or national origin; or (2) to limit, segregate, or classify his employees or applicants for employment in any way which would deprive or tend to deprive any

⁶⁶ *See id.*

⁶⁷ Pub. L. No. 88-352, 78 Stat. 241 (1964); 42 U.S.C. § 2000e-2 (Title VII).

⁶⁸ 29 C.F.R. pt. 1604.11.

⁶⁹ *See* Civil Rights Attorney’s Fees Award act, codified at 42 U.S.C. § 1988.

⁷⁰ 42 U.S.C. § 2000e-2 (Title VII).

⁷¹ 20 U.S.C. § 1681 (Title IX).

individual of employment opportunities or otherwise adversely affect his status as an employee because of such individual's race, color, religion, sex, or national origin."⁷²

Title VII imposes an exhaustion requirement, meaning that an employee alleging unlawful discrimination or retaliation must file an administrative charge with the EEOC (or a similar state or local agency) before suing in court.⁷³ Title VII claims by federal employees must be brought against the head of the relevant department, agency, or unit.⁷⁴

In *Ruiz v. City of New York*, No. 14-cv-5231 (VEC), 2015 WL 5146629 (S.D.N.Y. Sept. 2, 2015), a Title VII case, two plaintiffs alleged that coworkers at the New York Police Department and the City of the New York had engaged in several official and nonofficial discriminatory and retaliatory actions. In particular, the plaintiffs alleged that a coworker had circulated an image of the female plaintiff's face superimposed onto a naked woman's body. The court dismissed several of the plaintiffs' claims, but held that the plaintiffs had adequately alleged sexual harassment through a hostile work environment. The court highlighted the photo shopped image circulated by a coworker, several instances of sexually explicit graffiti using the plaintiffs' names, and a lewd text a coworker sent both plaintiffs.

In *Phillips v. Donahoe*, No. 12-410, 2013 WL 5963121 (W.D. Pa. Nov. 7, 2013), the plaintiff, a postal employee, brought claims against the Postmaster General after a coworker's cousin threatened the plaintiff, kept nude photographs of the plaintiff in sexually suggestive poses on his cell phone, and then showed the photographs to several coworkers. The plaintiff was ultimately terminated. On summary judgment, the court held that a reasonable jury could conclude that the plaintiff had experienced a hostile work environment because of her sex. Specifically, the court held that although the harassing conduct spanned a brief period of time, it was nonetheless sufficient for a trier of fact to find that the work environment was both objectively and subjectively abusive. In particular, the court highlighted the fact that the plaintiff had almost quit her job after she learned that pictures of her naked body had been shown to her coworkers, and that Pennsylvania law, as a general matter, reflects a societal interest in preventing the unauthorized exposure of an individual's intimate body parts. The court concluded, however, that the Postal Service could not be held vicariously liable for her coworker's harassing conduct because the plaintiff's supervisors took actions that were reasonably calculated to prevent further harassment. The court also denied the defendant's motion for summary judgment as to the plaintiff's retaliation claims.

Title IX (Educational Setting)

Under Title IX, "No person in the United States shall, on the basis of sex, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any education

⁷² 42 U.S.C. § 2000e-2(a) (Title VII).

⁷³ 42 U.S.C. § 2000e-5(e)(1).

⁷⁴ 42 U.S.C. § 2000e-16(c).

program or activity receiving Federal financial assistance”⁷⁵ To establish a Title IX claim against a school district based on student-on-student harassment, a plaintiff must be able to show (1) the harassment is so severe, pervasive, and objectively offensive that it effectively bars the victim’s access to an educational opportunity or benefit; (2) the defendant had actual knowledge of the harassment; and (3) the district acted with deliberate indifference to the harassment.⁷⁶

In *Doe v. Town of Stoughton*, No. 12-10467-PBS, 2013 WL 6195794 (D. Mass. Nov. 25, 2013), a Title IX case, the plaintiff was a 14-year old freshman attending public high school. A 17-year old junior solicited nude photographs from the plaintiff and, when she sent them to him, he distributed those photographs to friends and classmates through his cell phone and the Internet. Other classmates subsequently subjected the plaintiff to sexual harassment. For example, additional male students requested more nude photographs of her, students called her gender-charged derogatory names, and students threatened to widen the distribution of the photographs if she transferred to another school. The plaintiff and her mother reported the incidents to school employees in the guidance department, who promised to take action to prevent further harassment. No formal disciplinary measures were ever imposed, however, and no parents were notified, even after the junior who solicited the nude photographs was charged with statutory rape and pled guilty to assault and battery. The plaintiff brought various claims, including a Title IX claim, against the town of Stoughton, her school principal, and the town Superintendent of Schools.

The court held that the plaintiff’s Title IX and negligence claims survived summary judgment, but entered summary judgment in favor of the defendants on the other claims. With respect to the Title IX claims, the court found that a reasonable jury could find that the actions in question were because of the plaintiff’s sex, in that (1) students circulated nude photographs of the plaintiff, (2) the name-calling experienced by the plaintiff included several gender-charged words, (3) classmates spoke to the plaintiff about the photographs in a sexually demeaning manner, and (4) in this context, pointing, whispering, and staring by fellow students can be considered sexual harassment. The court further held that the harassment met the “severe, persistent, and objectively offensive” bar due to the high number of students who were engaging in the harassing behavior (estimated to be between 25 and 30), and the frequency of harassment (as often as every day for a number of months). Additionally, the court concluded a jury could reasonably find that the harassment deprived the plaintiff of a public school education based on the plaintiff’s testimony that the harassment caused her to develop an eating disorder that required extensive treatment, a weeklong hospitalization, and eventual withdrawal from school.

2. *Federal Statutory Civil Law for Enforcing Constitutional Claims, 42 U.S.C. § 1983*

If the culpable actors are government officials, victims can also consider suing for damages under 42 U.S.C. § 1983 if they believe their constitutional rights were violated. Potential legal theories include violations of the plaintiff’s rights under the Equal Protection Clause or the Fourth Amendment. For example, in *Doe v. Old Forge Borough*, No. 3:12-cv-2236, 2015 WL 4041435 (M.D. Pa. July 1, 2015), a volunteer junior firefighter was sexually assaulted by police officers

⁷⁵ 20 U.S.C. § 1681 (Title IX)(a)

⁷⁶ See *Davis v. Monroe County Bd. of Educ.*, 526 U.S. 629, 631-632 (1999).

and firefighters and suspended after one defendant told Old Forge Borough personnel that he had nude pictures of the plaintiff. On a motion to dismiss, the court dismissed most of the plaintiff's claims, but allowed her to pursue her claims against Old Forge Borough that her constitutional right to substantive due process was violated by the municipality's failure to supervise, train, or promulgate policies adequate to protect her.

Note, however, that claims under section 1983 against government officials often fail because of those actors' qualified immunity defense. *See Taylor v. Barkes*, 135 S. Ct. 2042, 2044 (2015). Qualified immunity shields government officials from civil damages liability unless the official violated a statutory or constitutional right that was clearly established at the time of the challenged conduct. *Id.*

B. Cases Against Non-Governmental Entities

1. *Federal Statutory Civil Law on Copyright, 17 U.S.C. § 501*

One successful (but unorthodox) tactic used by victims of cyber sexual abuse is to bring a suit alleging copyright violations in instances of nonconsensual online publication of private intimate material if the victim is the copyright owner of that material. Such cases have resulted in several large judgments in favor of plaintiffs. 17 U.S.C. § 501 provides that “the legal or beneficial owner of an exclusive right under a copyright is entitled, subject to the requirements of section 411, to institute an action for any infringement of that particular right committed while he or she is the owner of it.” If a victim wants to bring a federal copyright lawsuit, however, in many cases, they would first need to register any videos or photos to be protected with the United States Copyright Office. In other words, to use copyright law as a means of redress, a victim must publicly register a photo or video that they would rather no one ever see. A number of legal scholars have advocated using copyright law as an innovative way of combating cyber sexual abuse.⁷⁷ We note, however, that if the abuser actually took the images rather than the victim, then the abuser may be able to challenge any potential copyright claim by the victim, as copyrights are generally owned by the people who create the works of expression rather than the subjects of the photograph.⁷⁸

Additionally, if there was a copyrighted song accompanying the online post containing the intimate video, the cyber sexual abuse victim could consider contacting the copyright holder of the song and obtaining the rights to the song for the purposes of bringing a copyright action, and then sending a takedown notice under the Digital Millennium Copyright Act, 17 U.S.C. § 512, or pursuing a copyright action for statutory damages.⁷⁹

In *Jane Doe v. David K. Elam II*, case no. 2:14-cv-09788 (C.D. Cal. Apr. 4, 2018), a California woman and her boyfriend, David Elam, ended their relationship in 2013. Elam then

⁷⁷ Christine Hauser, *\$6.4 Million Judgment in Revenge Porn Case Is Among Largest Ever*, N.Y. TIMES (Apr. 11, 2018), <https://www.nytimes.com/2018/04/11/us/revenge-porn-california.html>.

⁷⁸ See 17 U.S.C.A. § 201(a).

⁷⁹ 17 U.S.C. § 501.

began to post sexual photographs and videos of her on pornography websites and impersonate her in online dating forums. He threatened to make her life “so miserable she would want to kill herself.” Strangers sent her explicit texts and e-mails, and some said they were on their way to her home. Doe began to fear for her life. Doe sued Elam in the Central District of California to get him to stop. Doe alleged copyright infringement, online impersonation with intent to harm, stalking, and the intentional infliction of emotional distress. Ultimately, in April 2018, the court awarded her \$6.4 million in one of the biggest judgments ever in a non-celebrity revenge porn case.⁸⁰ Doe was awarded \$450,000 in damages because of copyright infringement. She also received \$3 million in compensatory damages for emotional distress, and \$3 million in punitive damages.

As part of the process in having these photos taken down, Jane Doe also had to copyright photos of her breasts to get her intimate pictures off the Internet. Doe chose that route in part because Elam obtained the photos from Doe consensually when the two were in a relationship. Some websites refuse to remove images that were taken with consent if the person does not register a copyright. Doe’s copyright registrations therefore enabled her to get her images removed from such websites.⁸¹

In *Doe v. Fortuny*, case no. 08 C 1050 (N.D. Ill. Apr. 9, 2009), the defendant allegedly posted the plaintiff’s photograph on the Internet after obtaining it through a “Craigslis Experiment” in which he pretended to be a woman seeking a “str8 brutal dom muscular male” for sex. Over 100 men responded, including the plaintiff, providing photos and contact information. The defendant also allegedly posted this material on his blog, RFJason and Encyclopedia Dramatica. The plaintiff registered the copyright for his photographs within a month of the first posting and then sued the defendant for breach of that copyright and additional tort claims. The court entered a default judgment for the plaintiff because the defendant failed to appear or answer. The judgment consisted of \$35,001.00 in statutory damages for violation of the Copyright Act; \$5,000.00 in compensatory damages for public disclosure of private facts and intrusion upon seclusion; \$32,262.50 in attorney’s fees pursuant to 17 U.S.C. §505; and \$1,989.06 in costs. The defendant was also ordered to immediately remove and/or disable access, content and viewing capabilities of the plaintiff’s response to the defendant’s ad, the copyrighted photograph, and the plaintiff’s personal e-mail address on the defendant’s blog.

2. *Federal Statutory Civil Law Related To Unauthorized Computer Access: Computer Fraud and Abuse Act, 18 U.S.C. § 1030*

The Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030, criminalizes the intentional access of a protected computer without authorization (i.e., “hacking” a protected computer). The CFAA also provides a civil remedy for similar conduct, but in much more limited circumstances.⁸² In particular, damages may be available against a person who obtains information

⁸⁰ See Sara Ashley O’Brien, *Woman awarded \$6.45 million in revenge porn case*, CNN TECH (Apr. 9, 2018), <https://money.cnn.com/2018/04/09/technology/revenge-porn-judgment/index.html>.

⁸¹ *Id.*

⁸² 18 U.S.C. § 1030(g)

through unauthorized access to a computer, or who uses unauthorized access to a protected computer in furtherance of a fraudulent scheme. *Id.* “Protected” computers include those that are used in or affecting interstate or foreign commerce or communication, including a computer outside the United States that is used in a manner that affects interstate or foreign commerce or communications of the United States. As a practical matter, because of the interstate and international nature of the Internet, most ordinary computers, including cell phones, will qualify as “protected” computers under the CFAA.⁸³ The CFAA may be useful to victims where a perpetrator uses the victim’s computer to secretly record him or her, or where the perpetrator has hacked the victim’s computer or otherwise accessed it without authorization to distribute or obtain sexual photos or videos.

In order to bring a civil action under the CFAA, a civil plaintiff must demonstrate that the defendant’s conduct: (1) amounted to a loss of over \$5,000 in the course of one year; (2) modified or impaired the medical treatment of at least one individual; (3) physically injured any person; (4) threatened the public health or safety; or (5) damaged a computer used by the U.S. Government to promote national security.⁸⁴ If the CFAA violation causes only loss of money, then the damages are also only limited to economic damages.⁸⁵ The statute of limitations for the CFAA is two years.⁸⁶

The availability of civil actions and damages has been limited by some courts. For example, the District of Minnesota limits availability of civil actions under the CFAA to situations that involve knowingly or intentionally causing damage to a protected computer. *See Hot Stuff Foods, LLC v. Dornbach*, 726 F. Supp. 2d 1038, 1045 (D. Minn. 2010). In *Nexans Wires S.A., v. Sark-USA, Inc.*, 166 F. App’x 559 (2d Cir. 2006), the Second Circuit likewise affirmed the definition of “loss” to the plaintiff as “any remedial costs of investigating the computer for damage, remedying the damage and any costs incurred because the computer cannot function while or until repairs are being made.” This definition may prevent plaintiffs from bringing a civil action if the monetary loss they suffered is a result of the computer intrusion, but is not damage to the computer itself or to computer service.

In *Sewell v. Bernadin*, 795 F.3d 337 (2d Cir. 2015), the plaintiff and the defendant had a romantic relationship from 2002 until 2011. The plaintiff did not share her electronic passwords with anyone, including the defendant. In August 2011, the plaintiff discovered that someone had changed the password to her private e-mail account, so she could not log into that account. Around the same time, someone used her e-mail account to send malicious statements about her sexual activities to her family and friends through the account contact list. Six months later, in February 2012, the plaintiff discovered she could no longer access her Facebook account, and someone had used her Facebook account to post public, malicious statements about her sex life. Verizon records

⁸³ *See* § 1030(e)(2)(B)

⁸⁴ *See* §§ 1030(g), (c)(4)(A)(i)(I)-(IV).

⁸⁵ *Id.*

⁸⁶ *Id.*

confirmed that the defendant's computer had accessed the e-mail and Facebook servers where plaintiff's accounts were stored. The plaintiff sued under the CFAA in January 2014.

Because more than two years had passed from the time the plaintiff realized she could no longer access her e-mail account before she filed suit, the court held that the plaintiff's claims as to her e-mail account were time-barred. However, because two years had not yet run since the plaintiff discovered her Facebook account had been accessed without her consent, the court concluded her claims based on her Facebook account under the CFAA could proceed. Shortly after the Second Circuit held that the plaintiff's claims could proceed, the parties settled out of court.

3. *Federal Wiretap Act, 18 U.S.C. § 2520*

The federal Wiretap Act, 18 U.S.C. § 2520, protects individual privacy in communications with other people by imposing civil and criminal liability for intentionally intercepting communications using a device, unless that interception falls within one of the exceptions in the statute.⁸⁷ Although the Wiretap Act originally covered only wire and oral conversations (for example, using a device to listen in on telephone conversations), it was amended in 1986 to cover electronic communications as well (for example, e-mails or other messages sent via the Internet).⁸⁸

If a victim's sexual photos or videos are obtained through interception of an electronic communication, the perpetrator may be criminally and civilly liable under this statute. Whether or not communications were "intercepted" is a key issue under the Federal Wiretap Act. Although the statute defines "intercept" broadly as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device," many courts have adopted a more narrow construction requiring that "interception" occur while the communication is being transmitted.⁸⁹

In *Bruce v. McDonald*, No. 3:13-cv-221, 2014 WL 931522 (M.D. Ala. Mar. 10, 2014), husband and wife plaintiffs sued the wife's ex-husband and his attorneys for violations of the federal Wiretap Act. When the female plaintiff and the defendant divorced, they split custody of their only child. The plaintiff eventually married another man, her co-plaintiff in the lawsuit. Without authorization, the defendant gained access to his ex-wife's individual e-mail account, the plaintiffs' joint e-mail account, and their joint AdultFriendFinder account. The defendant printed out hundreds of pages of sexually explicit messages and photos from the accounts relating to plaintiffs' engagement in sexual conduct with other people. The defendant allegedly sent a packet of these documents to the Alabama Board of Pharmacy, which began taking actions to revoke the plaintiff's pharmacist license, and disclosed the documents to his attorneys in the child-custody dispute against the plaintiff. The attorneys used the documents in the custody case, and may have

⁸⁷ Civil claims under the Federal Wiretap Act, 18 U.S.C. § 2511, are sometimes referred to in court documents as being brought under the Electronic Communications Privacy Act. See *Clements-Jeffrey v. City of Springfield, Ohio*, 810 F. Supp. 2d 857 (S.D. Ohio 2011).

⁸⁸ 18 U.S.C. § 2520

⁸⁹ See, e.g., *United States v. Steiger*, 318 F.3d 1039, 1050 (11th Cir. 2003).

used the documents during a mediation. The new child custody agreement granted the defendant increased custody time, put limits on the plaintiff's sexual activities, and included other terms favorable to the defendant.

The plaintiffs argued that the defendant "intercepted" their e-mail messages by logging into their accounts without authorization. The court held that unauthorized access to an e-mail account, standing alone, does not constitute interception because interception does not occur unless the electronic communications were acquired while they were being transmitted. In other words, communications are "intercepted" if they are obtained while they are in motion, but are not "intercepted" if they are obtained while they are at rest.⁹⁰

⁹⁰ See *Bruce v. McDonald*, 2014 WL 931522 at *6 ("The Eleventh Circuit has adopted a construction of "interception" requiring that electronic communications must be acquired contemporaneously with their transmission. Logging into and acquiring messages from another individual's e-mail account does not necessarily happen contemporaneously with their transmission.").

PART 3 - DESCRIPTION OF RELEVANT SOCIAL MEDIA/ APPLICATIONS AND ASSOCIATED ABUSE

I. Overview

Social media and dating websites and applications (or “apps”) provide many opportunities for cyber abuse and cyber sexual abuse. This Section explores some of the more popular social media, messaging, and dating websites and apps, and provides information on their relevant cyber sexual abuse policies and reporting procedures.

II. Phone and Messaging Platforms

A. WhatsApp

WhatsApp is a secure messaging app for smartphones that operates similarly to text messaging. It is used frequently by international users for both messaging and calling, but its main attraction is that it is more secure than text messaging, as each individual message is encrypted, and cannot be read by third parties or even by WhatsApp itself.⁹¹

WhatsApp does not have a specific policy on cyber sexual abuse. The most relevant policy is that WhatsApp “may collect, use, preserve, and share your information if [it has] a good-faith belief that it is reasonably necessary to: (a) respond pursuant to applicable law or regulations, to legal process, or to government requests; (b) enforce our Terms and any other applicable terms and policies, including for investigations of potential violations; (c) detect, investigate, prevent, and address fraud and other illegal activity, security, or technical issues; or (d) protect the rights, property, and safety of our users, WhatsApp, the Facebook family of companies, or others.”⁹²

WhatsApp users may not use the app “in ways that violate, misappropriate, or infringe the rights of WhatsApp, our users, or others, including privacy, publicity, intellectual property, or other proprietary rights,” or in ways that are “illegal, obscene, defamatory, threatening, intimidating, harassing, hateful, racially, or ethnically offensive, or instigate or encourage conduct that would be illegal.”⁹³ If these terms are violated, WhatsApp reserves the right to terminate the user’s account. However, the termination of the violating user’s account will not delete the images from the recipient’s account.

B. Skype

Skype, which is operated and owned by Microsoft, is one of the most popular video-chat services internationally. It is used both for business and personal purposes, and can be used for

⁹¹ *End-to-end encryption*, WHATSAPP, <https://faq.whatsapp.com/en/android/28030015/> (last visited Jan. 8, 2019).

⁹² *WhatsApp Legal Info*, WHATSAPP, <https://www.whatsapp.com/legal/> (last visited Jan. 8, 2019).

⁹³ *See id.*

consensual sexual interaction (colloquially referred to as “Skype sex”). While “Skyping,” it is easy for one user to take a screenshot, depicting a person engaged in sexually explicit conduct, without the surveyed person’s knowledge.

Microsoft has a specific policy addressing nonconsensual porn. Microsoft will remove the shared content from its services (Skype and also Bing, OneDrive, Outlook, Xbox, Universal Store, etc.) if you fill out an online form at this webpage: <https://www.microsoft.com/en-us/concern/revengeporn>. The form asks where the information appeared, if the images were linked to the person’s name or social media identity, if there are accompanying documents such as a police report or restraining order, and the URLs that the victim requests to be removed. Microsoft can only remove the images and information from its own sites and search engines; it has no control over the information or images hosted on external websites. For this reason, it is important to fill out this request form as quickly as possible to lessen the likelihood of images spreading or going viral.

