

COMBATTING CYBER ABUSE

A Manual for Advocates



NEW YORK CYBER ABUSE TASK FORCE
Second Edition / July 2023

ABOUT THIS MANUAL.

What is the New York Cyber Abuse Task Force?

This Manual was originally created by the **New York Cyber Abuse Task Force (the “Task Force”)**, a coalition of New York-based legal and non-legal professionals, survivors, and other volunteers who are committed to fighting cyber abuse at the intersection of gender-based and intimate partner violence. The Manual was first created in 2018 after members of the Task Force saw an increase in technology-facilitated abuse (aka “tech abuse”) and identified the need for a comprehensive manual to support advocates fighting for victims and survivors.

The Task Force is a coalition of New York State based legal and non-legal professionals, cyber abuse survivors, and other individuals committed to fighting technology-facilitated abuse and intimate partner violence in all its forms, which includes but is not limited to the non-consensual dissemination, or threat of dissemination, of sexual images (cyber sexual abuse, sometimes referred to as “revenge porn”), hacking, stalking, spoofing, harassment, identity theft, and impersonation.

The Task Force has three main areas of focus: 1) advocating for comprehensive laws and policies that appropriately and inclusively address technology-facilitated abuse and protect and support victims of such abuse; 2) supporting attorneys and other service providers working with victims of technology-facilitated abuse by providing trainings, resources, and best practices; and 3) raising awareness about technology-facilitated abuse and victims’ rights through community and public outreach and education.

The Task Force includes representatives from a breadth of government and nonprofit agencies as well as survivors and independent civil attorneys, including Sanctuary for Families, C.A. Goldberg, PLLC, Day One, Cornell Tech’s Clinic to End Tech Abuse, Urban Justice Center, Safe Horizon, Legal Momentum, Legal Information for Families Today (LIFT), NYLAG, HerJustice, Legal Services NYC, Cyber Civil Rights Initiative, and others.

The work of the Task Force member organizations includes significant representation in New York Family Courts, Supreme Courts, criminal courts, and civil courts. Collectively, the Task Force member organization represent hundreds of individuals, including low-income litigants, across New York City as well as other areas of New York State. Many of the litigants represented by the Task Force member organizations are low-income people of color, women and women-identifying, members of the LGBTQ community, and more. A vast majority of the litigants represented by the Task Force member organizations are victims of gender-based violence and intimate partner violence.

To contact the New York Cyber Abuse Task Force, please

Visit: <https://www.cyberabuse.nyc>

E-mail Task Force Co-Chairs **Lindsey Song** (lsong@sffny.org) or **Annie Seifullah** (annie@cagoldberglaw.com).

A Note About the Manual

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 abuse or tech 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 abuse. Advocates should also **review the laws and policies in their applicable jurisdictions before providing advice and information.**

This Manual is primarily written to aid New York-based advocates and therefore primarily New York resources and law are covered. However, an index of resources, including international resources, is included at the end of this Manual.

TABLE OF CONTENTS

INTRODUCTION	7
I. What is Cyber Abuse aka Tech Abuse?	7
II. Scope of the Manual	9
III. The Conceptual Framework	9
IV. A Discussion on Trauma Informed Understanding	11
PART 1: CRIMINAL REMEDIES FOR VICTIMS OF TECH ABUSE	14
I. New York City and New York State Criminal Law	14
A. New York City Unlawful Disclosure Law	14
B. New York State Unlawful Disclosure Law	20
C. Differences between NY State and NY City Laws	25
D. Suffolk County Criminal Law	26
E. Nassau County Criminal Law	26
F. Common New York Penal Code Provisions Addressing Tech Abuse	27
G. Supporting Victims of Tech Abuse Who Report to Law Enforcement (New York)....	30
II. Federal Criminal Law	39
A. Computer Fraud and Abuse Act, 18 U.S.C. § 1030	39
B. Aggravated Identity Theft, 18 U.S.C. § 1028A	40
C. Federal Wiretap Act, 18 U.S.C. § 2520	40
D. Interstate Stalking or Harassment, 18 U.S.C. § 2261A	40
E. Interstate Threats or Extortion, 18 U.S.C. § 875	41
F. Obscene or Harassing Telephone Calls in Interstate or Foreign Communications, 47 U.S.C. § 233.....	41
G. Video Voyeurism Prevention Act of 2004, 18 U.S.C. § 1801	41
PART 2: CIVIL REMEDIES FOR VICTIMS OF TECH ABUSE	42
I. Civil Orders of Protection – New York	42
II. New York State and New York City Civil Causes of Action	46
A. New York City Civil Causes of Action	46
B. New York State Civil Causes of Action	47
III. Federal Causes of Action	51
A. NEW (2022) Civil Cause of Action for Disclosure of Intimate Images	51
B. Cases Against Governmental Entities	53
C. Cases Against Non-Governmental Entities	54
IV. RECENT SETTLEMENTS OF CIVIL CAUSES OF ACTION	57
PART 3: RELEVANT SOCIAL MEDIA AND TECH PLATFORMS ASSOCIATED WITH TECH ABUSE	61
I. Social Media	61