C. WeChat

WeChat is a Chinese messaging, social media and mobile payment app. Developed by Tencent and first released in 2011, WeChat is now one of the world’s largest mobile apps, with over 1 billion monthly active users.⁹⁴ WeChat is known as a “super app” because of its wide range of functions.⁹⁵ It provides messaging (text, voice, broadcast), video calls and conferencing, video games, location sharing, options to engage in city services (booking doctor’s appointment, paying traffic fines), and much more. Users can send saved or live photos and videos. The app can exchange location information with people nearby and enables the contacting of random users. There is a news feed and search functionality. WeChat also has a social feed of friend updates known as “Moments.” This allows users to post images, text, comments, and share music, articles and post “likes.” When a user posts Moments, they can set privacy by separating their friends into separate groups (e.g., a college friends group) and can select which groups can view the Moment. Only a user’s friends are able to view their Moments’ content; a friend can view other users’ likes and comments in Moments only if they are in a mutual friends group. A Moment can also be set to “Private,” viewable only by the user. Finally, WeChat Pay is a digital wallet service that enables users to pay bills, order goods and services, transfer money to other users, and pay in stores.

WeChat has different Terms of Service for users in China or Chinese citizens, and for users outside China. WeChat does not have a specific policy on nonconsensual pornography or image sharing.

⁹⁴ Lim Yung-Hui, *WeChat by Tencent: From Chat App to Social Media Platform*, FORBES (Feb. 4, 2013, 6:17 AM), <https://www.forbes.com/sites/limyunghui/2013/02/04/wechat-by-tencent-from-chat-app-to-social-mobile-platform/#29ccf43a7ad3>; Matthew Brennan, *One Billion Users and Counting: What’s Behind WeChat’s Success?*, FORBES (Mar. 8, 2018, 1:29 AM), <https://www.forbes.com/sites/outofasia/2018/03/08/one-billion-users-and-counting-whats-behind-wechats-success/#46908be0771f>.

⁹⁵ Miaozhen Zhang, *China’s WeChat: The Power of the Super App*, MEDIUM (Mar. 26, 2018), <https://medium.com/@miaozhen.zhang/chinas-wechat-the-power-of-the-super-app-dc144657625e>.

For users in China or citizens of China anywhere in the world, WeChat’s Terms of Service, published by Tencent, prohibits content that violates national laws and regulations and which disseminates “obscenity” or “pornography” or “insult[s] or slander[s] others.” The Terms also prohibit content relating to others’ “privacy, personal information or materials” or “information containing any sexual content or sexual connotation” or other information that “contradicts to social morality.”⁹⁶

If WeChat receives reports or complaints against a user in violation of these Terms, the Terms state that WeChat is entitled to remove or obscure relevant contents at any time without notice and impose a punishment on the account including issuing a warning, restricting or prohibiting use of some or all of the function, or banning the account altogether.⁹⁷

For users outside China, a different Terms of Service applies.⁹⁸ According to WeChat’s Acceptable Use Policy, it is prohibited for users to upload or transmit content that is “pornographic, sexually explicit, violent or otherwise of a mature nature” or encourages transmission of such content, and to “share or publish any other person’s personally identifiable information using WeChat without their express consent.” The Policy also prohibits content that is harmful or exploitative including via bullying, harassment, or threats of violence; breaches any laws or regulations; infringes on intellectual property rights; or is fraudulent, false, misleading or deceptive. Moreover, it is prohibited to “impersonate any person or misrepresent your affiliation with any person or entity in registering an account (including by creating a misrepresentative account name or accessing another user’s account) or in making any communications or sharing or publishing any content or information using WeChat.”⁹⁹ WeChat also has a specific Copyright Policy which details how the service deals with intellectual property-related complaints in accordance with the DMCA.¹⁰⁰

WeChat states in its Terms of Service that it may suspend or terminate a user’s access to his or her account if they reasonably believe that the user has breached these Terms or if the user’s use of WeChat creates risk for other users.

⁹⁶ *Agreement on Software License and Service of Tencent Weixin*, WECHAT, https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=weixin_agreement&s=default&cc=CN (last visited Jan. 8, 2019).

⁹⁷ *Id.*

⁹⁸ *WeChat Terms of Service*, WECHAT, https://www.wechat.com/en/service_terms.html (last visited Jan. 8, 2019).

⁹⁹ *WeChat Acceptable Use Policy*, WECHAT, https://www.wechat.com/en/acceptable_use_policy.html (last visited Jan. 8, 2019).

¹⁰⁰ *Protection of Intellectual Property in Action*, WECHAT, <https://www.tencent.com/legal/html/en-us/index.html> (last visited Jan. 8, 2019).

III. Social Media

A. Facebook

Facebook is one of the most popular social networking sites where users share photos, written posts, links, events, and much more to their “timeline” for their Facebook friends to see. Facebook is also the parent company for the popular social media applications WhatsApp and Instagram.¹⁰¹ If a Facebook account is “public,” anyone can see what the user posts, regardless of whether the user has Facebook — the public account information is accessible via the Internet and potentially elsewhere.¹⁰² If an account is “private,” only individuals that the user adds as friends can view their “timeline,” or public profile of what the user shares.

If a private account user shares an intimate photo on their page with friends, that photo will be accessible to everyone who is a Facebook friend of the individual who shares it. If a user shares an intimate photo publicly, then that photo will not only be accessible to everyone who visits the user’s profile but other users can then share the photo with more people on their own accounts or timelines.

If a user reports that an intimate photo of them has been shared without their consent, Facebook will remove the photo if it violates Facebook’s Community Standards on nudity and sexual content. Facebook states that they “default to removing sexual imagery to prevent the sharing of non-consensual or underage content.”¹⁰³ Facebook also uses “photo-matching technologies to help thwart further attempts to share the image on Facebook, Messenger and Instagram.”¹⁰⁴ Facebook has created its own Cyber Rights guide, called “Not Without My Consent.”¹⁰⁵

If a user violates Facebook’s Terms of Service by posting a nonconsensual sexually explicit photo that violates its Community Standards, the user may be prohibited from using Facebook or holding an account in the future.

To report an image or photo, a Facebook user who is logged in to their account can click the “Options” hyperlink (which appears at the bottom of the picture). After clicking the “Options”

¹⁰¹ Nina Godlewski, *What Company Owns Instagram? Five Companies Owned by Facebook and How They Use Your Information*, NEWSWEEK (Mar. 26, 2018, 2:21 PM), <https://www.newsweek.com/facebook-own-instagram-does-companies-apps-data-860732>.

¹⁰² *What is public information?* FACEBOOK, <https://www.facebook.com/help/203805466323736> (last visited Jan. 8, 2019).

¹⁰³ *Community Standards: Adult Nudity and Sexual Activity*, FACEBOOK, https://www.facebook.com/communitystandards/adult_nudity_sexual_activity (last visited Jan. 8, 2019).

¹⁰⁴ Antigone Davis, *Using Technology to Protect Intimate Images and Help Build a Safe Community*, FACEBOOK NEWSROOM (Apr. 5, 2017), <https://newsroom.fb.com/news/2017/04/using-technology-to-protect-intimate-images-and-help-build-a-safe-community/> (last visited Jan. 8, 2019).

¹⁰⁵ *Not Without My Consent*, FACEBOOK, <https://fbnewsroomus.files.wordpress.com/2017/03/not-without-my-consent.pdf> (last visited Mar. 20, 2019).

link, users have the option of clicking a link to “Give feedback or report photo,” which will lead to a reporting website.¹⁰⁶

B. Instagram

Instagram is a social media network for sharing photos and short videos on a profile, which can be made public (available to anyone on the Internet) or private (viewable only by those whom a user accepts as followers). It is largely used as a mobile app. Any Internet user can view Instagram photos if the photo’s privacy settings are set to public. If a person reports that an intimate photo has been shared of them without their consent, Instagram will remove the photo if it violates its Community Guidelines, which prohibits nudity and content showing sexual intercourse.¹⁰⁷

A user can report a photo or user through two options:

1. **Report within Instagram, directly from the photo.**

If you are logged in to the Instagram app, click “Report User” or “Report Photo” when looking at a posted image.

2. **Report directly to Instagram using an outside form.**

Instagram has a form that allows anyone to report a photo or a user that is violating Instagram’s Terms of Use, whether or not the person reporting has an Instagram account.¹⁰⁸

C. Snapchat

Snapchat, a multimedia messaging app, is one of the most popular mobile apps used by millennials and teens. Snapchat allows users to post and share pictures and messages that disappear after a period of time. “Snaps” (i.e., videos or pictures) are automatically made unavailable to recipients after they are viewed. There is sometimes an option to “replay” a Snap. “Snapchat stories” (i.e., a series of Snaps), which a user can post to their profile or send to specific recipients, disappear after 24 hours. Most messages sent via Snapchat, including Snaps and Stories, are deleted once they have been viewed, or once they expire after 24 hours. However, there are some exceptions, such as Memories. A user can save Snaps and Stories to Memories, which keeps them saved until the user deletes them. Memories are backed up by Snapchat.¹⁰⁹

¹⁰⁶ Various users reported on Quora.com that responses from Facebook took between 1-2 weeks to up to a month.

¹⁰⁷ *Instagram: Community Guidelines*, INSTAGRAM, https://help.instagram.com/477434105621119?helpref=faq_content (last visited Jan. 8, 2019).

¹⁰⁸ The form can be found here: https://help.instagram.com/contact/383679321740945?helpref=faq_content.

¹⁰⁹ *Snapchat Support: When does Snapchat delete Snaps and Chats?*, SNAPCHAT, <https://support.snapchat.com/en-US/a/when-are-snaps-chats-deleted> (last visited Jan. 8, 2019).

Snapchat has been used to share sexually explicit content and has become a popular platform for “sexting.”¹¹⁰ Even though many users believe that Snapchat is safe for sending sexually explicit images because the images disappear, there is always the possibility that the recipient of the image will take a screenshot (which is very easy to do) to preserve that image even after it disappears on the Snapchat app. Although the sender is notified of any screenshots that are taken, there is nothing the initial sender can do to get back the image or video after a screenshot has been taken.

Snapchat’s Community Guidelines prohibit accounts that promote or distribute pornographic content.¹¹¹ The Guidelines also encourage users to never “post, save, or send nude or sexual content involving people under the age of 18—even of yourself” and caution users not to take Snaps of “people in private spaces...without their knowledge and consent.” If a user violates these Guidelines, Snapchat states that they may remove the offending content, terminate the account, or notify law enforcement.

A user can report a story or account belonging to another user under Snapchat Support’s section titled “Safety” or within the app itself.

PRACTICE TIP: Snapchat now has *SnapCash*, which enables users to transfer money across accounts. This could enable online sexual abuse and pornography, and victims or advocates considering taking legal action against a perpetrator of cyber sexual abuse should try to obtain the monetary transactional history between the abuser and recipients of the Snaps.

Snapchat can retrieve the content of sent messages if at least one recipient has yet to view the Snap, and they will assist law enforcement in criminal investigations when a search warrant is obtained. A federal or state search warrant is required for requests that include message content.

D. Twitter

Twitter is a social media platform used as both a desktop website and an app; it is sometimes referred to as a “micro-blog.” Users can “tweet” (i.e., post) text, photos, and articles, and can “retweet” (i.e., share) what others post, but posts are limited to 280 characters (except for Japanese, Chinese, and Korean). The popularity of a person or celebrity is often measured by how many Twitter followers he or she has, and Twitter is used by individuals as well as companies, government officials, and others.

A “hashtag” (a word or phrase preceded by a “#” symbol) makes tweets searchable by that hashtag. For instance, if a user searches for #nude, all photos or tweets that are tagged with #nude across the entirety of Twitter will appear in the search results. Twitter can be used to share intimate

¹¹⁰ Sexting is sending, forwarding, or receiving sexually explicit messages, photos, or videos of oneself to others. It is usually done on mobile phones via text message or through apps that allow messaging (e.g., WhatsApp, Facebook Messenger, WeChat, or dating websites).

¹¹¹ *Community Guidelines*, SNAPCHAT, <https://support.snapchat.com/en-US/a/guidelines> (last visited Jan. 8, 2019).

photos of someone without his or her consent, and images can spread and “go viral” extremely quickly because of the way Twitter is set up to enable users to retweet and “like” others’ posts.

Twitter “prohibits the posting or sharing of intimate photos or videos that were or appear to have been taken or distributed without the subject’s consent.”¹¹² Twitter gives these examples that are not permitted in its Terms of Use:

- Hidden camera content involving nudity, partial nudity, and/or sexual acts;
- Images or videos that appear to have been taken secretly and in a way that allows the user to see the other person’s genitals, buttocks, or breasts (content sometimes referred to “creepshots” or “upskirts”);
- Images or videos captured in a private setting and not intended for public distribution; and
- Images or videos that are considered and treated as private under applicable laws.

To report an image or photo, there are two options.

1. Report within Twitter, directly from the image.

There is an option to report a user directly to Twitter if you believe the user has violated Twitter’s Rules:

Navigate to the offending Tweet → *More* → *Report* → *It’s abusive or harmful* → Select Either: *Includes an unauthorized photo of me* OR *give more information about the incident*

2. Report directly to Twitter from an outside form.

There is an external form that allows anyone to report a photo or a user violating Twitter’s Rules. An account is not required to report.¹¹³

Twitter will suspend any account it identifies as the original poster of intimate media that has been produced or distributed without the subject’s consent. It will also suspend any account dedicated to posting this type of content.

E. LinkedIn

LinkedIn is a professional social networking site. It is used primarily by working professionals seeking employment opportunities and employers looking to hire. Each user’s profile contains a resume-like history of their professional experience and education. LinkedIn

¹¹² *Help Center: Twitter Rules and policies: About intimate media on Twitter*, TWITTER, <https://help.twitter.com/en/rules-and-policies/intimate-media> (last visited Jan. 8, 2019)

¹¹³ The form can be found here: https://help.twitter.com/forms/private_information.

features a newsfeed similar in style to Facebook’s newsfeed, where users can see and share articles, photos, or posts. Limited public information is available, but only LinkedIn users who are logged into their accounts can view another user’s full public LinkedIn profile. LinkedIn is not typically used as a “revenge porn” site, but could potentially be used to post pictures without consent, especially to harass or embarrass a victim who uses the site for professional networking.

LinkedIn does not have a specific policy on cyber sexual abuse. However, its Terms of Use states that users may not “disclose information that [they] do not have the consent to disclose (such as confidential information of others (including [their] employer)).”¹¹⁴

To report an image posted without consent on LinkedIn, click the *More* icon in the right corner of the post on your LinkedIn homepage. Click *Report this post* → Select the applicable reason from the *Why are you reporting this?* pop-up window and follow the on-screen instructions → Click *Submit* to proceed with reporting the post, or *Back* to review your options.

F. Flickr

Flickr is a free online photo sharing platform managed by Yahoo where users can post and share photos. Flickr will remove intimate images that are posted without the subject’s consent. The Flickr Community Guidelines state, “Flickr also has a zero tolerance policy towards sharing adult or sexualized content of another person without that person’s consent (Non-Consensual Pornography).”¹¹⁵ Flickr also has a specific help page dedicated to assisting victims of cyber sexual abuse and providing information about potential resources and support.¹¹⁶

To report/remove a photo from Flickr, you must go through Yahoo’s removal process with the following steps:

At the bottom of the page that contains the photo or video, click *Report Abuse* → *Intimate content posted without my consent* → Enter your e-mail address → In the “What’s the problem?” field, describe that you appear in an intimate image or video without your consent and any additional details that may assist in an investigation → Enter the word “flickr” in the security field → Click *Send*. You may also send an e-mail to Flickr’s general help e-mail account at help@flickr.com.

G. Tumblr

Tumblr is a blogging website where users can post photos, music, written posts, links to articles, and others to their own blog page(s). There are more than 200 million blogs on the

¹¹⁴ *User Agreement*, LINKEDIN, <https://www.linkedin.com/legal/user-agreement> (last visited Jan. 8, 2019).

¹¹⁵ *Policies and Guidelines: Flickr Community Guidelines*, FLICKR, <https://www.flickr.com/help/guidelines> (last visited Jan. 8, 2019).

¹¹⁶ *Help Center: Trust and Safety: Get help if someone posts intimate content of you without your permission*, FLICKR, https://help.flickr.com/en_us/get-help-if-someone-posts-intimate-content-of-you-without-your-permission-SkxcY2Qjym (last visited Jan. 8, 2019).

platform.¹¹⁷ Flickr is popular among millennials, and is, as of February 2019, one of the ten most popular social networking sites online. Users can use Tumblr to search for and filter media based on their personal interests as well as trends in pop culture.

Tumblr will remove intimate content that is posted without permission and recently moved to ban all types of pornography from its platform altogether.¹¹⁸

According to a post dated August 11, 2018, Tumblr stated it would be eliminating any ambiguity in its zero-tolerance policy on nonconsensual sexual images:

We're adding a very simple statement . . . to our existing policy on harassment to remove any uncertainty . . . Don't engage in targeted abuse or harassment. Don't engage in the unwanted sexualization or sexual harassment of others. Posting sexually explicit photos of people without their consent was never allowed on Tumblr, but with the invention of deepfakes and the proliferation of non-consensual creepshots, we are updating our Community Guidelines to more clearly address new technologies that can be used to humiliate and threaten other people.¹¹⁹

As of December 17, 2018, Tumblr's Community Guidelines include the following statement under the "Privacy Violations" section: "Absolutely do not post non-consensual pornography—that is, private photos or videos taken or posted without the subject's consent."¹²⁰

Tumblr may require a victim to send a photo holding up a sign to prove that he/she/they is the one featured in the explicit content; however, Tumblr has implemented security measures to keep this material private.¹²¹

There are two ways to report an image posted without consent:

1. For logged in users on the dashboard

Click on the ellipses to the left of the reblog icon → Select *Flag this Post* → Select *This violates Tumblr's Community Guidelines* → Select *Someone is at risk of harm* → Select *Privacy violation* and answer the remaining questions to give Tumblr all of the information they need to take action.

¹¹⁷ *Why Tumblr?* TUMBLR, <https://www.tumblr.com/business> (last visited Jan. 8, 2019).

¹¹⁸ Jonah Engel Bromwich & Katie Van Syckle, *Tumblr Fans Abandon Ship as Tumblr Bans Porn*, N.Y. TIMES (Dec. 6, 2018), <https://www.nytimes.com/2018/12/06/style/tumblr-porn.html>.

¹¹⁹ *Our Community Guidelines are Changing*, TUMBLR (Aug. 27, 2018) (<https://staff.tumblr.com/post/177449083750/new-community-guidelines>).

¹²⁰ *Community Guidelines: What kind of violation is it?*, TUMBLR, <https://www.tumblr.com/abuse/> (last visited Jan. 8, 2019).

¹²¹ *Online Removal Guide*, CYBER CIVIL RIGHTS INITIATIVE, <https://www.cybercivilrights.org/online-removal/#tumblr> (last visited Jan. 8, 2019).

2. Users reporting content from the blog network can do so via Tumblr’s Privacy Violation Form.

Click on Tumblr’s Privacy Violation Form, which can be found here: <https://www.tumblr.com/abuse/privacy> → Click *Yes* (to “Is it your privacy that’s being violated?”) → Click *Private images of me have been posted* → Provide the information that is requested. (Tumblr needs proof of identity to move forward.)

H. YouTube

YouTube is a video-sharing website that allows users to upload videos onto their account for others to search and watch. YouTube contains a range of user-uploaded and corporate content such as vlogs (video blogs); music videos; movie trailers; public service announcements; and tutorials. A video’s settings can be set to public (seen by and shared with anyone), private (seen only by selected users) and unlisted (seen and shared by anyone with the link, but does not appear on YouTube or in search results). A user can search for particular content. YouTube also has a movie-screening service, where a user can rent or buy movies off the site, similar to Netflix or Amazon Video. Users do not need an account to search the site or watch YouTube videos. YouTube can be used for cyber sexual abuse if a user uploads pornographic or intimate videos of a subject without their consent.

YouTube does not have a specific policy on nonconsensual pornography, however YouTube prohibits content that is pornographic in nature or that contains nudity. It also prohibits “posting someone’s personal information; maliciously recording someone without their consent; deliberately posting content in order to humiliate someone; and unwanted sexualization, which encompasses sexual harassment or sexual bullying in any form.”¹²²

To report a video that violates the Community Guidelines, you may follow the directions found on this webpage, depending on how you wish to file the report (i.e., reporting a single video versus reporting an entire account): <https://support.google.com/youtube/answer/2802027>.

YouTube reserves the right to terminate a user's access to the Service if, “under appropriate circumstances, the user is determined to be a repeat infringer.” YouTube also reserves the right to decide “whether Content violates these Terms of Service for reasons other than copyright infringement, such as, but not limited to, pornography, obscenity, or excessive length. YouTube may at any time, without prior notice and in its sole discretion, remove such Content and/or terminate a user's account for submitting such material in violation of these Terms of Service.”¹²³

¹²² *Harassment and cyberbullying policy*, YOUTUBE, https://support.google.com/youtube/answer/2802268?hl=en&ref_topic=2803176 (last visited Jan. 8, 2019).

¹²³ *Terms of Service: Account Termination Policy*, YOUTUBE, <https://www.youtube.com/static?template=terms> (last visited Jan. 8, 2019).

IV. Pornography Websites

Nonconsensual intimate images can be posted without consent on any number of pornography websites (e.g. Porn Hub) or specific dedicated “revenge porn” websites (e.g., the now defunct, Anon-IB). There are several specific “revenge porn” websites, which are online collections of nude or sexually explicit images that are posted without the victim’s consent. Typically, these images are submitted to revenge porn websites by an ex-spouse or ex-partner, though at times, may be collected and submitted by hackers.

More established pornography websites do have policies in place to request removal of photos or videos uploaded without consent. For instance, Porn Hub has an online content removal portal where one can file a removal request: [https://www.pornhub.com/content-removal\(NSFW\)¹²⁴](https://www.pornhub.com/content-removal(NSFW)¹²⁴). Others websites will likely not respond to a request for removal, and your best avenue of remedy may be through a DMCA takedown notice (discussed *infra* in Part 5- Copyrighting and Removing Images from the Web).

V. Dating Websites

Currently, there are numerous dating websites and apps on the market. On these platforms, users create a profile to connect with other users seeking romantic encounters, and are generally able to filter algorithmic results by geography, age, and gender, among other criteria. Leading websites include Match.com, EHarmony, OK Cupid, Christian Mingle, JDate, and FetLife. Some websites provide places for prostitution such as Seeking Arrangement, Craigslist, and the now-defunct Backpage. Popular apps include Tinder, Grindr, Bumble, Coffee Meets Bagel, Hinge, PlentyOfFish, Happn, and Raya. The different services cater to different markets and have unique protocols. Some services are intended solely for facilitating sexual encounters (“hookup sites”) while others introduce people seeking long-term commitment. For the purposes of this section, only the most popular services are surveyed.

A. Match.com

Match.com is a dating website where individuals can create an online profile by answering questions about their sexual preference, desired age and characteristics of their intended partner, and other geographic and personal details that help the website generate search results fitting the criteria. The site has more than 7 million users. Match.com, and other similar dating websites, could be used to facilitate cyber sexual abuse if a user creates a profile of a victim without his or her consent using explicit photos or language, or threatens to do so.

Match.com does not have an explicit cyber sexual abuse policy. Match.com prohibits sharing “any offensive, inaccurate, abusive, obscene, profane, sexually oriented, threatening, intimidating, harassing, rude, vulgar, derogatory, sexist, defamatory, insulting, racially offensive,

¹²⁴ NSFW means “Not Safe for Work,” a reference used when a link likely contains pornographic images.

or illegal material, or any material that infringes or violates another person’s rights (including intellectual property rights, and rights of privacy and publicity).”¹²⁵

It also prohibits a user posting information that contains video, audio photographs, or images of another person without his or her permission (or in the case of a minor, the minor’s legal guardian); provides material that exploits people in a sexual, violent or other illegal manner; or that solicits passwords or personal identifying information for commercial or unlawful purposes from other users or disseminates another person’s personal information without his or her permission.”¹²⁶ Match.com reserves the right to terminate a user’s account if any of these terms, or other Terms of Use, are violated, and reserves the right to take legal action against a user.

To report a user for posting personal information without consent, you may use an online form found at: <https://www.match.com/help/contactus.aspx?lid=108>.

B. Tinder

Tinder is a dating app used primarily on smartphones. Users create a profile and can view other users’ profiles within their search parameters. If users want to connect, they “swipe right” on a person’s profile. If users are not interested, they “swipe left” to not be connected. If two users “swipe right” on each other, they will be connected and are able to message each other privately. Someone could use Tinder for cyber sexual abuse by creating a profile for someone without his or her permission. An abuser could easily impersonate a victim using publicly available or privately shared images (perhaps within the context of a prior relationship, consensual or otherwise) and set up unwanted or unknown in-person meetings by sharing the victim’s actual contact and address details.

Tinder’s Terms of Use states that users may not “impersonate any person or entity or post any images of another person without his or her permission; bully, “stalk,” intimidate, assault, harass, mistreat or defame any person; post any content that is hate speech, threatening, sexually explicit or pornographic; incites violence; or contains nudity or graphic or gratuitous violence; or solicit passwords for any purpose, or personal identifying information for commercial or unlawful purposes from other users or disseminate another person’s personal information without his or her permission.”¹²⁷

Tinder reserves the right to “investigate and/or terminate your account without a refund of any purchases if you have violated this Agreement,” including if the violations occurred outside the service. It also reserves the right to remove any content in violation of this agreement or “take

¹²⁵ *Match.com Terms of Use Agreement*, MATCH.COM (last revised Dec. 28, 2017), <https://www.match.com/registration/membagr.aspx>.

¹²⁶ *Id.*

¹²⁷ Terms of Use, TINDER, <https://www.gotinder.com/terms/us-2018-05-09> (last revised May 9, 2018).

any available legal action in response to illegal and/or unauthorized uses of [Tinder], including termination of your account.”¹²⁸

To file a report of content posted without permission, you can use this online form to contact customer service: <https://www.gotinder.com/help>. You may also call 214-853-4309 for general assistance.

C. Grindr

Grindr is a dating app for mobile smart phones that uses GPS software to connect people in close geographic proximity easily in real time. It is specifically geared towards the LGBTQ community, and there are approximately 27 million Grindr app users.¹²⁹ When a user opens the app, they see a grid of other Grindr users who are located within a certain distance. There is no matching system and any user can contact any other user.

Grindr expressly states in its Terms of Use to users that:

- “You will NOT use the Grindr Services or any information displayed within the Grindr Services to stalk, harass, abuse, defame, threaten or defraud other Users; violate the privacy or other rights of Users; or collect, attempt to collect, store, or disclose without permission the location or personal information about other Users;
- You will NOT include offensive or pornographic materials, or materials that are harmful in Your Grindr Services personal profile page;
- You will NOT include material on Your personal profile page which contains video, audio, photographs, or images of any person under the age of eighteen (18) at all or any person over the age of eighteen (18) without his or her express permission.”¹³⁰

Grindr reserves the right to suspend and/or terminate a user’s account for violating any of the Terms of Use.

Despite these policies, Grindr has proven to be unresponsive to even well-documented complaints regarding harassment and impersonating profiles, and unfortunately, without the company’s cooperation, victims have little recourse. In *Herrick v. Grindr, LLC*, 306 F. Supp. 3d 579, 584 (S.D.N.Y. 2018) the court dismissed a victim’s complaint attempting to hold Grindr liable for any of the damage (including harassment, stalking, emotional distress, invasion of privacy and

¹²⁸ *Id.*

¹²⁹ Jon Shadel, *Grindr was the first big dating app for gay men. Now it’s falling out of favor*, WASH. POST (Dec. 6, 2018), https://www.washingtonpost.com/lifestyle/2018/12/06/grindr-was-first-big-dating-app-gay-men-now-its-falling-out-favor/?utm_term=.99a8fc92a643.

¹³⁰ *Grindr Terms and Conditions of Service*, GRINDR, <https://www.grindr.com/terms-of-service/> (last visited Jan. 8, 2019).

copyright infringement) he suffered due to Grindr’s failure to remove and/or terminate the accounts set up by the victim’s ex-boyfriend impersonating the victim.¹³¹

To report an issue to Grindr, you may contact help@grindr.com or legal@grindr.com. There is no specific takedown policy for nonconsensual intimate or sexual content, but there is a takedown policy for copyright infringement.

D. Seeking Arrangement

Seeking Arrangement is a “Sugar Baby” and “Sugar Daddy” membership-based networking site.¹³² The site is designed to allow networking and matching between people who want to engage in “Sugaring,” where young people connect with older, wealthy people who exchange money and a lavish lifestyle for being “accompanied at all times” by the so-called “Sugar Babies,” with sexual interactions expected.¹³³ “Sugar Babies” can create a profile free of charge, and receive special benefits if they use a university ID. “Sugar Daddies” (and “Sugar Mommas”) register for free for a free trial period and then have to pay a monthly or annual membership fee. There are currently 8 million men and women registered on Seeking Arrangement.

Cyber sexual abuse is possible through Seeking Arrangement. As discussed with other services above, fake profiles could be created leading to harassment. Additionally, exchanging photos is very common on the site which could lead to exploitation and/or blackmail. It is also possible for a user of the site to post a photo of another person on their profile without the person’s consent.

Seeking Arrangement will remove photos of a victim posted on the site without consent.¹³⁴

To report a photo posted without the subject’s consent, the site states, “you can request that the photo be removed by writing to customer support. Be sure to provide your e-mail address so we may contact you if we have questions.” They may require a copy of a government-issued ID or other evidence to prove that the photo belongs to the person making the report. To write to customer support, you can fill out the fields found at this webpage: <https://www.seeking.com/help/ticket>.

¹³¹ The case is currently on appeal in the Second Circuit. See Adam Klasfeld, *Appeal over Grindr Nightmare Takes On '96 Internet Law*, COURTHOUSE NEWS SERVICE (Jan. 7, 2019) <https://www.courthousenews.com/appeal-over-grindr-nightmare-takes-on-96-Internet-law/>.

¹³² For a definition of “sugar” relationships, see *Sugar Relationship*, SEEKING ARRANGEMENT, <https://www.seeking.com/glossary/sugar-dating/sugar-relationship> (last visited Jan. 8, 2019).

¹³³ Amanda M. Fairbanks, *Seeking Arrangement: College Students Using ‘Sugar Daddies’ To Pay Off Loan Debt*, HUFFINGTON POST (Dec. 6, 2017), https://www.huffingtonpost.com/2011/07/29/seeking-arrangement-college-students_n_913373.html.

¹³⁴ *Terms of Use*, SEEKING ARRANGEMENT (Oct. 30, 2018), <https://www.seeking.com/terms>.

E. Craigslist

Craigslist is the most popular online classified advertisements site in the United States, with categories ranging from items for sale to job postings to services offered to items wanted. Craigslist is often used as an outlet for cyber sexual abuse when users post intimate or sexual images of victims on a Craigslist ad, often with personal identifying information. Although personal ads on Craigslist were discontinued in March 2018, there is a page in the community section called “Missed Connections.”¹³⁵ Missed Connections is a tool for users to post descriptions of meetings with strangers that they did not have the capability, time or confidence to approach, in hopes that the stranger will recognize the posting and contact the user. This site, though less dangerous than the personal ads that are often used exclusively for sexual encounters, could be used for cyber sexual abuse if photos, identification, or contact information of a victim is posted with a sexually explicit message.

If an image is shared without consent, the victim can contact Craigslist to request its removal using an online form. The form requires the victim to input specific information, such as the ID on the post itself, as well as the location of the posting and keywords that might appear in the text of the post. To report/request removal of a posting, you can contact Craigslist at this link: https://sfbay.craigslist.org/contact?step=form&reqType=abuse-911_other.

VI. **Google Search Results**

Google is a search engine that can be used to find information related to a search topic. Google uses a computer program called a “web crawler” that searches through billions of websites and examines their content to find matching “keywords.” The search results are links to the websites that contain content most related to your search input.

When Internet users search for sexual content on Google, nonconsensual images of a cyber sexual abuse victim could appear in the search results. If the image is linked to the victim’s name, birthday, phone number, or other personally identifying pieces of information, those non-consensual intimate images may show up in search results by friends, family members, or potential employers, having serious repercussions for the victim’s mental health, career options, and financial stability.

Google will remove nonconsensual images from search results if:

- The subject is nude or shown in a sexual act;
- The subject intended the content to be private and the imagery was made publicly available without their consent; or

¹³⁵ Lisa Bonos, *Goodbye, Craigslist personal ads. Those seeking casual sex will miss you*, WASH. POST (Mar. 23, 2018), https://www.washingtonpost.com/news/soloish/wp/2018/03/23/goodbye-craigslist-personal-ads-those-seeking-casual-sex-will-miss-you/?noredirect=on&utm_term=.62022d638751.

- The subject did not consent to the act and the imagery was made publicly available without their consent.¹³⁶

Google can only prevent a page from appearing in its search results. It cannot remove content from websites that host it, so Google recommends reaching out to the webmaster of the site to request removal first. You can get more details on that process at this link: <https://support.google.com/websearch/answer/9109>.

To report and request that content be removed from Google search results, you can use an online form found here: <https://support.google.com/websearch/troubleshooter/3111061#ts=2889054%2C2889099%2C2889064%2C3143868%2C6256340>.

PRACTICE TIP: It is important to make the request to remove content as quickly as possible to reduce the chance that the image(s) will appear in search results and be widely shared by others. But always remember to first take a screenshot of the search results in the event that you later want to pursue legal action.

VII. Other

A. Reddit

Reddit is a social news aggregation, web content rating, and discussion website. Reddit users submit content to the site and then other members vote the content “up or down.” Posts are organized by subject into user-created boards called “subreddits,” which cover a variety of topics including news, science, movies, video games, music, books, fitness, food, and image-sharing. Submissions with more up-votes appear towards the top of their subreddit and, if they receive enough votes, ultimately on the site’s front page. Reddit is a frequent outlet for abusers to post sexual images without the subject’s consent.

Reddit prohibits the dissemination of images or videos depicting any person in a state of nudity or engaged in any act of sexual conduct apparently created or posted without their permission.¹³⁷ Images or video of intimate parts of a person’s body, even if the person is clothed or in public, are also not allowed if apparently created or posted without their permission and “contextualized in a salacious manner (e.g., ‘creepshots’ or ‘upskirt’ imagery).”¹³⁸ Moreover, Reddit prohibits users from posting fake explicit content, such as “lookalike pornography.”

¹³⁶ *Remove unwanted & explicit personal images from Google*, GOOGLE, <https://support.google.com/websearch/answer/6302812?hl=en> (last visited Jan. 8, 2019).

¹³⁷ Matt Burgess, *The fightback against AI-generated fake pornography has begun*, WIRED (Feb. 8, 2018), <https://www.wired.co.uk/article/deepfakes-banned-reddit-ai-creates-fake-porn-gyfcats>.

¹³⁸ *Reddit Help: Rules & Reporting: Account and Community Restrictions: Do Not Post Involuntary Pornography*, REDDIT, <https://www.reddithelp.com/en/categories/rules-reporting/account-and-community-restrictions/do-not-post-involuntary-pornography> (last visited Jan. 8, 2019).

1. Report within Reddit if you have an account, directly from the post:

Click the “comments” link under the post → *report* → Type in “Involuntary Pornography” as the report reason and click submit → Send the URL of the comments page to contact@reddit.com with the subject “Involuntary Pornography Report.”

2. Report to Reddit without an account:

Click the “comments” link under the post → Send the URL of the comments page to contact@reddit.com with the subject “Involuntary Pornography Report.”

3. A reporting webpage can also be found at this link:
<https://www.reddithelp.com/en/submit-request/breaking-content-policy>.

VIII. A Note on Liability for Social Media Providers

Due to a 1996 federal law, the Communications Decency Act (“CDA”), and its Section 230 exception (“Section 230”), Internet service providers (“ISPs”) are generally not held liable for posts made by individuals on their websites or applications. Put simply, Section 230 provides broad immunity for ISPs and makes it nearly impossible for lawyers to hold companies like Facebook, Grindr, Craigslist, and others accountable for abuse that happens on their websites and apps. There has been recent legislative progress in creating limited exceptions to Section 230, specifically for websites that knowingly promote or facilitate advertising activity that violates federal sex-trafficking laws, but ISPs have been extremely successful in arguing that free speech concerns trump further regulation.

PART 4 - EVIDENCE COLLECTION

Physical evidence will help corroborate witness testimony and might even be considered stronger than testimony, so collecting physical evidence to support your/your client's case is important. When it comes to issues of evidence preservation in cyber sexual abuse cases, time is often of the essence. Data can be erased by an abuser or deleted automatically (such as Snapchat posts or text messages) and devices where such evidence is preserved may be lost, stolen, or broken. Backing up evidence in multiple formats and locations is critical. Cloud storage is preferable to device storage (keeping in mind that cloud storage may be vulnerable to hacking attempts). Moreover, if your client plans on contacting the web sites directly to have the posts taken down, you and/or your client should preserve the evidence before making those requests.

Make sure you are thinking broadly about what evidence to preserve. You want to capture all relevant posts and pictures online and in your client's apps; all texts, messages, voicemails and call logs from your client's phone and other devices; as well as any data that could connect the online post to the abuser, such as the IP address or geolocation data of the poster.

I. Prior to Litigation: Active Steps Clients Can Take to Preserve Evidence

Even though a victim's first impulse might be to destroy all traces of any photos they find online, they should collect the evidence first by taking screenshots and turning web pages into PDFs. (See [Appendix A](#) for a Step-by-Step Evidence Preservation Guide which includes a description on turning web pages into PDFs.) A victim should ideally take screenshots of all potential evidence for their case, including but not limited to:

- Copies of any nonconsensual images and videos shared online;

PRACTICE TIP: Ensure that any screenshotted photos or videos are saved in a secure and safe location so that they will not be further stolen and/or disseminated by an abuser.

- Online Comments;
 - It is important to save comments regarding cyber sexual abuse, such as threats to post images/videos, or references to the images/videos themselves, because they underscore the harm of nonconsensual pornography to people like judges, prosecutors, and police and they demonstrate how the consumers of nonconsensual pornography end up becoming harassers by proxy.¹³⁹
- The search results that lead to the nonconsensual pornography;

¹³⁹ See Samantha Allen, *How to Fight Back Against Revenge Porn*, DAILY BEAST (Jan. 12, 2016, 12:01 AM), <https://www.thedailybeast.com/how-to-fight-back-against-revenge-porn> (discussing how important evidence collection is to fighting cyber sexual abuse).

- The web pages hosting the nonconsensual pornography – be sure to capture screenshots that include the date, time, and URL of the website. Ensure that the screenshot gets all of the information. (Also, a company called Page Vault helps preserve these images); and
- Texts, e-mails, and other communications related to the abuse.

PRACTICE TIP: When screenshotting a text, call, e-mail or other communication from a contact, ensure that the *original* phone number or e-mail address is visible in the screenshot, other than merely the contact name. This ensures proper admission into evidence at later proceedings – if the original phone number or e-mail address is not visible, it is much more difficult to authenticate the evidence.

Taking Screenshots

- On a computer:
 - On a Windows laptop or computer: Find the key on the keyboard that says: PrtScn, Prt Scr, or Print Screen. Press Ctrl and then the PrtScn keys. Immediately after taking the screenshot, open a document that lets you paste an image (such as Word, Google Docs, or Paint), and “paste” the screenshot. You should right-click on the image to save it as a separate file.
 - On a Mac laptop or computer: At the same time, press these keys: Shift + Command + 3. This will save the screenshot onto your computer desktop as a picture.
- On an iPhone:
 - To take a screenshot on any model iPhone except the iPhone X, hold down the Home button and the Lock button simultaneously.
 - To take a screenshot on an iPhone X (which does not have a Home button), hold down the Lock button and the Volume Up button simultaneously.
 - The phone will ask you to either “save screenshot” or “delete screenshot.” Click on “save screenshot,” and the screenshot will be saved to your camera roll.
- On an Android phone:
 - To take a screenshot on an Android phone, depress the Volume Down button and the Power button at the same time. The phone will take a screenshot, which will show up in the Gallery app.

Print out Pages and Store Them Securely

- For a Screenshot: On some computers, you can print a screenshot directly by opening the image and selecting “print” from the File menu. On others, you may need to paste

your screenshot or photo into a document using a program like Word, Pages, or Google Docs. You can then print the document that includes the screenshot.

- For a Web Page: Print the webpage by selecting “Print” from the File menu and following the prompts.
- You may also want to e-mail or text the document to a device that you will continue to have secure access to so that you have an extra copy in case the printout is lost or destroyed.

PRACTICE TIP: Screenshots should capture the date, time, and URL of the website.¹⁴⁰

PRACTICE TIP: If a communication doesn’t fully fit in one screenshot, make sure you overlap them and take multiple screenshots. Additionally, screenshots that are edited in any way will very likely not be deemed admissible in court as they have been manipulated.

PRACTICE TIP: For evidence that may be used in support of a complaint, save a digital copy to a computer file and save a printout to a binder. Take the binder with you when you go to your local police precinct, domestic violence clinic, or family court self-help center to file papers. Your printouts can then be attached to a police report or an application for a restraining order. The more organized a victim is, the greater the likelihood that law enforcement, restraining order clinics, online platforms, and prospective legal counsel will be able to help them.

- A victim or advocate should also attempt to contact the websites that are hosting the images/file a report with the websites and ask them to remove it. This may not always work, but it is important when building a legal case that the victim displays that they are actively trying to remove the non-consensually shared images.

PRACTICE TIP: A thorough summary of many of the most common social media, dating, and other websites and their cyber sexual abuse policies as well as guides on requesting takedowns of offending materials, is listed earlier in this Manual.

PRACTICE TIP: Consider making an argument based on Copyright Infringement; see Part 5 of this Manual.

PRACTICE TIP: Be aware of specific social media platforms and the ramifications for screenshotting these platforms. If you take screenshot on Snapchat or Instagram, it alerts the person who sent it. Applications such as Save my Snap will automatically save snaps without notifying the sender, but this is a

¹⁴⁰ PAGE VAULT, <https://www.page-vault.com/>.

violation of Snapchat’s terms. Relatedly, if you block someone on Instagram, you will no longer have access to your history of direct messages with them.

PRACTICE TIP: Evidence might be needed from intermediaries, like websites and e-mail service providers to unmask an anonymous defendant. You may need to ask those online service providers to save the evidence for later use (See subsection B below).

Videos

For a video, you should download the video onto a secure hard drive.

- **Downloading a video:** It is easiest to use an online video converter. Some examples include KeepVid, Convert2mp3.net, and ClipConverter.cc. Copy the link of the video into the website and click “Download.” Make sure, when downloading, that you are downloading the video, and not only the audio (do not download in mp3, but download in mp4). Once the video is downloaded, open it on your computer to make sure it is the right one and save it.
- **Saving to a secure, external hard drive:** Once the video is downloaded, transfer it to a secure hard drive or flashdrive. Purchase or find an external hard drive that is safe and your abuser does not have access to. Companies who sell external hard drives include; Western Digital, Lenovo, and Seagate. A flashdrive acts like a smaller and cheaper version of an external hard drive. To save the video onto the hard drive, connect the hard drive to the computer which the video is saved on (plug the Hard Drive or Flash Drive into a USB port). Open File Explorer. Click on the video and drag it to the external drive’s folder. After it is saved on the drive, unplug the drive and delete the video from the computer.