A. Facebook.....	61
B. Instagram.....	63
C. LinkedIn.....	63
D. Snapchat.....	64
E. TikTok.....	65
F. Twitter.....	65
G. Tumblr.....	67
H. YouTube.....	67
II. Phone and Messaging Platforms.....	68
A. WhatsApp.....	68
B. Skype.....	68
C. WeChat.....	69
III. Discussion Boards/Servers.....	71
A. Reddit.....	71
IV. Pornography Websites.....	71
V. Dating Websites.....	72
A. Match.com.....	72
B. Tinder.....	72
C. Grindr.....	73
D. Seeking Arrangements.....	74
E. Craigslist.....	75
VI. Google Search Results.....	75
PART 4: TECH ABUSE EVIDENCE & TRIAL ADVOCACY.....	77
I. Prior to Litigation: Active Steps to Preserve.....	77
II. Important Considerations During Litigation.....	82
A. Litigation Hold Requests.....	82
B. Organizing Evidence.....	83
C. Presenting Evidence at Trial.....	84
PART 5: COPYRIGHTING & REMOVING IMAGES AND VIDEOS FROM THE WEB.....	88
A. Background and Initial Consideration.....	88
B. Registering a Copyright with the Copyright Office.....	88
C. Benefits of Registration.....	90
D. DMCA; DMCA Complaints and Takedown Notices.....	91
E. Takedowns and Subpoenas.....	93
F. De-Indexing from Google.....	93
PART 6: BEST PRACTICES FOR SAFETY PLANNING IN THE CONTEXT OF TECH ABUSE.....	98

A. General Safety Tips: The “Digital Breakup Plan”	98
B. Securing Cell Phones and Tablets.....	99
C. Computers, E-mail, and Online Browsing.....	101
D. Social Media Accounts	102
E. Credit Cards and ID Theft	103
F. Nonconsensual Pornography: Images and Videos	104
G. Detecting Spyware	105
PART 7: RESOURCES	107
I. Directory of Useful Websites (Written Resources).....	107
II. Directory of Service Organizations.....	109
III. Teen Dating Violence Hotline Numbers:	119
PART 8: APPENDICES	120

APPENDIX	DOCUMENT
A.	Ten 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 technology-facilitated abuse language on Orders of Protection
D.	Family Offense Petitions alleging technology-facilitated abuse
E.	Family Court Orders of Protection including provisions prohibiting technology-facilitated abuse
F.	Case law interpreting federal criminal and civil statutes
G.	New York City Administrative Code § 10-180
H.	New York Penal Law § 245.15
I.	New York Family Court Act § 812
J.	New York Criminal Procedure Law § 530.11
K.	New York Civil Rights Law § 52-b
L.	Apple Guide: Device and Data Access when Safety is at Risk

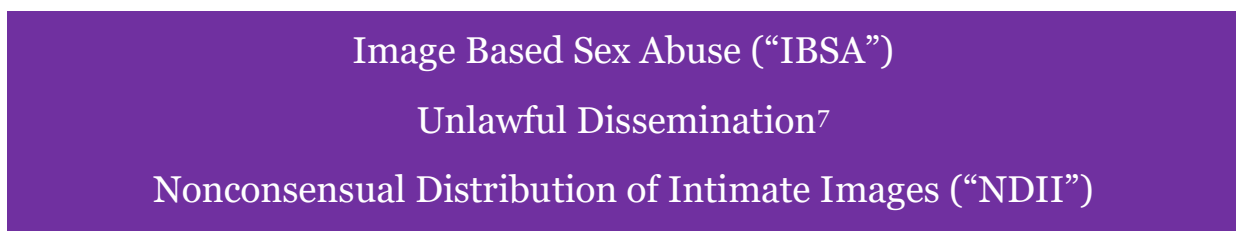
INTRODUCTION

I. What is Cyber Abuse aka Tech Abuse?

Perpetrators¹ of intimate partner violence are increasingly using online platforms or other digital technologies to abuse, exploit, harass, and threaten their victims. This type of abuse includes an array of harassment and stalking 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 “Unlawful Dissemination,” “image-based sex abuse,” or “IBSA” for short). All of these harms fall under the umbrella of **Cyber Abuse**, which is sometimes also called **Technology-Facilitated Abuse** (or “**Tech Abuse**” for short). Readers will notice that we use these terms interchangeably throughout the Manual. A glossary of terms can be found at the Cyber Civil Rights Initiative,⁴ Online Harassment Field Manual,⁵ and Maru⁶.

Image based sex abuse (“IBSA”), formerly known as “revenge porn,” is perhaps the most severe form of tech abuse. The term “revenge porn,” though commonly used, is somewhat of a misnomer and advocates have shifted away from using this term for a variety of reasons. In many cases, perpetrators are not motivated by revenge or by any personal feelings toward the victim. Additionally, the term “revenge” inappropriately victim-blames by implying that a 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 like the New York Cyber Abuse Task Force prefer to use broader and less problematic terms, such as:



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

² “Spoofing” is the disguising of a sender’s identity so that the recipient believes the sender is someone else. *See, e.g., What is a spoofing attack?* MALWAREBYTES, <https://www.malwarebytes.com/spoofing> (last visited July 17, 2023).