Ethical Considerations in Accessing or Sharing Data

Be aware that unlawfully intercepting or disclosing online communications without authorization is a felony under the Electronic Communications Privacy Act.¹⁴¹

Additionally, the NYC Lawyer’s Association Committee on Professional Ethics as warned that a lawyer who received metadata inadvertently from opposing counsel should avoid reviewing that metadata.¹⁴² Attorneys should take due care when communicating with opposing counsel by removing metadata from documents prior to sending. However, an attorney’s failure to remove this data does not permit the opposing counsel to utilize metadata that was inadvertently sent. Using such metadata is unethical if opposing counsel intends to search for the attorney’s “work

¹⁴¹ See 18 U.S. Code § 2511.

¹⁴² *Topic: Searching inadvertently sent metadata in opposing counsel’s electronic documents* (NYCLA COMM. ON PROF. ETHICS, OP. NO. 738, 2008), https://www.nycla.org/siteFiles/Publications/Publications1154_0.pdf (“A lawyer who receives from an adversary electronic documents that appear to contain inadvertently produced metadata is ethically obligated to avoid searching the metadata in those documents.”).

product client confidences or secrets or if the recipient is likely to find opposing counsel’s work product or client confidences or secrets by searching the metadata.”¹⁴³

PRACTICE TIP: Never pretend to be someone else online to access the content or to get the user to admit to posting the content.

The New York State Bar Association Committee on Professional Ethics has advised that a lawyer who represents a client in a pending litigation, and who has access to the social media network used by another party in litigation, may access and review the public social network pages of that party to search for potential impeachment material. As long as the lawyer does not “friend” the other party in an unethical manner or direct a third person to do so in order to obtain information, accessing the social network pages of the party will not violate New York Rule of Professional Conduct 8.4 (prohibiting deceptive or misleading conduct), Rule 4.1 (prohibiting false statements of fact or law), or Rule 5.3(b)(1) (imposing responsibility on lawyers for unethical conduct by non-lawyers acting at their direction).¹⁴⁴

PRACTICE TIP: An attorney (or the attorney’s agent) may use their real name and profile to send a “friend request” to obtain information from an unrepresented person’s social networking website without disclosing the reasons for making the request. While there are ethical boundaries to such “friending,” they are not crossed when an attorney or investigator uses only truthful information to obtain access to a website, subject to compliance with all other ethical requirements.

PRACTICE TIP: However, an attorney or investigator is prohibited from using publicly available information to create a false Facebook profile listing schools, hobbies, interests, or other background information likely to be of interest to a targeted witness in the hopes of getting the target to accept a friend request from the fake profile. This behavior is unethical and prohibited.

PRACTICE TIP: When preserving evidence, do not just preserve evidence that you believe is favorable to you. It is best to preserve all evidence that may be relevant to a dispute, including e-mails, text messages, correspondence, documents, photographs, videos, etc. Failure to properly preserve all the evidence, even if you believe it may be negative or unfavorable to you, may result in sanctions or adverse findings against you by a court.

¹⁴³ *Id.*

¹⁴⁴ NEW YORK STATE BAR ASS’N COMM. ON PROF. ETHICS, OP. NO. 843 (2010) (discussing lawyer’s access to public pages of another party’s social networking site for the purpose of gathering information for client in pending litigation), <http://www.nysba.org/CustomTemplates/Content.aspx?id=5162>; *see also* NEW YORK STATE BAR ASS’N COMM. ON PROF. ETHICS, FORMAL OP. NO. 2010-2 (2010) (discussing obtaining evidence from social networking websites), https://www.nycbar.org/pdf/report/uploads/20071997-Formal_Opinion_2010-2.pdf.

II. Important Considerations During Litigation

A. Litigation Hold Requests

While intermediary websites and platforms might maintain logs of users who access their systems, they do not keep this data for very long. Logs are useful identification tools. Data might include the date and time a user accessed the site or the user's IP address, which is a number assigned to every computer connected to the Internet that functions like a street address or phone number for the computer to which it is assigned. Internet service providers lease IP addresses to Internet users for a period of time. An Internet user could be identified by asking the website for the IP address associated with the content, and then asking for the identity of the person who was assigned to that IP address at the time. Generally, platforms will not give out this kind of information without a subpoena. However, they can preserve the information when and if they receive a hold request so that it will be available if a subpoena is sent during civil or criminal litigation. Therefore, promptly sending hold requests is critical to preparing for litigation.

Unfortunately, subpoenas are unlikely to be effective. The platform will likely claim that sharing the information violates the Stored Communications Act, and many providers are located in California and will insist on a local subpoena. Send the hold request first and then work on pursuing a subpoena.

A hold request letter should:

- a. inform the website that legal action is being considered;
- b. provide links to the material;
- c. request that the website provide, or archive and hold, all identifying information regarding the party or parties responsible for posting the material, including IP addresses.

B. Organizing Evidence

Cyber sexual abuse cases can quickly become overwhelmingly complex with large amounts of digital evidence. When presenting the evidence to law enforcement or family court, or perhaps even a jury, a clearly organized chart of the evidence will compellingly complement your arguments and can be included as an appendix in filings. Starting this chart early on will reduce your workload and confusion later.

At trial, the main hurdle is often proving that a specific perpetrator sent a specific transmission. Offenders tend to use new devices and public Wi-Fi when distributing the photos/videos. Services exist to mask IP addresses. Some may also use throwaway devices and/or a virtual private network (VPN) to make it seem as if the distribution originated from China or Russia. Getting logs and connection data from a foreign VPN provider (if the logs even exist) is difficult and tedious. Defendants will commonly argue that they themselves were hacked. A well-organized evidence chart can be used to show that only that perpetrator would have the motive and ability to create the campaign of cyber sexual abuse your client endured.

Consider different organizational systems depending on your specific case. Usually a chronological compilation will be most useful and straightforward; however, organizing by jurisdiction where abuse occurred, type of abuse, or suspected perpetrator may be better, depending on your facts. Consider different formats such as Excel, Word, or PDF. References or hyperlinks can be employed so that your chart remains neat and organized.

You will likely want to include the following information:

- Date, time, and location where victim became aware of the incident;
- What happened and the content of the material posted (in as much detail as possible);
- Documentation of the event and material posted (including whether it is still needed from a provider);
- Who you think did it;
- Evidence that they did it (such as IP address); and
- Effect on victim (if they had a specific reaction or consequence).

C. Presenting Evidence at Trial

Assuming you have successfully collected digital evidence of the abuse, it may still be difficult to use that evidence at trial. This section discusses the applicable admissibility and hearsay rules, largely using the Federal Rules of Evidence, which are largely followed in most jurisdictions. The evidence rules were created when it was more difficult to create fraudulent documents than it is now, and the law is slow to respond to fast-changing technology.

Some of the main barriers when it comes to evidence collection include:

- a. Proof of distribution (main hurdle): Offenders tend to use new devices and public Wi-Fi when distributing the photos/videos. Some may also use throwaway devices and/or a virtual private network (VPN), to make it seem as if the distribution originated from China or Russia. Getting logs and connection data from a foreign VPN provider (if the logs even exist) can be difficult and tedious.¹⁴⁵
- b. Issues with the original transmission: If neither the victim nor the perpetrator have a record or copy of the original transmission (perhaps both upgraded their devices or deleted old messages), then only their mobile carrier(s) may have the record of the initial transmission (if they were sent by text). Acquiring this data is time-consuming and resource-intensive. Note that many mobile carriers do not keep copies of the

¹⁴⁵ *The (Il)legalities and Practicalities of Revenge Porn*, BLACKSTONE LAW (last visited Jan. 10, 2019), <http://www.blackstone-law.com/bs/index.php/b1/90-blog/155-the-il-legalities-and-practicalities-of-revenge-porn>.

content of text messages, and the ones that do often keep the data only for a short period of time.¹⁴⁶

- c. Online evidence: It can be difficult to authenticate evidence that is found online and on social media, as many evidence rules were created when it was more difficult to create fraudulent documents than it is now.

D. Admissibility

The rules of evidence establish a series of hurdles that Electronically Stored Information (ESI) usually must overcome before being admitted into evidence.

- **Relevance** (Federal Rule of Evidence 401): Does the ESI have any tendency to make some fact that is of consequence to the litigation more or less probable than it otherwise would be? This fact must be one of consequence in determining the action.¹⁴⁷
- **Authenticity** (Federal Rule of Evidence 901): Is the ESI what it purports to be? The most common way to authenticate the evidence is through the testimony of a witness with knowledge of the evidence that it is what it claims to be.¹⁴⁸
 - This can frequently be done by affidavit from the provider in civil litigation but a criminal trial requires the in-person testimony from a representative of the provider.
- **Hearsay** (Federal Rule of Evidence 801): If offered for its substantive truth, is the ESI hearsay, and if so, is it covered by an exception to the hearsay rule?¹⁴⁹
- **Original Writing** (Federal Rule of Evidence 1003): Is the ESI an original or duplicate under the original writing rule, or if not, is there admissible secondary evidence to prove the content of the ESI?
 - This requirement is not as daunting as it sounds because courts have ruled that duplicates from social media can be admitted as evidence (See below section on duplicates under Hearsay).¹⁵⁰

¹⁴⁶ Suzanne Choney, *How long do wireless carriers keep your data?*, NBC NEWS (Sept. 29, 2011, 3:05 PM), <https://www.nbcnews.com/technolog/how-long-do-wireless-carriers-keep-your-data-120367/>.

¹⁴⁷ See FED. R. EVID. 401.

¹⁴⁸ See FED. R. EVID. 901.

¹⁴⁹ See FED. R. EVID. 801.

¹⁵⁰ See FED. R. EVID. 1003.

- **Probative Value and Unfair Prejudice:** Is the probative value of the ESI substantially outweighed by the danger of unfair prejudice, such that it should be excluded despite its relevance?¹⁵¹
- **Sufficient Likelihood:** When it comes to evidence that is coming from a website or an account, the requesting party must show “sufficient likelihood” that such an account would include relevant information that is “not otherwise available” before being granted access to it.¹⁵²

E. Authenticity

There are two main standards for authenticating ESI at trial. Under the Maryland Standard, social media evidence may only be authenticated through testimony from the creator of the social media post; hard-drive evidence or Internet history from the purported creator’s computer; or information obtained directly from the social media site itself.¹⁵³

However, New York uses the most common approach, known as the Texas Standard.¹⁵⁴

- The judge acts as gatekeeper for the evidence and the jury makes the final decision as to the reliability of that evidence;
- The party seeking to introduce the ESI must provide sufficient circumstantial evidence to support a finding that the ESI is what it purports to be.

F. Self-Authentication

Most online content is not self-authenticating. Precedent holds that the authentication of Internet printouts requires a witness declaration in combination with a document’s circumstantial indicia of authenticity (i.e., the date and web address that appear on them) to support a reasonable juror in the belief that the documents are what the declarant says they are. Without either, authentication fails.

- Sometimes (not always) Facebook profiles can be self-authenticating.
 - In *People v. Valdez*, 201 Cal. App. 4th 1429, 1434-37, 135 Cal. Rptr. 3d 628, 630 (Cal. Ct. App. 2011), a police expert printed copies of the defendant’s profile on a social media website that contained photographs of and biographical information about the defendant. The expert went on to explain that although the profile is

¹⁵¹ See FED. R. EVID. 403.

¹⁵² See *Trail v. Lesko*, No. GD-10-017249, 2012 Pa. Dist. & Cty. Dec. (C.P. July 3, 2012); see also Kathleen Pulver, *Social Media Posts as Evidence*, U. RICH. J. L. & TECH. BLOG (Jan. 18, 2017), <http://jolt.richmond.edu/2017/01/18/social-media-posts-as-evidence/>.

¹⁵³ *Griffin v. State*, 19 A.3d 415 (Md. 2011).

¹⁵⁴ *Tienda v. State*, 358 S.W.3d 633 (Tex. Crim. App. 2012)

accessible to the public, only the individual who created the profile, or one who has access to that person’s login ID and password, has the ability to upload or manipulate content on the page. As a result, the court held that a reasonable trier of fact could conclude from the information posted—including personal photographs, communications, and other details—that the social media profile belonged to the defendant.

PRACTICE TIP: A lawyer can ask specific questions to make authentication easier, such as making sure user admits to using the platform/account/device in question and admits to posting the content.

G. Hearsay Rules/How to Introduce ESI

Most social media posts that will be relevant in the cyber sexual abuse context are admissible under various evidentiary rules in the Federal Rules of Evidence (double-check your jurisdiction).

- Some posts may not be hearsay at all as they are a party admission or a prior inconsistent statement.¹⁵⁵
- Others may fall under a hearsay exception such as a present sense impression, an excited utterance, a then-existing condition, or a recorded recollection,¹⁵⁶ or if the creator of the post is unavailable to testify.¹⁵⁷
- Social media posts can also be used as evidence for or against credibility and not for the truth of the matter asserted, and therefore avoid hearsay issues.¹⁵⁸
- ESI may also become relevant with regard to character evidence;¹⁵⁹ however, they may not be used solely to show bad character.¹⁶⁰

The Best Evidence Rule is commonly misunderstood and should not be a significant issue for using ESI (FRE 1001-1008).¹⁶¹ The BER solely means that evidence should be provided

¹⁵⁵ See FED. R. EVID. 801.

¹⁵⁶ See FED. R. EVID. 803.

¹⁵⁷ See FED. R. EVID. 804.

¹⁵⁸ See FED. R. EVID. 806.

¹⁵⁹ See FED. R. EVID. 404, *see also* FED. R. EVID. 405.

¹⁶⁰ *Quagliarello v. Dewees*, 86 Fed. R. Evid. Serv. (Callaghan) 21 (E.D. Pa. 2011) (holding photographs from social networking sites inadmissible when offered solely to prove bad character).

¹⁶¹ See FED. R. EVID. 1001-1008.

directly, i.e., that a social media post should be introduced itself rather than just be discussed by a declarant.

- Duplicates are not prohibited under the BER (FRE 1003);¹⁶² instead they are admissible to the same extent as an original (unless questions are raised about its authenticity; etc.). Therefore printouts of ESI are admissible so long as they meet the other applicable standards.
 - *United States v. Nobrega*, No. 1:10-CR-00186-JAW, 2011 WL 2116991, at *5–6, 2011 U.S. Dist. LEXIS 55271, at *20–21 (D. Me. May 23, 2011), held that a printout of an instant message chat was admissible as a duplicate under Rule 1003.

For further information, see this helpful practicum from the American Bar Association: Josh Gilliland, *iWitness: The Admissibility of Social Media Evidence*, AM. BAR ASS'N (May 26, 2017).¹⁶³

¹⁶² See also FED. R. EVID. 1003.

¹⁶³ Available at https://www.americanbar.org/groups/litigation/publications/litigation_journal/2012_13/winter/the_admissibility_social_media_evidence/.

PART 5 - COPYRIGHTING AND REMOVING IMAGES AND VIDEOS FROM THE WEB

I. Understanding the Process

A. Background and Initial Considerations

To obtain a copyright under the federal Copyright Act of 1976 (“Copyright Act”), 17 U.S.C. § 101, a person must demonstrate that they produced an “original work[] of authorship fixed in any tangible medium.”¹⁶⁴ Therefore, the Copyright Act only offers copyright protection to the author of an image, such as the photographer or videographer, rather than the subject of the image.¹⁶⁵ Where a “selfie” is at issue and thus the author of the image becomes a victim of cyber sexual abuse,¹⁶⁶ the victim could have the benefit of the copyright.

In addition, the Copyright Act recognizes that where a work is “prepared by two or more authors with the intention that their contributions be merged into inseparable or interdependent parts of a unitary *whole*,” the work becomes a “joint work” with two or more authors.¹⁶⁷ Given this language, a sex tape that is knowingly made by the victim and the abuser could qualify for copyright protection in favor of the victim.

While a theoretical copyright attaches at the moment of creation (or “fixation” in the parlance of the Copyright Act), it is necessary to register the copyright with the United States Copyright Office in order to have a viable copyright infringement claim. Courts often look to the “expert opinion” of the Copyright Office for support.¹⁶⁸

B. Registering a Copyright with the Copyright Office

Copyright registration is not a prerequisite to obtaining copyright protection or exercising rights as a copyright owner, but copyright registration is a prerequisite for the pursuit of a copyright infringement action.

To register a copyrighted work with the Copyright Office, one must submit a registration application either by mail or online. Online registration is recommended as it has a lower filing

¹⁶⁴ 17 U.S.C. § 102(a).

¹⁶⁵ See, e.g., *Garcia v. Google, Inc.*, 786 F.3d 733, 744 (9th Cir. 2015) (en banc) (holding that an actress in a work was not the author of the work for purposes of a copyright claim)

¹⁶⁶ This scenario could play out in a number of ways: the victim and the abuser may have once been in a relationship wherein the victim shared an intimate image or video with the abuser consensually; the abuser may have coerced the victim into taking and sharing an intimate image or video; the abuser may have hacked into the victim’s phone or computer to retrieve the intimate image or video.

¹⁶⁷ 17 U.S.C. § 101 (emphasis added).

¹⁶⁸ *Garcia.*, 786 F.3d at 741.

fee and faster processing time, and there are status tracking capabilities. In addition, where the copyrighted work is a video or an image, it is easier to upload the work to the electronic Copyright Office (“eCO,” see <https://www.copyright.gov/registration/>) than mailing it.

Registration requires the following:

- Application Form;
- Filing Fee (usually under \$100)
- Deposit (i.e., a copy of the work being registered must be “deposited” with the Copyright Office. Deposit copies are retained by the Copyright office and not returned).

Registration comes with numerous benefits (see below) and is therefore highly recommended. The process of registration takes several months, but some courts have allowed applications for copyright registration as opposed to actual registration to suffice in copyright infringement claims.¹⁶⁹

PRACTICE TIP: In cases of cyber sexual abuse involving the disclosure of intimate images, verify with your client who the author of the image is. If your client is the author or is a “joint” author, consider registering the copyright as soon as possible. If the client is not the author and neither is the abuser (e.g., if the image was taken by a third party and the abuser somehow got hold of it), check if your client is willing to coordinate with the third-party author to register the copyright.

C. Benefits of Registration

Registration is recommended for a number of reasons. Copyright registration ensures that the facts of a copyright are on the public record, and the Copyright Office provides a certificate of registration, which is often required by the court in a copyright infringement case. In addition, to be eligible for statutory damages and attorneys’ fees in a copyright infringement case, the copyrighted work must be registered before infringement commences, with limited exceptions. Actual damages in an infringement suit may be either nominal or difficult to prove so having the ability to claim statutory damages is extremely significant and may even determine whether it makes sense to sue in the first place. Finally, if registration occurs within five years of publication, it is considered *prima facie* evidence in a court of law of the validity of the copyright and of the facts stated in the registration certificate.

¹⁶⁹ Note that this so-called “Application Rule” is not applied universally or consistently. In fact, the Copyright Alliance believes this rule is entirely inconsistent with the law and legislative history. See *Must a creator have a physical Certificate of Registration to bring a lawsuit in federal court?*, COPYRIGHT ALLIANCE (2019) https://copyrightalliance.org/ca_faq_post/must-a-creator-have-a-physical-certificate-of-registration-to-bring-a-lawsuit-in-federal-court/.

Potential concerns

In order to register a copyright, the victim must provide a copy of the “work” to be copyrighted to the Copyright Office, meaning that in cases of cyber sexual abuse, often times the victim will be providing the very image that caused offense and trauma in the first place. Many victims are justifiably concerned about further spreading an image they have worked hard to remove from the Internet. However, the U.S. Copyright Office has stated that “only the person processing the [copyright] application would see the pictures” requested to be copyrighted.¹⁷⁰ Many victims have successfully utilized copyright to combat cyber sexual abuse as websites and servers are often quick to remove copyrighted material from their sites.¹⁷¹

D. DMCA; DMCA Complaints and Takedown Notices

Section 512 of the Digital Millennium Copyright Act (“DMCA”), 17 U.S.C. § 101 *et seq.*, outlines requirements for a copyright holder to file a takedown notice with a website or computer service hosting (the “ISP”).¹⁷²

A takedown notice should be served on the designated agent of the ISP and include the following:

- (i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.
- (ii) Identification of the copyrighted work claimed to have been infringed or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.
- (iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.
- (iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and an electronic mail address at which the complaining party may be contacted.

¹⁷⁰ Erica Fink, *To fight revenge porn, I had to copyright my breasts*, CNN BUSINESS (Apr. 27, 2015, 1:32 PM) <https://money.cnn.com/2015/04/26/technology/copyright-boobs-revenge-porn/index.html>.

¹⁷¹ Amanda Levendowski, Note, *Using Copyright to Combat Revenge Porn*, 3 N.Y.U. J. INTELL. PROP. & ENT. L. 422 (2014), https://jipel.law.nyu.edu/wp-content/uploads/2015/05/NYU_JIPEL_Vol-3-No-2_6_Levendowski_RevengePorn.pdf.

¹⁷² 17 U.S.C. § 512. Some websites (including Google) provide DMCA complaint forms, but there is no guarantee they will be responsive to such complaints. See Gabrielle Fonrouge, *Google has a history of failing to remove revenge porn: lawyers*, NY POST (June 21, 2018, 5:20 PM), <https://nypost.com/2018/06/21/google-has-history-of-failing-to-remove-revenge-porn-lawyers/>.

- (v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.
- (vi) A statement that the information in the notification is accurate and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.¹⁷³

In construing the DMCA, courts have recognized that a party demanding a takedown “faces liability if [he or she] knowingly misrepresented in the takedown notification . . . a good faith belief the video was not authorized by the law, i.e., did not constitute fair use.”¹⁷⁴ Accordingly, it is important that the party demanding the takedown actually have lawful authority as (or from) the copyright owner.

DMCA also requires ISPs to include the contact details of its designated agent “on its website in a location accessible to the public” and to provide such details to the Copyright Office.¹⁷⁵ Thus, to the extent the information cannot be found on the ISP’s website, a victim may request it from the Copyright Office.

E. Takedowns and Subpoenas

DMCA permits a copyright owner or person authorized to act on the owner’s behalf to request a subpoena from the clerk of any U.S. District Court to be issued to any ISP hosting infringing material in order to identify the alleged infringer.¹⁷⁶

The subpoena request should include:

- A copy of the takedown notice,
- a proposed subpoena, and
- a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under title 17 of the U.S.C.

¹⁷³ 17 U.S.C. § 512.

¹⁷⁴ *Lenz v. Universal Music Corp.*, 815 F.3d 1145, 1154 (9th Cir. 2016), *cert. denied*, 137 S. Ct. 416 (2016), and *cert. denied*, 137 S. Ct. 2263 (2017); 17 U.S.C. § 512(f).

¹⁷⁵ 17 U.S.C. § 512(c)(2).

¹⁷⁶ 17 U.S.C. § 512(h). *Recording Indus. Ass’n of Am., Inc. v. Verizon Internet Services, Inc.*, 351 F.3d 1229, 1233 (D.C. Cir. 2003) (“subpoena may be issued only to an ISP engaged in storing on its servers material that is infringing or the subject of infringing activity”).

F. De-Indexing from Google

It is possible for Google to either temporarily or permanently remove sites from its index and cache of Internet search results;¹⁷⁷ the process is known as “de-indexing.” In theory, de-indexing is a useful tool for addressing cyber sexual abuse issues, for example where an abuser posts intimate images or personal information of a victim on a website. In practice, however, de-indexing can be difficult to achieve.

Google has published various policies which set out its approach to de-indexing. In summary, Google:

- *will* de-index where the content in question includes information required to be removed by law (“Legal Removals”); and
- *may* de-index where the content in question includes either personal information (“Personal Information Removals”) or unwanted and explicit personal images (“Personal Images Removals”).

In all cases, to initiate the de-indexing process the complainant, or an authorized representative of the complainant, must complete the relevant online Google request form. The applicable form varies depending on the nature of the content at issue.¹⁷⁸

1. *Legal Removals*

Under its Legal Removals policy,¹⁷⁹ Google states that it “*will*” de-index where a website includes:

- Child sexual abuse imagery; or
- Other content, if in response to a valid legal request, such as copyright takedown notices meeting the requirements of the Digital Millennium Copyright Act.

Accordingly, a victim of cyber sexual abuse that involves the disclosure of intimate images or videos can have Google de-index the relevant webpages upon request if the victim owns the copyright in that content. Relevantly, and as discussed earlier in this section, the victim may hold

¹⁷⁷ See *Site removed from the Google Index*, Help Center, GOOGLE, <https://support.google.com/webmasters/answer/40052?hl=en>.

¹⁷⁸ The Google removal requests forms and webpages can be located at the following URLs:

Removing Content from Google, <https://support.google.com/legal/troubleshooter/1114905?rd=1#ts=1115655>.

Removing Information from Google, <https://support.google.com/websearch/troubleshooter/3111061#ts=2889054%2C2889099%2C2889064%2C3143868%2C6256340>.

¹⁷⁹ *Removal policies*, Help Center, GOOGLE, <https://support.google.com/websearch/answer/2744324>.

that copyright either as a result of taking the picture or video, or by subsequently acquiring copyright under a written agreement.

2. *Personal Information Removals*

Under its Personal Information Removals policy,¹⁸⁰ Google states that it “*may*” (rather than “*will*”) de-list content containing “certain types of sensitive personal information.” Google’s policy further states that the kind of information it may remove includes:

- National identification numbers (such as social security, tax identification, foreign resident registration or identity numbers);
- Bank account or credit card numbers;
- Images of people’s signatures;
- Nude or sexually explicit images uploaded or shared without consent; and
- Confidential, personal medical records.

However, Google’s policy also expressly states that Google does not ordinarily de-list information such as dates of birth, addresses, telephone numbers or any other personal data that is publicly available on government websites. Further, Google will look to the following factors, on a case-by-case basis, to determine whether any particular piece of personal information is sufficiently sensitive to justify de-listing:

- Is the information a government-issued identification number?
- Is the information confidential, or is it publicly available?
- Can the information be used for common financial transactions?
- Can the information be used to obtain more information about an individual that would result in financial harm or identity theft?
- Is the information a personally identifiable nude or sexually explicit photo or video shared without consent?

In short, victims of cyber sexual abuse (which involves the disclosure of highly sensitive personal information likely to result in identity theft or other harm) could seek to have the relevant website de-indexed via a request to Google. That said, under the policy, the decision whether to de-index in any given case ultimately remains at Google’s absolute discretion.

¹⁸⁰ *Id.*

3. *Personal Image Removal*

In response to growing public concerns about cyber sexual abuse and “revenge porn,” Google introduced a dedicated “Unwanted and Explicit Personal Images” policy in 2015.¹⁸¹ Under that policy, Google states that it will remove intimate images, but only under certain circumstances that meet its requirements. More specifically, Google asserts that it removes personal images where the complainant:

- is featured personally; and
- is nude or shown in a sexual act; and
- intended the content to be private and the imagery was made publicly available without their consent (the policy expressly refers to “revenge porn” as a specific example); or
- did not consent to the act and the imagery was made publicly available without their consent.

Google can prevent a page from appearing in its search results, but it cannot remove content from websites that host it. Google, therefore, recommends that victims first contact the webmaster for the offending site to request removal. Google’s website provides complainants with guidance on how to identify and contact the applicable webmaster.¹⁸²

If a complainant wishes to proceed with a Google removal request, the policy requires them to provide the following personal information via its dedicated request form:

- Full name;
- Country;
- Contact e-mail address;
- URL for where the content is live, if applicable;
- A sample URL of Google search results where the image or video appears; and
- Screenshots of the offending content (with the sexually explicit portions obscured using image-editing software.)

In short, a victim of cyber sexual abuse can seek to have abusive content or websites de-indexed under Google’s “Unwanted and Explicit Personal Images” policy. However, to do so, the

¹⁸¹ *Remove unwanted & explicit personal images from Google*, Help Center, GOOGLE, <https://support.google.com/websearch/answer/6302812?hl=en>. See also, “*Revenge porn*” and *Search*, Google Public Policy Blog, GOOGLE, <https://publicpolicy.googleblog.com/2015/06/revenge-porn-and-search.html>.

¹⁸² *Contact a site’s webmaster*, Help Center, GOOGLE, <https://support.google.com/websearch/answer/9109>.

victim must satisfy Google’s specific conditions for removal, and even then, Google retains discretion regarding whether or not to de-index in any given case.

G. Impact of Court Orders

While it may be possible for victims of cyber sexual abuse to obtain Family Court orders requiring an abuser to remove content from a website,¹⁸³ those orders are not binding on third parties to the proceeding, such as webmasters, ISPs, Google, or other search engines.¹⁸⁴ In addition, such companies traditionally enjoy immunity from liability for cyber sexual abuse taking place on their platforms due to the CDA Section 230 exemption discussed *supra* in this Manual.¹⁸⁵

The newly passed New York State cyber sexual abuse law (*see supra* Part 1- Criminal Legal Remedies for Victims of CSA, Section I.A.) contains a provision allowing a victim to seek a court order of removal from a website hosting or transmitting a cyber sexual abuse image of the victim. However, as this law has yet to be signed into law as the time of writing this Manual, there is not yet information available as to the effectiveness of this provision.

Recent case law suggests it may be possible to hold Internet companies accountable for their conduct where they play an active, primary role in curating and promoting offending “third-party” content.¹⁸⁶ Given the broad CDA immunity, however, you should not count on legal actions to force websites to take images down or otherwise impose liability on websites.

¹⁸³ See Part 5 - Copyrighting and Removing Images and Videos from the Web, Sections I.F-G of the Manual.

¹⁸⁴ See, e.g., *Hassell v. Bird*, 420 P.3d 776 (Cal. 2018).

¹⁸⁵ See Part 5 - Copyrighting and Removing Images and Videos from the Web, Sections I.F-G of the Manual.

¹⁸⁶ *FTC v LeadClick Media LLC*, 838 F.3d 158 (2d Cir, 2016).

PART 6 - TECHNOLOGY SAFETY PLANNING AND BEST PRACTICES

If you are working with a client who has already been a victim of cyber sexual abuse and/or technology abuse, or expresses fear that his or her abuser may use technology against them, use this section to guide your client through technology best practices.

While working through safety planning with your client, it is critical to consider the safety implications of removing or limiting the abuser's access to their technology. If the abuser realizes that they have been "caught" and/or no longer has access to information about your client, this may escalate the abuse. Always do technology safety planning in the context of a comprehensive safety plan. If you need assistance working with your client to create a comprehensive safety plan, consult Part 7- Resources of this Manual for referrals.

This section will start by covering some general technology and online safety tips that can apply to all digital media, as well as some preventive measures. It will then go on to discuss certain media, devices, or accounts in more specific detail.

I. General Safety Tips: The "Digital Breakup Plan"

If your client is considering leaving an abusive relationship, there are things he or she can do ahead of time to try to mitigate the damage that his or her abuser can do with technology. Use this list as a starting point for your client's "digital breakup plan":

- Change all passwords on all accounts to secure, unique ones that cannot be guessed by the abuser. Help your client try to remember every account that they may have online, including e-mail, social media, "cloud" storage, school, banking, and even shopping accounts (which may have stored credit card and address information).¹⁸⁷
- Do not set passwords as children's names, important dates, or other personal things that might be easy for someone who knows your client to guess. The most secure passwords are those that contain only random strings of letters, numbers, and symbols.
- Along the same lines, do not use answers to password-reset security questions that the abuser knows. Give fake answers to security questions, or better yet, use random strings of letters, numbers and symbols as these answers as well.
- Do not use the same password for every account; if the abuser manages to get the password for one account (e.g., through keystroke logging), then they will have access to all your client's accounts. Many people use the same password on all their accounts because it is too hard to remember so many different random and unique passwords. Instead, a free online password manager allows you to create one secure, unique

¹⁸⁷ For guidance through common online accounts, see *Coach: Crash Override's Automated Cybersecurity Helper*, CRASH OVERRIDE, <http://www.crashoverridenetwork.com/coach.html> (last accessed Mar. 21, 2019).

password to log into the manager, and then the manager creates and saves random passwords for every other site.¹⁸⁸

- Turn on two-factor authentication for every website and account that offers it, especially the password manager. Two-factor authentication (2FA) requires both a password and a one-use code sent to a cell phone or other device to log in. Using 2FA means that someone can only log into your client’s account if they have physical access to their cell phone. If 2FA is available on an account, it is usually turned on through the settings tab. Ensure that the phone the codes will be sent to is a safe one that the abuser does not have physical access to.
- Enable firewalls and install antivirus and anti-spyware software on all devices.
- Have your client’s computers and electronic devices analyzed for spyware. There might be spyware installed on your client’s device if it is behaving strangely — e.g., running slowly, draining the battery too quickly, crashes more often — or if the abuser seems to know information about the client that they should not know. This manual contains some information about detecting spyware, *see supra* Part 6-Technology Safety Planning. Your client can also take the computers/devices to a professional to have them analyzed.
- Have your client search their belongings for GPS tracking devices (e.g., car, purse). They can also ask law enforcement for help. Have your client search their home, or ask law enforcement to search their home, for hidden cameras, particularly in areas that the abuser has had physical access to, or objects in the home that were gifts from the abuser to the client or family members. Note that “camera detectors” are effective in detecting wireless cameras, but not those that are hardwired.

Of course, tech tips alone will not keep your client’s information safe, if the abuser has access to non-digital sources of information. Brainstorm with your client about how else their abuser may be able to get information or monitor their activities. Does the abuser have access to the client’s home? Mail? Workplace? Do they have children or mutual friends who may share information?

II. Securing Cell Phones and Tablets

Cell phones (and tablets with Wi-Fi or data plans) are a very common source for an abuser to collect all sorts of information about your client, including their location, their communications, and their photos and videos. Spyware installed on the device is one way for an abuser to secretly monitor your client, but even without spyware, your client’s cell phone can broadcast a lot of dangerous information about them.

¹⁸⁸ LastPass is a helpful free online password manager, <https://www.lastpass.com/>. LastPass also allows your client to store their fake answers to security questions, as discussed above.

- Put a passcode on the phone, so that even if the abuser has physical access to the phone, they cannot open it up to access the information.
- Turn off automatic login and/or saved passwords, so that if someone has access to the phone, they cannot log into online accounts with sensitive information.
- Turn off location sharing and Bluetooth when not in use.
- Go through the phone's privacy settings: both the general privacy settings, as well as the individual settings for all installed apps.
- Review the apps that are installed on the phone, and delete any unfamiliar ones.
- Check if the abuser has access to the client's phone account (e.g., on their family plan). Consider removing the abuser from the plan, or change the password to the account.
- Be aware if your client's phone is acting strangely, which may indicate spyware or other malicious tracking software:
 - Running slowly, getting hot, battery draining;
 - Spikes in data usage;
 - Takes longer to shut down;
 - Screen lights up when not in use;
 - Clicks or sounds on calls;
 - Incoming calls on bills that user did not receive.
- If malware or spyware is discovered, be careful about transferring content to a new phone, which will also transfer all the malicious content.

For iPhones specifically:

- Enable Touch ID or a passcode.
- Check your client's iCloud and Apple ID, change the passwords, and delete any e-mail addresses that your client does not want to have access to the account.
- Consider turning off the setting to automatically back up photos, mail, contacts, etc. to iCloud.
- Turn off the "Find my Phone" feature, which allows someone to find the location of the phone by logging into iCloud.

- Turn off Family Sharing, or turn off the feature that shares the phone’s location with family members.
- Turn off Location Services for any apps that are not currently being used.
- Set up the privacy settings of individual apps to control what information on the phone each app can access.
- Be very cautious about “jailbreaking” the phone, which will remove important security features that prevent malware and spyware.¹⁸⁹

III. Computers, E-mail, and Online Browsing

If your client uses a desktop or laptop computer (which may be easier or harder than a phone for the abuser to have physical access to, depending on their living situation), there are additional safety steps to discuss with your client.

As computers are more likely to be shared by multiple family members than phones or tablets, especially if the parties live together, it is critical to weigh every safety step against the possibility that limiting the abuser’s access to the computer and/or wireless network will tip the abuser off that the client is preparing to leave the relationship, and may be more dangerous than leaving the computer alone. If the abuser has physical access to your client’s computer, and/or is on a shared network with your client, and it is unsafe to limit this access, your client may wish to consider using a safer device, such as a library computer, for any communications and/or web browsing that they wish to keep private.

If it is safe for your client to take precautions on the computer, follow these safety tips:

- As discussed in Section I above, change all online passwords and enable 2FA. Enable a password lock on the computer itself, and remove the abuser’s login profile from the computer.
- Password-protect the wireless network, and remove any of the abuser’s devices as authorized devices on the network.
- Enable firewalls, install anti-spyware/anti-virus software, and always keep the software up-to-date.¹⁹⁰
- When reading e-mail, do not open attachments from unknown senders. When browsing, do not visit unknown websites or click on unknown links.

¹⁸⁹ For more detailed iPhone safety tips, see *iPhone Privacy & Security Guide*, Technology Safety, NATIONAL NETWORK TO END DOMESTIC VIOLENCE, <https://www.techsafety.org/iphoneguide/>.

¹⁹⁰ A reputable and free antivirus program for both PC and Mac is Avast, www.avast.com.

- Turn off cookies in the browser settings, and regularly delete cookies and search history. Many browsers also offer “private” or “incognito” browsing which does not record the browsing history and deletes cookies after the browsing session is closed.
- If your client’s abuser seems to know too much about your client’s computer activity, then there is a possibility that the computer has been compromised, for example by “keylogging” software, which records all the keystrokes that are made to that computer. With an active and fully updated antivirus program running, it is harder for keyloggers to be installed, but if your client suspects one and has a PC:
 - Open the Task Manager and check the Task Manager window for suspicious programs running; search the names of unknown processes on the Internet to see if they might be malicious.
 - In the Start menu search bar, type in “msconfig” and press enter. Go to “Startup”, and see if there are any suspicious programs that are configured to start up when the computer boots. If a program looks suspicious, search for its name on the Internet to see if it might be malicious.
 - The program may be able to be uninstalled just like any regular program using the Control Panel. Once uninstalled, run a scan with antivirus software to ensure that it is completely gone. However, if the keylogger is very malicious, regular uninstallation may not work. Your client can consult with an IT or help desk professional for assistance in removing the keylogger, or it may require the operating system to be completely reinstalled.
 - If it is a desktop computer, look at where the keyboard cable connects to the tower. If there is a device plugged in between the keyboard cable and the tower, it might be a hardware keylogger.

IV. Social Media Accounts

Social media is a goldmine of information that your client may be inadvertently sharing with their abuser. Descriptions of specific social media sites and the ways they can be used are discussed more in-depth earlier in this Manual, *supra* Part 3- Description of Relevant Social Media/Applications and Associated Abuse. In general, your client should take certain precautions on all their social media sites (in addition to changing all their passwords and enabling 2FA):

- Turn off location services.
- Check all privacy settings. Set up notifications to get a message if someone tags, messages, or comments on your client’s posts. Set up a notification to let your client know whenever someone has logged into their account.
- Be careful about “checking in” to locations, as this will allow the abuser to track your client’s location.

- Beware of “geotags” on photos, which is hidden data that records the GPS location of where the photo was taken. Sharing that photo on social media may expose your client’s location even if they do not explicitly “check in” somewhere.
 - On an iPhone, you can turn off geotags in Settings/Privacy/Location Services/Camera. To remove geotags from photos already taken, use a photo privacy app from the App Store.
- Do not link social media accounts with e-mail accounts.

The victim may wish to block or unfriend their abuser. Their counsel should discuss with them whether this is safer or whether it will trigger the abuser to retaliate. It also means that the victim will no longer be able to see what the abuser is sharing about them, which may make it harder to react. In addition, their counsel may lose access to evidence that you may need for a current or future legal case. If the victim decides to block or unfriend the abuser, counsel should consider whether there are ways to preserve the evidence beforehand.

V. Credit Cards and ID Theft

This Manual does not focus on identity-theft issues. However, identity theft is definitely a tactic that a digital abuser may use, so we have included a few tips for instances where your client fears that their abuser has their Social Security number or may try to steal their identity and open fraudulent accounts. You can begin by having your client run a credit report on all three of the credit reporting agencies (Experian, Equifax, and Transunion). Everyone has the right to get one free credit report from each of these agencies once a year, for a total of three free credit reports a year.

A victim should use www.annualcreditreport.com to request their free credit report. There are other websites that purport to be free, but many of them require a trial account to be opened, or for “credit monitoring services” to be purchased.

Be aware that running a credit report using a confidential address may then make that address become part of the credit report, and if an abuser can access the credit report, the abuser will then have the confidential address. Instruct your client to use a prior, known address to run the report, or have them register for a confidential address if that is offered in your state (it is offered in New York).

If any of the credit reports show fraudulent activity, your client should:

- Call the fraud department of all their accounts, report the fraud, and follow the directions given by the service rep. This may include closing the accounts, getting new cards, changing passwords and PINs, etc.
- Contact each of the credit reporting agencies to put a “fraud alert” on their file.

- Report the ID theft to FTC and local police; share the police report with the credit reporting agencies.¹⁹¹

VI. Nonconsensual Pornography: Images and Videos

Discuss with your client whether he or she is aware of any intimate images or videos of themselves that their abuser may use to threaten, extort, or harm them. Your client may have shared intimate images voluntarily during the relationship. However, his or her abuser could also have obtained private photos or videos without your client’s knowledge or consent. Images can be captured through hidden cameras, by recording or screenshots through Skype or another video chat, or by accessing your client’s photos, either from the physical device where they are saved, or from “cloud” storage. If you are counseling a client who reveals that they are considering sharing intimate photos with a partner, you could suggest that your client take precautions, such as avoiding showing any identifying features (e.g., face, tattoos, birthmarks), using a neutral non-identifying background with dark lighting, or adding a filter to the photo.

By following the general safety steps outlined above, your client may be able to prevent their abuser from obtaining intimate images. However, if your client knows that the abuser already has intimate images, there are a few steps that may help prevent the abuser disseminating these images, or at least alert your client quickly if the images have been shared, so that they can take swift action.

- Have your client do a Google search, and then set up a Google news alert, for their name, so that they get an e-mail whenever a new hit is found.
- Facebook has launched a program in which people can voluntarily share the intimate images that they fear might be disseminated, and Facebook then converts those images to a digital code to prevent someone else from uploading and posting the photo. Discuss with your client whether this is something they are comfortable doing. This project is discussed more in-depth at <https://www.techsafety.org/blog/2018/7/10/facebooks-proactive-approach-to-addressing-nonconsensual-distribution-of-intimate-images>.
- Discuss with your client their legal options if the images do become public, including how to preserve the evidence for later legal action. Legal remedies against the abuser are covered in [Part 1- Criminal Legal Remedies for Victims of CSA](#) and [Part 2- Civil Legal Remedies for Victims of CSA](#) and evidence collection and preservation is discussed in [Part 4- Evidence Collection](#) of this Manual.

VII. Detecting Spyware

Spyware is any computer program or hardware that enables an unauthorized person to monitor communications, location, and other data, often without detection. Dozens of programs

¹⁹¹ The FTC has a comprehensive document called “Identity Theft, a recovery plan” that covers the steps to take in more detail. *IdentityTheft.gov*, FEDERAL TRADE COMM’N, <https://www.identitytheft.gov/>.

and applications exist that allow users to track another person's whereabouts, take photos, record ambient audio, and remotely wipe or lock the device.¹⁹²

Spyware is difficult to detect and remove because it is often hidden. The abuser may be able to download spyware secretly and obscure its presence on a phone or computer. In addition, there are several "dual-use" applications that are "designed for legitimate purposes, such as anti-theft tracking apps, 'Find My Friends,' emergency response apps, parental control apps, and others," but that can be used to commit intimate partner violence.¹⁹³

Preventing spyware from being downloaded can be difficult. Many apps have functionality to hide their icons from a phone's screen. Be wary of phones that have been "jailbroken" or "unlocked," as this removes security features that prevent spyware from being downloaded. Educate your children and family members so they do not inadvertently install spyware.

While there is no sure way of detecting spyware, the following are things clients should look out for. Law enforcement and advocates can help if spyware is believed to have been downloaded.

- Be aware if your phone or computer:
 - is running slowly;
 - is getting hot;
 - has a quick-draining battery;
 - has spikes in data usage;
 - takes longer to shut down;
 - lights up while not in use;
 - clicks or has odd sounds while on calls;
 - has any new or suspicious hardware, like a keyboard, cord, or USB drive; or
 - has incoming or outgoing calls that you do not recognize.
- Be aware if your abuser knows things that you've only told people via e-mail, text message, or phone calls (ex: your whereabouts, your search history, etc.)

¹⁹² RAHUL CHATTERJEE ET AL., *The Spyware Used in Intimate Partner Violence* 9 (2018), <https://www.ipvtechresearch.org/pubs/spyware.pdf>.

¹⁹³ DIANA FREED ET AL., "A Stalker's Paradise": *How Intimate Partner Abusers Exploit Technology* 6-7 (2018), <http://www.nixdell.com/papers/stalkers-paradise-intimate.pdf>.

Individuals should be careful about looking for and removing spyware because it could be dangerous to alert the abuser of your suspicion. Use a computer or phone at work, a public library, a community center, an Internet café, or a friend or family member's computer to perform searches or send e-mails to avoid detection by the abuser. Continue to use your device for innocuous tasks, like checking the weather, so your partner does not get suspicious.

Removing spyware is challenging. The only sure way to remove spyware is to discard the device and get a new one. Short of this, wiping the device to its original factory settings is often effective. It is suggested that clients back up their device before resetting it, as this can be helpful to law enforcement personnel to have a record of the device's activity. It is important *not* to download the contents of the backup to a new or recently wiped device, as the spyware could reinstall itself.

Enabling firewalls and installing an anti-spyware/antivirus software, and keeping the software up-to-date, can help detect and remove spyware, but even the best anti-spyware software is not always effective. A reputable and free antivirus program for both PC and Mac is Avast (www.avast.com). Clearing your browser history and deleting cookies will not remove spyware.

PART 7 - RESOURCES

A. Directory of Useful Websites

- <http://www.crashoverridenetwork.com> – Crash Override is a crisis helpline, advocacy group and resource center for victims of online abuse.
- <https://www.techsafety.org/> - This website is run by the National Network to End Domestic Violence and includes a number of helpful safety toolkits for survivors of technology abuse as well as advocates.
- <https://hackblossom.org/domestic-violence/>- An online scenario and strategy guide for domestic violence victims of technology abuse.
- <https://www.cybercivilrights.org/victim-resources/> - The Cyber Civil Rights Initiative provides emotional support, technical advice, and information to current victims of online abuse. This link is a list of resources available for victims.
- <https://www.cybercivilrights.org/online-removal/> - The Cyber Civil Rights Initiative provides emotional support, technical advice, and information to current victims of online abuse. This link is a guide to requesting removal of cyber sexual abuse content found online.
- <https://rcjlawgroup.com/2013/02/12/helpful-tips-for-victims-of-revenge-porn/> - Helpful tips and overview of resources for victims of cyber sexual abuse.
- <https://copyrightalliance.org/education/copyright-law-explained/> - Overview of copyright law.
- <https://www.copyright.gov/help/faq/faq-general.html> - General FAQ regarding copyright laws.
- <https://www.identitytheft.gov/> - Federal Trade Commission website with guide on how to address and respond to identity theft, available at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.
- <https://inteltechniques.com/data/workbook.pdf> - A helpful personal data removal workbook tool and credit freeze guide for survivors interested in eliminating personal online information and data from the Internet.

B. Directory of Service Organizations

Organization	Mission and Services	Contact Information
Access Now	24/7 Digital Security Helpline; free	E-mail: help@accessnow.org https://www.accessnow.org/help/
Covenant House	Provides housing and supportive services to youth facing homelessness.	https://www.covenanthouse.org/
Cyber Civil Rights Initiative (National Hotline)	Free, confidential support available 24/7 for victims of cyber sexual abuse	Call: 844-878-2274 https://www.cybercivilrights.org/ccri-crisis-helpline/
Cyber Civil Rights Initiative	Pro bono legal assistance	https://www.cybercivilrights.org/professionals-helping-victims/
Day One	Day One partners with youth to end dating abuse and domestic violence through community education, supportive services, legal advocacy, and leadership development.	Toll-free hotline: 800-214-4150 Text line – 646-535-DAY1 (3291) https://www.dayoneny.org/
DMCA Defender	Reputation management and DMCA takedown specialists	http://dmcadefender.com/
Her Justice	Her Justice is a nonprofit organization that provides free legal help to women living in poverty in New York City.	You can call the live Legal Help Line and speak with a legal professional at 718.562.8181 on Thursdays from 10AM to 1PM. https://herjustice.org/
K&L Gates Cyber Civil Rights Legal Project.	Pro bono legal services to victims of revenge porn	Go to http://www.cyberrightsproject.com/ for more information and to fill out a contact form
Legal Momentum	Legal Momentum is a long-time leader in advancing the rights of women and girls. We secure equality and opportunity for women and girls with targeted litigation, innovative policy advocacy, and education.	https://www.legalmomentum.org/ Helpline request form available at: https://www.legalmomentum.org/get-help-form

Legal Services NYC	Legal Services NYC fights poverty and seeks racial, social, and economic justice for low income New Yorkers.	Call 917-661-4500 for the Legal Assistance Hotline, Monday through Friday from 10 a.m. to 4 p.m. https://www.legalservicesnyc.org/
LIFT – Legal Information for Families Today	The mission of Legal Information for Families Today is to enhance access to justice for children and families by providing legal information, community education, and compassionate guidance, while promoting system-wide reform of the courts and public agencies.	Call 212-343-1122 https://www.liftonline.org/
National Domestic Violence Hotline	24/7 hotline; provides connections to local domestic violence agencies	Call: 1-800-799-7233 www.thehotline.org
NYLAG	NYLAG provides free civil legal services to New Yorkers who cannot afford a private attorney.	For family or matrimonial issues, including domestic violence, call 212-613-5000 on Tuesdays between 9 a.m. and 5 p.m. https://www.nylag.org/
Operation Safe Escape	Organization of security professionals assisting victims of domestic violence with escaping and remaining free of abusive relationships.	https://goaskrose.com
RAINN	24/7 hotline; provides connections to local sexual violence agencies	Call: 1-800-656-HOPE (4673) www.rainn.org .

<p>Sanctuary for Families</p>	<p>Sanctuary for Families provides resources and advocacy for survivors of domestic violence, sex trafficking, and related forms of gender violence. Sanctuary provides holistic services for survivors of gender-based violence, including legal assistance and representation, counseling and crisis intervention, shelter, economic empowerment services, children and family programs, anti-trafficking advocacy, trainings, and other programming.</p>	<p>Call 212-349-6009 extension 221 to reach the Sanctuary helpline, Monday through Friday , 9 a.m. to 5 p.m.</p> <p>To request legal services, please call 212-349-6009 extension 246 and leave a voicemail message.</p> <p>www.sanctuaryforfamilies.org</p>
<p>Safe Horizon</p>	<p>24/7 hotline; provides support with crisis counseling, safety planning, assistance finding a shelter, information about resources. Assistance available in any language.</p>	<p>www.safehorizon.org</p> <p>For help with domestic violence, call: 1-800-621-HOPE (4673)</p> <p>For help with all crimes, call 866-689-HELP (4357)</p> <p>For help with rape and sexual assault, call 212-227-3000</p> <p>For hearing impaired clients, call TDD line at 866-604-5350</p>
<p>Urban Justice Center</p>	<p>The Urban Justice Center serves New York City's most vulnerable residents through a combination of direct legal service, systemic advocacy, community education and political organizing.</p>	<p>www.urbanjusticecenter.org</p> <p>Call the intake line 718-875-5062 on M, W, Fri (9am-5pm).</p> <p>For domestic violence services, visit www.dvp.urabnjustice.org</p>
<p>Without My Consent</p>	<p>Without My Consent is a non-profit organization seeking to combat online invasions of privacy.</p>	<p>http://www.withoutmyconsent.org/</p>

PART 8 - APPENDICES

APPENDIX	DOCUMENT
A.	10 Tips for Protecting Your Data and Privacy in the Age of Cyber Technology
B.	Evidence Preservation – Saving Websites as PDFs
C.	Family Court memorandum supporting the inclusion of cyber sexual abuse language on Orders of Protection
D.	Family Offense Petitions alleging cyber sexual abuse
E.	Family Court Orders of Protection including provisions prohibiting cyber sexual abuse

Appendix A - 10 Tips for Protecting Your Data and Privacy in the Age of Cyber Technology

1. Sign out of all accounts when using computers, cell phones, and other devices, especially public and shared devices.
2. Avoid using the same password for multiple accounts and change your password regularly.
3. Make sure you select a complex password that friends and family cannot guess. Use a mix of numbers, symbols, and uppercase and lowercase letters. This makes it harder for hackers to gain access to your data.
4. Be cautious when using unsecured networks. Unsecured networks put your data at greater exposure because they are typically open to the public and lack strong firewalls.
5. Enable notifications for suspicious activities, such as when your account is accessed on a new device and in a new location. Review instructions on how to add these notifications.
6. Enable dual-factor authentication, which requires you to verify your login through a unique link or code that is typically sent to a second device or to your e-mail. It takes a few extra moments, but it will help prevent unwanted access.
7. On your mobile device, review the access permissions that you grant applications (such as permission to view your location, photos, camera, and contacts) and update accordingly.
8. Regularly empty the trash folders on your accounts.
9. Limit who can view the content of your online profiles by making your profile “private” or by adjusting the website’s default settings to align viewership permissions to your preference.
10. Before signing up for an account, familiarize yourself with the website’s process for having content posted by or about you removed from the website.

Appendix B- Evidence Preservation – Saving Websites as PDFs

1. On a computer: Different internet browsers will include different mechanisms for converting web pages into PDFs.
 - On Google Chrome:
 - **Step 1:** Open the Settings menu by clicking the three-dot icon in the top right-hand corner and choose “Print.” This will bring you a printing window.
 - **Step 2:** In the printing window, look for the heading “Destination” and choose “Change.” This will bring you to a “Select a Destination Under Local Destinations.” you should see an option to “Save as PDF.” Select it. That will load a preview of the pages and allow you to select pages, change the layout, and soon.
 - **Step 3:** Once you have made the changes that you need, select “Save.”
 - On Safari:
 - **Step 1:** Start on the web page you want to save. Head up to “File” and choose “Print,” or press “Command” and “P” to open the printer window.
 - **Step 2:** Got to the lower left-hand corner of the window where it says “PDF,” and select this drop-down menu. Here you will see a number of options to save the PDF, save it into the cloud, save it as an instant message, open it in Preview before deciding to save, and so on. For a basic save, select “Save as PDF.” Otherwise, choose the option that best fits your needs.
 - **Step 3:** Name your file and location, and select “Save.”
 - On Firefox:
 - **Step 1:** Click the menu icon in the top right-hand corner.
 - **Step 2:** Click “Print” from the drop down menu.
 - **Step 3:** Click “Print” in the top left-hand corner.
 - **Step 4:** In the resulting window, select “Microsoft Print to PDF” from the printer options. Hit OK when ready.
 - **Step 5:** Choose a name and save location and hit the “Save” button.
 - On Internet Explorer:
 - Open the Internet Explorer menu by clicking/tapping the gear icon at the top right or hitting Alt+X.
 - Navigate to File > Save as... or enter the Ctrl+S keyboard shortcut.
 - Choose an appropriate “Save as type.” from the bottom of the Save Webpage window.
2. On an iPhone:
 - **Step 1:** Open the webpage you want to save in Safari.
 - **Step 2:** Tap the Action button (the square button with the upward-facing arrow).

- Step 3: Tap the “Save PDF to iBooks” button in the top row.
 - Note: If you’re a Dropbox user, you could also tap the “Save to Dropbox” option under the Action button. This will save webpages as PDFs to your Dropbox account.
- 3. On an Android:
 - Step 1: Open the page you want to save in Google Chrome.
 - Step 2: Tap the three-dot menu button in the top-right corner of the screen.
 - Step 3: Tap “Share,” then tap “Print.”
 - Step 4: Once Android has finished creating a preview of the page you want to save, tap the “Save to drop-down” menu at the top of the page.
 - Step 5: Select “Save to Google Drive” to upload a PDF of the page to your Drive account or tap “Save as PDF” to save the file to your phone’s local storage.
 - Step 6: To find the file later, either go to your Google Drive or go to “Downloads” in the app drawer on your Android.

Appendix C – Family Court memorandum supporting the inclusion of cyber sexual abuse language on Orders of Protection



Sample Cyber Sexual Abuse Memorandum

Sanctuary for Families

Center for Battered Women's Legal Services

30 Wall Street, 8th Floor

New York, NY 10005

(212) 349-6009

FAMILY COURT OF THE STATE OF NEW YORK
COUNTY OF X

----- X
In the Matter of an Article 8 Proceeding :
 :
A.B. :
 : File No. 123456
 Petitioner, :
 v. : Docket No. O-00001-16
 :
C.D :
 :
 Respondent.
----- X

PETITIONER’S MEMORANDUM OF LAW AND REQUEST FOR RELIEF

On March 23, 2016, Petitioner A.B. filed a Family Offense Petition in X County Family Court, alleging that Respondent C.D. committed several family offenses against her and praying for relief. *See* Exhibit 1 (Petitioner’s Family Offense Petition filed March 23, 2016). Following a brief hearing before Referee Y, Referee Y entered a Temporary Order of Protection against Respondent. *See* Exhibit 2 (Petitioner’s Temporary Order of Protection issued March 23, 2016). The Temporary Order of Protection ordered the Respondent to stay away from Petitioner and Petitioner’s home, school, business, and place of employment; to “refrain from communication or any other contact by mail, telephone, e-mail, voice-mail or other electronic or any other means with [Petitioner]”; and to “refrain from [listed family offenses] or any criminal offense against [Petitioner].” *Id.* at 1.

In addition to this relief, Petitioner requested that the Court order the Respondent to “[r]efrain from using pet[itioner]’s likeness and/or intellectual property on any social media outlets [and] [r]efrain from social media harassment and sexual humiliation online.” Exhibit 1. Referee Y reserved judgment as to whether this relief would be granted and ordered Petitioner,

with the assistance of law students from the Courtroom Advocate Project, to file a Memorandum of Law addressing whether the Court has the power to grant the requested relief.

Pursuant to Referee Y's request, the Petitioner hereby submits this Memorandum of Law and Request for Relief. Because the Court does possess the power to grant the requested relief, Petitioner respectfully requests that the Court grant all of the relief prayed for in her Petition. Specifically, Petitioner requests the inclusion of the following language on her Temporary Order of Protection:

“The Respondent is not to post or transmit or cause a third party to post or transmit, any images, pictures, video, or other media, depicting the Petitioner in a naked state, depicting the Petitioner’s intimate parts, or depicting Petitioner participating in any sexual act OR threaten to do the same”

Date: April 30, 2016

Lindsey Marie Song, Esq.
Sanctuary for Families, Inc.
Center for Battered Women’s Legal
Services
Attorneys for Petitioner
30 Wall Street, 8th Floor
New York, NY 10005
(212) 349-6009 ext. 330

Contributions by:

James G. Mandilk
Yale Law School '17

Megan C. McGuiggan
SUNY Buffalo School of Law '17

STATEMENT OF THE CASE

Petitioner A.B. and Respondent C.D. entered into a dating relationship in approximately June 2013. Petitioner ended their dating relationship in early February 2016, and Respondent immediately commenced a pattern of harassing and threatening communication towards Petitioner, despite Petitioner's requests for this communication to cease. Specifically, Respondent "has been relentless with his attempts to contact her through text, e-mail, calls and social media." Exhibit 1, at 2. Respondent has threatened to hurt and kill Petitioner and "to 'make sure [she] never did this to another person again.'" *Id.* at 1. In mid-March, his attempts increased in frequency, with Respondent "attempting to contact [P]etitioner through various channels, including calling and e-mailing her job, at []least 40 times daily." *Id.* In conjunction with these unrelenting attempts to contact her, Respondent threatened to, and then did, send video and pictures to Petitioner's work email depicting Petitioner naked and engaging in sexual activity. *See id.* at 1-2. Respondent then "threatened to send the video directly to her employer, jeopardizing her current job and her career." *Id.* at 2. Petitioner did not know that Respondent had this video of her, and upon seeing it and receiving his threat, she became very frightened. *Id.* Given that Respondent previously carried out his threat to send the files to her work email—and in light of the broader pattern of harassing and threatening behavior exhibited by his excessive attempts to communicate with Petitioner—she reasonably "fears that Resp[ondent] will carry out his threats" to disseminate naked photographs and video of her. *Id.*

Disseminating sexually explicit images of a past romantic partner is a serious, and increasingly prevalent, method of domestic violence colloquially referred to as "revenge porn." *See generally* Emily Poole, *Fighting Back Against Non-Consensual Pornography*, 49 U.S.F. L. Rev. 181 (2015); *see also* Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 Wake Forest L. Rev. 345 (2014). Once an image is posted online by an abuser, the

image can quickly spread to many websites; it is then exceedingly difficult to remove all copies of the offending image. This attempt to continue to exert control over an ex-lover through humiliation has been explicitly criminalized by some state legislatures. Susan L. Pollett, *Revenge Porn: Will Legislation Help To Prevent It?*, N.Y. L.J. (Apr. 28, 2016) (“[Eighteen] states . . . passed criminal legislation between 2013 and 2015 to address [revenge porn].”). Although New York State currently has no law directly criminalizing all revenge porn, posting revenge porn arguably violates broader criminal prohibitions on harassment and stalking.

Based on this societal trend and Respondent’s explicit threats, Petitioner has a reasonable fear that Respondent will post sexually explicit images of her, causing irreparable reputational harm. Because “the Family Court has the authority to impose reasonable conditions when they are likely to be helpful in eradicating the root of family disturbance,” *Miriam M. v. Warren M.*, 859 N.Y.S.2d 66, 67-68 (1st Dept. 2008), this Court can and should order the Respondent to refrain from disseminating sexually explicit media (photos, video, or other forms of media) of the Petitioner.

SUMMARY OF ARGUMENT

Before requesting this Memorandum, Referee Y expressed concern that disseminating sexually explicit media of Petitioner might not be a crime in New York and, therefore, that even if Respondent disseminated such images it would not be a family offense. However, the Court may enter an Order of Protection ordering Respondent to refrain from disseminating sexually explicit media regardless of whether disseminating sexually explicit media is classified as a family offense under the Family Court Act. While it is true that the Court must find the existence of at least one family offense before it may enter an Order of Protection, Petitioner has alleged acts by Respondent—including threats of violence—that rise to the level of family offenses. Because Petitioner has made a prima facie case that family offenses have been committed by

Respondent, this Court may enter an Order of Protection throughout the pendency of this matter. In that Order, the Family Court is not limited to proscribing conduct that is a family offense.

The Court may enter an Order of Protection that includes provisions ordering Respondent to “refrain from harassing, intimidating or threatening” conduct. N.Y. Family Ct. Act 842(c). It may also require Respondent “to observe such other conditions as are necessary to further the purposes of protection.” N.Y. Family Ct. Act 842(k); *see also* N.Y. Comp. Codes R. & Regs. tit. 22, § 205.74(c)(6) (“An order of protection entered in accordance with section 841(d) of the Family Court Act may, in addition to the terms and conditions enumerated in sections 842 and 842-a of the Family Court Act, require the petitioner, respondent or both . . . to: . . . comply with such other reasonable terms and conditions as the court may deem necessary and appropriate to ameliorate the acts or omissions which gave rise to the filing of the petition.”) *Miriam M. v. Warren M.*, 859 N.Y.S.2d 66, 67-68 (2008) (“The Family Court has the authority to impose reasonable conditions when they are likely to be helpful in eradicating the root of family disturbance”). In Petitioner’s case, Respondent has engaged in a pattern of behavior that includes threats to terrorize and humiliate Petitioner by sending sexual images of Petitioner to her employer, including images taken without Petitioner’s consent. Under the Section 842(c) and 842(k), this Court has the power to enter an Order of Protection ordering Respondent not to send such images; indeed, judges in fellow New York Family Courts have entered similar orders. Regardless of whether disseminating sexually explicit media is a family offense, therefore, this Court can and should grant the requested relief.

Furthermore, on the facts of this case, disseminating sexually explicit media depicting Petitioner would be a family offense. New York stalking laws—specifically, “Stalking in the Fourth Degree”—proscribe a person from engaging in a course of conduct that serves no

legitimate purpose and is intended to harm and intimidate the victim. N.Y. Penal Law § 120.45(2) (McKinney 2012). While the course of conduct must be aimed at harming the victim directly, such conduct includes communications made to third parties that are likely to cause the victim emotional or physical harm. *See id.* Here, Respondent began exhibiting threatening behaviors and engaging in a course of conduct intended to intimidate and harass Petitioner beginning in February 2016. In addition to threatening to harm Petitioner, relentlessly contacting her at work and home, and sending sexually explicit images of Petitioner to her work email account, Respondent has also threatened to send the same images to Petitioner's supervisor and colleagues. Because Respondent's doing so would be a continuation of his threatening and emotionally harmful course of conduct that is barred by state law, this Court can specifically order Respondent not to disseminate revenge porn depicting Petitioner to any third parties.

I. THIS COURT HAS THE POWER TO ORDER THE REQUESTED RELIEF EVEN IF DISSEMINATING SEXUALLY EXPLICIT MEDIA IS NOT CURRENTLY CATEGORIZED AS A FAMILY OFFENSE.

In the case at bar, Referee Y found good cause to believe—and Petitioner will prove at a fact-finding hearing, should this matter proceed to fact-finding—that the Respondent committed several family offenses. These include, but are not limited to, stalking in the fourth degree and harassment in the second degree, based on Respondent’s threats to hurt and/or kill Petitioner. *See* Exhibit 1, at 1. Because Petitioner has made a prima facie case that Respondent committed these family offenses against her, the Court may issue an Order of Protection pursuant to Section 841(d) of the Family Court Act. The operative question, then, is not whether disseminating sexually explicit photos of the Petitioner is a family offense; rather, it is whether the Court may impose the remedy sought by the Petitioner. As previously noted by the Third Department, “[t]he major criterion of the reasonableness of conditions imposed is whether they are likely to be helpful in eradicating the root of family disturbance.” *Leffingwell v. Leffingwell*, 448 N.Y.S.2d 799, 800 (3rd Dept. 1982); *accord Miriam M. v. Warren M.*, 859 N.Y.S.2d 66, 67-68 (1st Dept. 2008). In line with this broad mandate, New York Family Courts have ordered respondents not to disseminate revenge porn in the past. *See, e.g.*, Final Order of Protection issued Fall 2015 in New York County Family Court including the language, “The Respondent is not to post or transmit or cause a third party to post or transmit, any images or pictures depicting the Petitioner in a naked state.” (Weinstein, J.).

The Court’s power to fashion relief is outlined in Section 842 of the Family Court Act, which allows this Court to require the Respondent to obey “reasonable conditions of behavior.” Section 842 provides at least two avenues for ordering the relief Petitioner requests: Section 842(c) and 842(k). Section 842(c) allows the Court to order that the Respondent “refrain from

committing a family offense . . . or any criminal offense . . . , *or from harassing, intimidating or threatening* [a member of the same family or household].”¹ Every phrase in a statute should be given meaning. *See, e.g., Jane Y. v. Joseph Y.*, 474 N.Y.S.2d 681, 683 (Fam. Ct. 1984) (“In the construction of a statute, meaning and effect should be given to all its language, if possible, and words are not to be rejected as superfluous when it is practicable to give each a distinct and separate meaning.”) (citing McKinney's Consolidated Laws of New York, Book 1, Statutes, § 231). If “harassing, intimidating or threatening” were limited to family offenses under the Family Court Act and/or criminal offenses under the New York Penal Code, then “harassing, intimidating or threatening” would be a superfluous phrase because both family offenses and crimes are independently enumerated. Therefore, Section 842(c) should be read to proscribe conduct that is “harassing, intimidating or threatening” that is not specifically included under family offenses or criminal offenses. This reading is supported by the legislature’s intent that Orders of Protection proceedings are intended “for the purpose of attempting to stop the violence, end the family disruption and obtain protection.” N.Y. Fam. Ct. Act § 812 (McKinney).

In the instant matter, if Respondent sent sexually explicit depictions of Petitioner to Petitioner’s coworkers and/or supervisor, that would constitute the continuation of a pattern of “harassing, intimidating or threatening” behavior. Respondent has threatened to hurt and/or kill Petitioner. He has contacted her many times—by phone, text, social media, and in person—despite her repeated requests that he stop. He sent sexually explicit images of Petitioner,

¹ The section as drafted is limited to a “criminal offense against the child or against the other parent or against any person to whom custody of the child is awarded, or from harassing, intimidating or threatening such persons,” but this language is broadened later in the same section: “Notwithstanding the foregoing provisions, an order of protection, or temporary order of protection where applicable, may be entered against . . . a member of the same family or household as defined in subdivision one of section eight hundred twelve.” N.Y. Fam. Ct. Act § 842 (McKinney). Section 812(1) includes as “members of the same family or household” persons who “have been in an intimate relationship regardless of whether such persons have lived together at any time.” *Id.* § 812(1)(e) (McKinney). As the Petitioner and Respondent were in an intimate relationship from approximately June 2013 through February 2016, the Petitioner and Respondent are, therefore, “members of the same family or household.”

including a video that was taken without her knowledge or consent, to her work email. In light of this history, if Respondent were to carry out his threat, even if disseminating the images would not constitute a family offense under the Family Court Act or a penal offense under the New York Penal Code, it would be “harassing, intimidating or threatening.” Therefore, Section 842(c) of the Family Court Act gives this Court power to order the Respondent not to carry out his threat.

In addition to its broad power to prohibit “harassing, intimidating or threatening” conduct under 842(c), the Court is also empowered to require the Respondent “to observe such other conditions as are necessary to further the purposes of protection.” N.Y. Fam. Ct. Act § 842(k) (McKinney). This additional relief can require the Respondent to “comply with such other reasonable terms and conditions as the court may deem necessary and appropriate to ameliorate the acts or omissions which gave rise to the filing of the petition.” N.Y. Comp. Codes R. & Regs. tit. 22, § 205.74(c)(6).

The First Department has held that it is error to refuse to grant reasonable relief under this clause if the relief is “likely to be helpful in eradicating the root of the family disturbance,” even if the misconduct alleged is not itself a family offense. In *Miriam M.*, the facts before the Family Court established that the Respondent had committed family offenses against the Petitioner (his sister) and that he had also hit the Petitioner’s domestic partner. *Miriam M.*, 859 N.Y.S.2d 66 (1st Dept. 2008). The First Department held that although the Petitioner’s domestic partner “d[id] not fall within the statutory definition of ‘member[] of the same family or household’” and therefore Respondent’s actions could not constitute a family offense, the Family Court was empowered to “impose reasonable conditions where they are ‘likely to be helpful in eradicating the root of family disturbance.’” *See id.* at 581-82 (citing *Matter of Leffingwell v. Leffingwell*,

448 N.Y.S.2d 799 (1982)). The First Department therefore modified the family court order to include a provision ordering the respondent to stay away from the petitioner's domestic partner and the domestic partner's place of employment. *See Miriam M.*, 859 N.Y.S.2d at 67 (1st Dept. 2008).

Section 842(k) has allowed New York family courts to grant Orders of Protection with a variety of conditions that are not directly targeted at family offenses, but instead are intended to "further the purposes of protection" of the Petitioner. N.Y. Fam. Ct. Act § 842(k) (McKinney). The Third Department in one instance affirmed the following portions of an Order: "[that the Respondent] (a) refrain from any violent, offensive conduct towards the petitioner; (b) refrain from consumption of alcoholic beverages in the marital residence; (c) refrain from entering the home in an intoxicated state; [...]; and (e) vacate his home." *Leffingwell v. Leffingwell*, 448 N.Y.S.2d 799, 800 (1982). Additionally, other New York family courts have granted Orders of Protection prohibiting conduct very similar to that at issue in this case. *See, e.g.*, Final Order of Protection issued Fall 2015 in New York County Family Court including the language, "The Respondent is not to post or transmit or cause a third party to post or transmit, any images or pictures depicting the Petitioner in a naked state." (Weinstein, J.).

As these cases illustrate, Order of Protection remedies are not limited to prohibitions against family and criminal offenses. Petitioner's fear that Respondent will disseminate naked photos and video of her without her consent is at "the root of the family disturbance." *Matter of Miriam M.* at 67-68. Therefore, to "further the purposes of protection" of the Petitioner, this Court can and should grant the requested relief under 842(k) or the "harassing, intimidating or threatening" provision of 842(c).

II. IN THIS CASE, DISSEMINATING SEXUALLY EXPLICIT PHOTOGRAPHS TO PETITIONER’S THIRD PARTY ACQUAINTANCES IS A FAMILY OFFENSE.

This Court can grant protective order relief even when the proscribed misconduct is not a family offense. *See supra* I. But even if the Court requires that *all* conduct proscribed by a protective order be a family offense, granting Petitioner’s requested relief—that the Court order Respondent not to disseminate sexually explicit media of Petitioner without her consent—is still appropriate under the facts here.

While New York State has not yet adopted a specific “revenge porn” statute, state courts have prosecuted “revenge porn” under other headings, such as stalking, harassment, coercion, unlawful surveillance, copyright infringement, and invasion of privacy. *See* N.Y. Penal Law § 135.60 (coercion); N.Y. Penal Law § 250.45 (unlawful surveillance); Alaska Stat. § 11.61.210 (harassment); *see also* Danielle Citron, *How to Make Revenge Porn a Crime Without Trampling Free Speech* (Slate, Nov. 7, 2013) (explaining that while many existing criminal laws do not address revenge porn, harassment laws apply when the defendant engages in a harassing course of conduct).² While revenge-porn-specific legislation would help ensure that New York victims receive adequate protection, such legislation is not required to prosecute this conduct. *See* Susan L. Pollet, *Revenge Porn: Will Legislation Help to Prevent It?*, N.Y. L. J. (Apr. 28 2016) (explaining that while victims have sued under tort and copyright theories, New York’s proposed law specifically criminalizing revenge porn would have a more substantial deterrent effect); Citron & Franks, *Criminalizing Revenge Porn*, 49 Wake Forest L. Rev. at 367 (suggesting that

² Available at http://www.slate.com/articles/news_and_politics/jurisprudence/2013/11/making_revenge_porn_a_crime_without_trampling_free_speech.html.

disseminating revenge porn can be “criminal harassment” when abuse is persistent); *see also* Eric Goldman, *California’s New Law Shows It’s Not Easy to Regulate Revenge Porn*, *Forbes* (Oct. 8, 2013).³

In the instant case, Respondent has repeatedly threatened to send sexually explicit media of the Petitioner third parties. *See* Exhibit 1. To avoid further harm to Petitioner, the Court can and should order Respondent not to do so. First, if Respondent carries out this threat, his actions would become a “course of conduct” designed to intimidate and harm Petitioner, and would therefore be illegal under New York stalking laws. *See* N.Y. Penal Law § 120.45(2)-(3) (McKinney 2012). Because stalking is a family and criminal offense, the Court can specifically order Respondent not to engage in a course of conduct that includes disseminating these images to third parties. Second, because Respondent’s threats to disseminate these images serve no legitimate purpose other than to harass and intimidate Petitioner, it is irrelevant that Respondent may have obtained some of the images lawfully.

A. THE COURT CAN ORDER RESPONDENT NOT TO DISSEMINATE SEXUALLY EXPLICIT IMAGES OF PETITIONER BECAUSE THIS CONDUCT WOULD BE STALKING IN THE FOURTH DEGREE.

First, Respondent’s sending sexually explicit photographs to Petitioner’s employer or colleagues—in conjunction with his other threatening conduct—constitutes the family offense of stalking in the fourth degree. *See* N.Y. Penal Law § 120.45. Under this provision, a person is

³ *Available at* www.forbes.com/sites/ericgoldman/2013/10/08/californias-new-law-shows-its-not-easy-to-regulate-revenge-porn/ (“[O]ther laws already apply to other involuntary porn categories. For example, hacking into someone’s computer or cellphone is already illegal; if the victim made the recording him/herself, copyright law protects it; and if the parties had confidentiality expectations, privacy doctrines may apply. Anti-stalking and anti-harassments laws can also apply to involuntary porn, especially where a defendant distributes recordings to hurt the victim. Indeed, we have so many laws and crimes already on the books, it’s challenging to find any examples of in civil or anti-social behavior that isn’t already illegal under multiple overlapping laws.”)

guilty of stalking when he intentionally and for no legitimate purpose, engages in a “course of conduct” directed at a person that he knows or reasonably show know “causes material harm to the mental or emotional health of such person, where such conduct consists of following, telephoning, initiating communication . . . with such person . . . or a third party with whom such person is acquainted.” *See id.* § 120.45(2) (emphasis added). For purposes of the statute, a “course of conduct [is] a pattern of conduct composed of a series of acts over a period of time, however short, evidencing a continuity of purpose.” *People v. Payton*, 161 Misc.2d 170 (Kings Cnty. Crim. Ct. 1994). While the “course of conduct” must be directed at harming the victim, such conduct can include harmful communications made to third parties. *See* N.Y. Penal Law § 120.45(2).

Here, if Respondent carries out his threat to disseminate these images to Petitioner’s employer, his actions would be part of Respondent’s continuing course of conduct intended to harass Petitioner. Starting around February 15, 2016, Respondent began threatening to harm or kill Petitioner, repeatedly contacting Petitioner at her home and at work, sending sexually explicit images to Petitioner’s work email, and informing Petitioner that he recorded a sexually explicit video without her consent. *See* Exhibit 1. On March 7, 2016, Respondent specifically threatened to sexually humiliate Petitioner by sending the images to Petitioner’s third party acquaintances—particularly to her boss or colleagues—and Petitioner understandably fears that Respondent’s doing so would harm her career and professional reputation. *See* Exhibit 1. Petitioner became fearful that Respondent would follow through with his threat, which prompted her to file a Family Offense Petition in Kings County Family Court three days later. *See id.*

Respondent’s threatening behavior has remained consistent for nearly two months, and if Respondent were to send sexually explicit media of Petitioner to Petitioner’s third party

acquaintances, his doing so would be a continuation of the harmful conduct that began on February 15, 2016 and is therefore barred by Section 120.45(2). Moreover, while Respondent has not yet sent these images to a third party, he is likely to follow through with his threats to do so, given that Respondent previously threatened to send sexually explicit images of Petitioner to her work email account, and did so shortly after. *See* Exhibit 1. Upon information and belief, Respondent also tampered with these images to appear as though he had shared them publicly, causing Petitioner to fear that he had shared the images with her acquaintances. Given that Respondent has carried out previous threats towards Petitioner, the requested relief is particularly appropriate here.

Finally, forbidding Respondent from disseminating these images is wholly consistent with the policy underlying other New York stalking provisions, including Section 120.45(3), which proscribes certain conduct that “is likely to cause such person to reasonably fear that his or her employment, business or career is threatened.” In this case, Petitioner fears that Respondent will irreversibly damage her career and professional reputation by disseminating these images. Exhibit 1. As Respondent’s actions in threatening Petitioner’s career and sending sexually explicit media depicting Petitioner to third parties fall within a “course of conduct” proscribed by New York stalking laws, the Court can and should grant Petitioner’s requested relief.

B. RESPONDENT’S THREAT TO DISSEMINATE SEXUALLY EXPLICIT MEDIA IS DESIGNED TO INTIMIDATE PETITIONER AND SERVES NO LEGITIMATE PURPOSE.

Finally, while outlawing revenge porn has raised First Amendment concerns, disseminating sexually explicit images—even when the images have been lawfully obtained with the victim’s consent—is still proscribed by New York stalking laws. Indeed, state courts have

found that “while constitutionally protected activity has been specifically excluded in some anti-stalking statutes, New York’s statute is broader. . . [t]hus, seemingly constitutional behavior, if it is made part of a ‘course of conduct’ with the requisite scienter . . . will violate New York’s anti-stalking statute.” *Payton*, 161 Misc.2d at 174. It matters not whether a person has obtained the images lawfully or with the victim’s consent, but whether disseminating the images serves *no legitimate purpose*. See N.Y. Penal Law § 120.45 (emphasis added). Conduct serves no legitimate purpose when it lacks “expression of ideas or thoughts other than threats and/or intimidating or coercive utterances.” *People v. Shack*, 86 N.Y.2d 529, 538 (1995). Therefore, Section 120.45 covers all communications in which the respondent lacks a legitimate “reason or excuse” for engaging the other party, “other than to hound, frighten, intimidate, or threaten” the victim. *People v. Stuart*, 100 N.Y.2d 412, 428 (affirming defendant’s stalking conviction when he failed “to show that his intrusive behavior involved some valid purpose other than hounding [complainant] to the point of harm”).

Here, Respondent can offer no explanation as to why he has threatened to disseminate these images other than to harm, intimidate, or sexually humiliate Petitioner. At least one video Respondent has threatened to distribute was obtained without Petitioner’s knowledge or consent, in violation of New York’s unlawful surveillance statute.⁴ A video obtained in contravention of state law can serve no lawful, legitimate purpose. See N.Y. Penal Law § 250.45(3)(b) (“when a person uses . . . an imaging device in a bedroom . . . there is a rebuttable presumption that such person did so for no legitimate purpose); *People v. Piznarski*, 113 A.D.3d 166, 177 (3rd Dept.

⁴ “A person is guilty of unlawful surveillance in the second degree when . . . for the purpose of degrading or abusing a person, he [] intentionally uses or installs, or permits the utilization or installation of an imaging device to surreptitiously view, broadcast, or record a person dressing or undressing or the sexual or other intimate parts of such person at a place and time when such person has a reasonable expectation of privacy, without such person’s knowledge or consent.” N.Y. Penal Law § 250.45 (McKinney 2012) (unlawful surveillance in the second degree).

2013) (finding no legitimate purpose for the defendant's "surreptitiously recording" a victim while the two were in a bedroom and engaged in a sexual act). Even if Respondent obtained some images lawfully or with Petitioner's consent, his secretly filming Petitioner and wide array of threatening behaviors shows Respondent's bad faith and lack of legitimate reason to distribute the images. Because Respondent's threats to publicize these images serve to frighten, intimidate, and embarrass Petitioner, there can be no legitimate purpose underlying this conduct.

CONCLUSION

Disseminating sexually explicit photos and video of Petitioner without her consent is arguably a family offense. Even if such behavior does not rise to the level of a family offense, such conduct can be prevented by the Court the interest of “further[ing] the purposes of protection” of the Petitioner. N.Y. Fam. Ct. Act § 842(k) (McKinney).” Therefore, this Court can and should grant the requested relief and, in all future Temporary or Final Orders of Protection, order Respondent to refrain from disseminating sexually explicit media of Petitioner.

Date: April 30, 2016

Lindsey Marie Song, Esq.
Sanctuary for Families, Inc.
Center for Battered Women’s Legal
Services
Attorneys for Petitioner
30 Wall Street, 8th Floor
New York, NY 10005
(212) 349-6009 ext. 330

Contributions by:

James G. Mandilk
Yale Law School ’17

Megan C. McGuiggan
SUNY Buffalo School of Law ’17

Appendix D- Family Offense Petitions alleging cyber sexual abuse



**Sample Family Offense Petition Alleging
Cyber Sexual Abuse**

Sanctuary for Families

Center for Battered Women's Legal Services

30 Wall Street, 8th Floor

New York, NY 10005

(212) 349-6009

**FAMILY COURT OF THE STATE OF NEW YORK
COUNTY OF *INSERT COUNTY***

----- x

Petitioner (DOB -----)

File No. 123456
Docket No. O-123456-17

Petitioner,

-against-

**AMENDED PETITION
Family Offense**

Respondent (DOB -----)

Respondent,

----- x

TO THE FAMILY COURT:

The undersigned Petitioner respectfully states that:

- 1. Petitioner resides at ADDRESS CONFIDENTIAL.
- 2. Respondent resides at 123 Cloud Lane, New York, NY 11111.

3. (Upon information and belief), the Respondent **who was in an intimate relationship with** the Petitioner, committed an act or acts, which constitute the following family offense(s) against Petitioner and/or her children: (disorderly conduct) (aggravated harassment in the second degree) (harassment in the first degree) (harassment in the second degree) (menacing in the second degree) (menacing in the third degree) (reckless endangerment) (assault in the second degree) (assault in the third degree) (attempted assault) (stalking in the first degree) (stalking in the second degree) (stalking in the third degree) (stalking in the fourth degree) (sexual misconduct) (forcible touching) (sexual abuse in the third degree) (sexual abuse in the second degree) (criminal obstruction of breathing or blood circulation) (strangulation in the second degree) (strangulation in the first degree) (identity theft in the third degree) (identity theft in the second degree) (identity theft in the first degree) (grand larceny in the fourth degree) (grand larceny in the third degree) (coercion in the second degree):

- a. On or about January 11, 2017, upon information and belief, Respondent hacked into Petitioner’s Snapchat account and sent naked photos and videos of Petitioner to her Snapchat contacts, without Petitioner’s knowledge or consent. Upon information and belief, the photos sent were photos that only Respondent had access to. Respondent sent this media through Snapchat following an incident on or about December 9, 2016, where Respondent texted Petitioner, in sum and substance, that he would distribute naked photos of her if she did not respond to him. Petitioner filed a police report regarding this incident. As a result of this incident, Petitioner feared for her safety and suffered annoyance and alarm.

- b. On or about January 8, 2017, Respondent texted words to the effect of, “ho” and “bitch.” When Petitioner told Respondent she would call the police, Respondent threatened to show a video of Petitioner naked in the shower to the police if she attempted to have him removed from the home. He said words to the effect of, “I will show [the police] how you get down.” Petitioner filed a police report regarding this incident. As a result of Respondent’s actions, Petitioner feared for her safety and suffered annoyance and alarm.
- c. On or about December 18, 2016, upon information and belief, Respondent texted Petitioner words to the effect of, “I miss you” and “remember this night.” Respondent sent Petitioner a photograph of Petitioner in a naked state along with these texts – a photo only Respondent had access to. As a result of this incident, Petitioner feared for her safety and suffered annoyance and alarm.
- d. On or about November 4, 2016, Respondent posted a video on Facebook Live and showed a photo of the Petitioner’s naked private body, specifically the side of her body from the breast to butt cheeks. The photo showed Petitioner’s tattoo on the left side of her back and buttocks. As a result of this incident, Petitioner feared for her safety and suffered annoyance and alarm.
- e. Throughout the parties’ relationship, from approximately February 2016 through the present, Respondent has engaged in a pattern of physically, verbally, and emotionally abusive behavior towards Petitioner. Upon information and belief, Respondent has naked images of Petitioner and Petitioner fears he will disseminate these images, as he has threatened to disseminate other images of Petitioner in the past. As a result of Respondent’s actions, Petitioner feared for her safety and suffered annoyance and alarm.

4. The following are the names, ages and relationships to the Petitioner and/or Respondent of each and every child in the family household:

<u>Name of child</u>	<u>Date of Birth</u>	<u>Relationship to Petitioner and/or Respondent</u>
----------------------	----------------------	---

Not applicable

5. Upon information and belief, the following aggravating circumstances, if any, are present in this case ["Aggravating circumstances" shall mean physical injury or serious physical injury to the Petitioner caused by the respondent, the use of a dangerous instrument against Petitioner by the Respondent, a history of repeated violations of Orders of Protection by the Respondent, prior convictions for crimes against the Petitioner by the Respondent or the exposure of any family or household member to physical injury by the Respondent and like

incidents, behavior and occurrences which constitute an immediate and ongoing danger to the Petitioner or any member of the Petitioner's family or household]:

Not applicable.

6. Upon information and belief, the following criminal, matrimonial or Family Court proceedings involving the Respondent have been filed:

Petitioner filed a police report regarding the incident that occurred on January 8, and January 11, 2017; the cases are currently pending.

7. Indicate whether a previous application has been made to any court or judge for the relief requested herein and, if so, the relief, if any, granted and the date of such relief:

This petition is an amended version of the petition Petitioner filed pro se on or about January 12, 2017, and for which a temporary Order of Protection was extended.

8. (Upon information and belief) Respondent is licensed or has a license application pending to carry, possess, repair, sell or otherwise dispose of the following firearms [if known, specify type of firearms, type of license(s), date of issuance of license(s) and expiration date(s), whether license has been suspended or revoked and, if so, the date of such action and, if not currently licensed, whether license application is pending]:

Not applicable.

9. (Upon information and belief) Respondent is in possession of the following licensed and unlicensed firearms [specify number and type of firearms and whether licensed or unlicensed, if known]:

Not applicable.

10. (Upon information and belief) There is a substantial risk that Respondent may use or threaten to use a firearm unlawfully against petitioner (and members of petitioner's family or household) for the following reasons:

Not applicable.

WHEREFORE, Petitioner prays

- (a) that the Respondent be adjudged to have committed the family offense(s) alleged;
- (b) that the Court enter an Order of Protection, specifying conditions of behavior to be observed by the Respondent in accordance with Section 842 of the Family Court Act:

- Respondent to STAY AWAY from Petitioner, Petitioner's home, Petitioner's school, and Petitioner's place of employment;
- Respondent to have NO CONTACT with Petitioner, by mail, telephone, e-mail, through other persons, or any other means, including third party contact;
- Respondent to refrain from assault, stalking, harassment, menacing, reckless endangerment, disorderly conduct, intimidation, threats, or any criminal offense against Petitioner;
- Respondent is not to post or transmit or cause a third party to post or transmit, any images, pictures, video, or other media, depicting the Petitioner in a naked state, depicting the Petitioner's intimate parts, or depicting Petitioner participating in any sexual act OR threaten to do the same;

and for such other and further relief as to the Court seems just and proper.

Dated: January 2017
 COUNTY, New York

PETITIONER

Sworn to before me on this
_____ day of January 2017

Notary Public

Appendix E - Family Court Orders of Protection including provisions prohibiting cyber sexual abuse



**Sample Orders of Protection addressing
Cyber Sexual Abuse**

Sanctuary for Families
Center for Battered Women's Legal Services
30 Wall Street, 8th Floor
New York, NY 10005
(212) 349-6009

ORI No: NY023023J

Order No: [REDACTED]

NYSID No: _____

At a term of the Family Court of the State of New York,
held in and for the County of Kings, at 330 Jay Street, Brooldyn, NY
11201, on August 25, 2016

PRESENT: [REDACTED] Court Attorney Referee

In the Matter of a FAMILY OFFENSE Proceeding

[REDACTED]
Petitioner

- against -

[REDACTED]
Respondent

File # [REDACTED]

Docket # [REDACTED]

Order of Protection

Both Parties Present in Court

NOTICE: YOUR FAILURE TO OBEY THIS ORDER MAY SUBJECT YOU TO MANDATORY ARREST AND CRIMINAL PROSECUTION, WHICH MAY RESULT IN YOUR INCARCERATION FOR UP TO SEVEN YEARS FOR CRIMINAL CONTEMPT, AND/OR MAY SUBJECT YOU TO FAMILY COURT PROSECUTION AND INCARCERATION FOR UP TO SIX MONTHS FOR CONTEMPT OF COURT.

THIS ORDER OF PROTECTION WILL REMAIN IN EFFECT EVEN IF THE PROTECTED PARTY HAS, OR CONSENTS TO HAVE, CONTACT OR COMMUNICATION WITH THE PARTY AGAINST WHOM THE ORDER IS ISSUED. THIS ORDER OF PROTECTION CAN ONLY BE MODIFIED OR TERMINATED BY THE COURT. THE PROTECTED PARTY CANNOT BE HELD TO VIOLATE THIS ORDER NOR BE ARRESTED FOR VIOLATING THIS ORDER.

A petition under Article 8 of the Family Court Act, having been filed on June 16, 2016 in this Court and On Consent, and [REDACTED] having been present in Court and advised of the issuance and contents of this Order.

NOW, THEREFORE, IT IS HEREBY ORDERED that [REDACTED] observe the following conditions of behavior:

[01] Stay away from:

[A] [REDACTED];

[B] the home of [REDACTED];

[E] the place of employment of [REDACTED];

[14] Refrain from communication or any other contact by mail, telephone, e-mail, voice-mail or other electronic or any other means with [REDACTED] No third party contact.;

[02] Refrain from assault, stalking, harassment, aggravated harassment, menacing, reckless endangerment, strangulation, criminal obstruction of breathing or circulation, disorderly conduct, criminal mischief, sexual abuse, sexual misconduct, forcible touching, intimidation, threats, identity theft, grand larceny, coercion or any criminal offense against [REDACTED].;

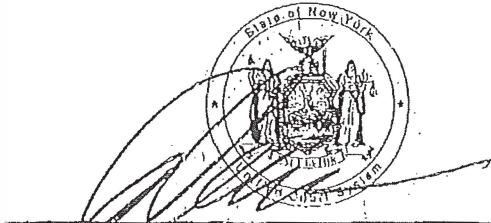
[99] Observe such other conditions as are necessary to further the purposes of protection: [REDACTED];

THE RESPONDENT SHALL REFRAIN FROM POSTING OR TRANSMITTING OR CAUSE A THIRD PARTY TO POST OR TRANSMIT MEDIA (IMAGES, PICTURES, AUDIO, VIDEO) DEPICTING THE PETITIONER.;

It is further ordered that this order of protection shall remain in force until and including June 24, 2017.

Dated: August 25, 2016

ENTER



Court Attorney Referee

PURSUANT TO SECTION 1113 OF THE FAMILY COURT ACT, AN APPEAL FROM THIS ORDER MUST BE TAKEN WITHIN 30 DAYS OF RECEIPT OF THE ORDER BY APPELLANT IN COURT, 35 DAYS FROM THE DATE OF MAILING OF THE ORDER TO APPELLANT BY THE CLERK OF COURT, OR 30 DAYS AFTER SERVICE BY A PARTY OR THE ATTORNEY FOR THE CHILD UPON THE APPELLANT, WHICHEVER IS EARLIEST.

The Family Court Act provides that presentation of a copy of this order of protection to any police officer or peace officer acting pursuant to his or her special duties authorizes, and sometimes requires such officer to arrest a person who is alleged to have violated its terms and to bring him or her before the court to face penalties authorized by law.

Federal law requires that this order is effective outside, as well as inside, New York State. It must be honored and enforced by state and tribal courts, including courts of a state, the District of Columbia, a commonwealth, territory or possession of the United States, if the person restrained by the order is an intimate partner of the protected party and has or will be afforded reasonable notice and opportunity to be heard in accordance with state law sufficient to protect due process rights (18 U.S.C §§ 2265, 2266).

It is a federal crime to:

- cross state lines to violate this order or to stalk, harass or commit domestic violence against an intimate partner or family member;
- buy, possess or transfer a handgun, rifle, shotgun or other firearm or ammunition while this Order remains in effect (Note: there is a limited exception for military or law enforcement officers but only while they are on duty); and
- buy, possess or transfer a handgun, rifle, shotgun or other firearm or ammunition after a conviction of a domestic violence-related crime involving the use or attempted use of physical force or a deadly weapon against an intimate partner or family member, even after this Order has expired (18 U.S.C. §§ 922(g)(8), 922(g)(9), 2261, 2261A, 2262).

Check Applicable Box(es):

Party against whom order was issued was advised in Court of issuance and contents of Order

Order personally served in Court upon party against whom order was issued

Service directed by other means[specify]: _____

[Modifications or extensions only]: Order mailed on [specify date and to whom mailed]: _____

Warrant issued for party against whom order was issued[specify date]: _____

ADDITIONAL SERVICE INFORMATION [specify]: _____

ORI No: NY030023J
Order No: [REDACTED]
NYSID No: _____

At a term of the Family Court of the State of New York,
held in and for the County of New York, at 60 Lafayette Street, New
York, NY 10013, on October 22, 2015

PRESENT: Honorable [REDACTED]
In the Matter of a FAMILY OFFENSE Proceeding

[REDACTED]
Petitioner,

- against -

[REDACTED]
Respondent.

File # [REDACTED]
Docket # [REDACTED]
Order of Protection

Both Parties Present in Court

NOTICE: YOUR FAILURE TO OBEY THIS ORDER MAY SUBJECT YOU TO MANDATORY ARREST AND CRIMINAL PROSECUTION, WHICH MAY RESULT IN YOUR INCARCERATION FOR UP TO SEVEN YEARS FOR CRIMINAL CONTEMPT, AND/OR MAY SUBJECT YOU TO FAMILY COURT PROSECUTION AND INCARCERATION FOR UP TO SIX MONTHS FOR CONTEMPT OF COURT.

THIS ORDER OF PROTECTION WILL REMAIN IN EFFECT EVEN IF THE PROTECTED PARTY HAS, OR CONSENTS TO HAVE, CONTACT OR COMMUNICATION WITH THE PARTY AGAINST WHOM THE ORDER IS ISSUED. THIS ORDER OF PROTECTION CAN ONLY BE MODIFIED OR TERMINATED BY THE COURT. THE PROTECTED PARTY CANNOT BE HELD TO VIOLATE THIS ORDER NOR BE ARRESTED FOR VIOLATING THIS ORDER.

A petition under Article 8 of the Family Court Act, having been filed on March 05, 2015 in this Court and On Consent, and [REDACTED] having been present in Court and advised of the issuance and contents of this Order,

NOW, THEREFORE, IT IS HEREBY ORDERED that [REDACTED] observe the following conditions of behavior:

[01] Stay away from:

[A] [REDACTED];

[A] [REDACTED] WHEREVER [REDACTED] MAY BE; RESPONDENT IS TO STAY AT LEAST 100 YARDS AWAY;

[B] the home of [REDACTED];

[14] Refrain from communication or any other contact by mail, telephone, e-mail, voice-mail or other electronic or any other means with [REDACTED] RESPONDENT IS NOT TO COMMUNICATE WITH THE PETITIONER VIA ANY MEANS WHATSOEVER, INCLUDING BUT NOT LIMITED TO ELECTRONIC MEANS, TELEPHONE, EMAIL, TEXTING, SOCIAL MEDIA OR INTERNET MESSAGE BOARDS. NO THIRD-PARTY CONTACT;

[02] Refrain from assault, stalking, harassment, aggravated harassment, menacing, reckless endangerment, strangulation, criminal obstruction of breathing or circulation, disorderly conduct, criminal mischief, sexual abuse, sexual misconduct, forcible touching, intimidation, threats, identity theft, grand larceny, coercion or any criminal offense against [REDACTED]



[12] Surrender any and all handguns, pistols, revolvers, rifles, shotguns and other firearms owned or possessed, including, but not limited to, the following: ALL FIREARMS IN HIS POSSESSION and do not obtain any further guns or other firearms. Such surrender shall take place immediately, but in no event later than FORTHWITH at AT THE NEAREST NYPD PRECINCT;

[99] Observe such other conditions as are necessary to further the purposes of protection: THE RESPONDENT [REDACTED], IS NOT TO POST OR TRANSMIT OR CAUSE A THIRD PARTY TO POST OR TRANSMIT, ANY IMAGES OR PICTURES DEPICTING THE PETITIONER IN A NAKED STATE; NOT POST, TRANSMIT, OR CAUSE A THIRD PARTY TO POST OR TRANSMIT, ANY THREATS OF PHYSICAL HARM TO THE PETITIONER OR HER IMMEDIATE FAMILY, INCLUDING IN PERSON, ON THE INTERNET, SOCIAL MEDIA, MESSAGE BOARD, PHONE, ETC;

It is further ordered that this order of protection shall remain in force until and including October 21, 2016.

Dated: October 22, 2015

ENTER



Honorable _____

PURSUANT TO SECTION 1113 OF THE FAMILY COURT ACT, AN APPEAL FROM THIS ORDER MUST BE TAKEN WITHIN 30 DAYS OF RECEIPT OF THE ORDER BY APPELLANT IN COURT, 35 DAYS FROM THE DATE OF MAILING OF THE ORDER TO APPELLANT BY THE CLERK OF COURT, OR 30 DAYS AFTER SERVICE BY A PARTY OR THE ATTORNEY FOR THE CHILD UPON THE APPELLANT, WHICHEVER IS EARLIEST.

The Family Court Act provides that presentation of a copy of this order of protection to any police officer or peace officer acting pursuant to his or her special duties authorizes, and sometimes requires such officer to arrest a person who is alleged to have violated its terms and to bring him or her before the court to face penalties authorized by law.

Federal law requires that this order is effective outside, as well as inside, New York State. It must be honored and enforced by state and tribal courts, including courts of a state, the District of Columbia, a commonwealth, territory or possession of the United States, if the person restrained by the order is an intimate partner of the protected party and has or will be afforded reasonable notice and opportunity to be heard in accordance with state law sufficient to protect due process rights (18 U.S.C §§ 2265, 2266).

It is a federal crime to:

- cross state lines to violate this order or to stalk, harass or commit domestic violence against an intimate partner or family member;
- buy, possess or transfer a handgun, rifle, shotgun or other firearm or ammunition while this Order remains in effect (Note: there is a limited exception for military or law enforcement officers but only while they are on duty) ; and
- buy, possess or transfer a handgun, rifle, shotgun or other firearm or ammunition after a conviction of a domestic violence-related crime involving the use or attempted use of physical force or a deadly weapon against an intimate partner or family member, even after this Order has expired (18 U.S.C. §§ 922(g)(8), 922(g)(9), 2261, 2261A, 2262).

Check Applicable Box(es):

- Party against whom order was issued was advised in Court of issuance and contents of Order
- Order personally served in Court upon party against whom order was issued
- Service directed by other means: Respondent in Court/Delivered to Corrections
- [Modifications or extensions only]: Order mailed on [specify date and to whom mailed]:
- Warrant issued for party against whom order was issued[specify date]: _____
- ADDITIONAL SERVICE INFORMATION [specify]: _____

ORI No: [redacted]
Order No: [redacted]
NYSID No: [redacted]

At a term of the Family Court of the State of New York,
held in and for the County of Kings, at 330 Jay Street, Brooklyn, NY
11201, on August 01, 2018

PRESENT: [redacted] Court Attorney Referee

In the Matter of a FAMILY OFFENSE Proceeding

[redacted]
Petitioner

- against -

[redacted]
Respondent

File # [redacted]
Docket # [redacted]
Order of Protection

Both Parties Present in Court

NOTICE: YOUR FAILURE TO OBEY THIS ORDER MAY SUBJECT YOU TO MANDATORY ARREST AND CRIMINAL PROSECUTION, WHICH MAY RESULT IN YOUR INCARCERATION FOR UP TO SEVEN YEARS FOR CRIMINAL CONTEMPT, AND/OR MAY SUBJECT YOU TO FAMILY COURT PROSECUTION AND INCARCERATION FOR UP TO SIX MONTHS FOR CONTEMPT OF COURT.

THIS ORDER OF PROTECTION WILL REMAIN IN EFFECT EVEN IF THE PROTECTED PARTY HAS, OR CONSENTS TO HAVE, CONTACT OR COMMUNICATION WITH THE PARTY AGAINST WHOM THE ORDER IS ISSUED. THIS ORDER OF PROTECTION CAN ONLY BE MODIFIED OR TERMINATED BY THE COURT. THE PROTECTED PARTY CANNOT BE HELD TO VIOLATE THIS ORDER NOR BE ARRESTED FOR VIOLATING THIS ORDER.

A petition under Article 8 of the Family Court Act, having been filed on April 02, 2018 in this Court and On Consent, and [redacted] having been present in Court and advised of the issuance and contents of this Order.

NOW, THEREFORE, IT IS HEREBY ORDERED that [redacted] observe the following conditions of behavior:

[01] Stay away from:

- [A] [redacted];
- [B] the home of [redacted];
- [C] the school of [redacted];
- [D] the business of [redacted];
- [E] the place of employment of [redacted];

[14] Refrain from communication or any other contact by mail, telephone, e-mail, voice-mail or other electronic or any other means with [redacted] no third party or social media contact;

[02] Refrain from assault, stalking, harassment, aggravated harassment, menacing, reckless endangerment, strangulation, criminal obstruction of breathing or circulation, disorderly conduct, criminal mischief, sexual abuse, sexual misconduct, forcible touching, intimidation, threats, identity theft, grand larceny, coercion or any criminal offense against [redacted];

[99] Observe such other conditions as are necessary to further the purposes of protection: no accessing social media accounts owned by [redacted]; No impersonating [redacted] online; NO distributing, disseminating, publishing intimate photographs, images, texts, videos of [redacted];



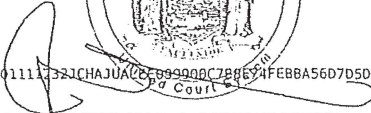
It is further ordered that this order of protection shall remain in force until and including August 01, 2019.

Dated: August 01, 2018

ENTER



201808011112321CHAJUAUC69900C788674FE8BA56D7D506FC215F



[Redacted Name], Court Attorney Referee

PURSUANT TO SECTION 1113 OF THE FAMILY COURT ACT, AN APPEAL FROM THIS ORDER MUST BE TAKEN WITHIN 30 DAYS OF RECEIPT OF THE ORDER BY APPELLANT IN COURT, 35 DAYS FROM THE DATE OF MAILING OF THE ORDER TO APPELLANT BY THE CLERK OF COURT, OR 30 DAYS AFTER SERVICE BY A PARTY OR THE ATTORNEY FOR THE CHILD UPON THE APPELLANT, WHICHEVER IS EARLIEST.

The Family Court Act provides that presentation of a copy of this order of protection to any police officer or peace officer acting pursuant to his or her special duties authorizes, and sometimes requires such officer to arrest a person who is alleged to have violated its terms and to bring him or her before the court to face penalties authorized by law.

Federal law requires that this order is effective outside, as well as inside, New York State. It must be honored and enforced by state and tribal courts, including courts of a state, the District of Columbia, a commonwealth, territory or possession of the United States, if the person restrained by the order is an intimate partner of the protected party and has or will be afforded reasonable notice and opportunity to be heard in accordance with state law sufficient to protect due process rights (18 U.S.C §§ 2265, 2266).

It is a federal crime to:

- cross state lines to violate this order or to stalk, harass or commit domestic violence against an intimate partner or family member;
- buy, possess or transfer a handgun, rifle, shotgun or other firearm or ammunition while this Order remains in effect (Note: there is a limited exception for military or law enforcement officers but only while they are on duty) ; and
- buy, possess or transfer a handgun, rifle, shotgun or other firearm or ammunition after a conviction of a domestic violence-related crime involving the use or attempted use of physical force or a deadly weapon against an intimate partner or family member, even after this Order has expired (18 U.S.C. §§ 922(g)(8), 922(g)(9), 2261, 2261A, 2262).

Check Applicable Box(es):

- Party against whom order was issued was advised in Court of issuance and contents of Order
- Order personally served in Court upon party against whom order was issued
- Service directed by other means[specify]: _____
- [Modifications or extensions only]: Order mailed on [specify date and to whom mailed]: _____
- Warrant issued for party against whom order was issued[specify date]: _____
- ADDITIONAL SERVICE INFORMATION [specify]: _____