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.

⁴ *Guide for Media*, CYBER CIVIL RIGHTS INITIATIVE, <https://cybercivilrights.org/news/media-kit/media-guide/> (last visited July 17, 2023).

⁵ *Online Harassment Field Manual*, PEN AMERICA, <https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/> (last visited July 17, 2023)

⁶ *Glossary of Terms*, MARU, <https://about.maruchatbot.co/glossary-of-terms.html> (last visited July 17, 2023)

⁷ For the purposes of this Manual, we will use the terms Unlawful Dissemination and Image Based Sex Abuse (or IBSA for short), however, all of the listed alternatives are acceptable.

Cyber Sexual Abuse (“CSA”) Nonconsensual Pornography (“NCP”)

With the ubiquitous use of social media platforms and growing ease of electronic communication, perpetrators of IBSA and other forms of technology abuse are able to inflict major and lasting damage very quickly. The harms caused tech abuse, especially IBSA, 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. Images and videos that become the fodder of tech 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 surreptitiously).

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.

A Note on the COVID-19 Pandemic

Member organizations of the Task Force have reported a disturbing increase in clients suffering cyber sexual abuse, and technology-facilitated abuse throughout the pandemic. Attorneys and advocates noted a large increase in reports of technology abuse from clients and the community, including sextortion, online stalking and threats, cyber sexual abuse, and more. Clients, trapped in their homes, reported hundreds of harassing text messages and social media messages, violent threats, spyware and stalkerware, and more. A large 2019 study found a 400% increase in the number of victims of CSA from 2016 (Eaton & Ruvalcaba 2019).

With the ubiquitous use of social media platforms and growing ease of electronic communication, perpetrators of technology abuse are able to inflict major and lasting damage very quickly. The harms caused by these forms of 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. Unfortunately, technology moves faster than statutes and case law, and often faster than judges, law enforcement, and other systems as well. It is critical that systems are provided with the tools and resources to effectively respond to cyber sexual abuse, and other forms of technology-facilitated abuse, to protect survivors and empower them to move into lives of safety and security.

II. Scope of the Manual

The original mission of the Task Force was to pass laws in support of victims of IBSA. Since that goal was accomplished, our mission has shifted to advocating for survivors who find themselves at the intersection of **tech abuse and intimate partner (or gender-based) violence**.

This Manual reflects that shifted focus by providing an overview of various types of technology-facilitated abuse. On a micro level, the Manual reviews specific statutes and legal remedies that address tech abuse at both local and national levels. On a macro level, the Manual begins with an introduction to some of the conceptual framework (“big picture”) ideas upon which the Task Force operates.

III. The Conceptual Framework

The Task Force has four foundational concepts that guide its work. The first foundational concept is:

1: The most dangerous and persistent forms of tech abuse occur in the context of intimate partner violence and image-based sex abuse.

The tech abuse that this Manual seeks to address typically take the form of one determined abuser targeting one victim by using technology to frighten, control, bully, harm, monitor, intimidate or threaten them. Tech abuse can be an isolated incident, or it can be a repeated and persistent pattern.

One determined abuser can cause a tremendous amount of harm and disruption in the life of their target. And the harm is amplified when the abuser has intimate and specific knowledge of the person they are targeting.

For a victim, this type of tech abuse can feel endless and inescapable.

The second foundational concept that guides the Task Force’s work is:

2: You don’t have to be a **tech expert** to understand **tech abuse**.

That’s because intimate partner violence is about **power and control**. We encourage readers of this Manual to avoid focusing on the specific technicalities and complex functions of technology platforms or devices and focus instead of how these tech tools are being used. Which usually take the form of harassment, stalking, bullying, intimidation, or threatening conduct towards the victim.

Some tech abusers are tech-savvy. However: a perpetrator can cause a lot of harm without being a tech-savvy person. We have witnessed our clients experience tremendous harm and disruption in their lives caused by nothing more than an abuser who knows how to make fake accounts by making up usernames and passwords. ***Tech abuse is abuse. Period.***

The third foundational concept that guides the Task Force’s work is:

3: Technology-facilitated abuse should be treated with the same seriousness as “in person” abuse.

A prevailing tech abuse myth is that if someone is being targeted online, then they can just “log off” and the abuse will stop. But this is simply not true.

Tech abuse can cause extreme harm to the person being targeted regardless of the target’s use of tech or the internet. Tech abuse can destroy victims’ reputations, get them fired from jobs, or lead them to have suicidal thoughts or self-harming behaviors. We also have seen countless cases where cyber abuse escalated to in-person abuse, for example when tech abusers creating impersonating profiles of their victim in order to trick strangers into coming to their job or their house. *Doxing*⁸ is also a very serious type of tech abuse that can turn into “in person” stalking, harassment, and violence.

It is unfair to require that a victim change their behavior because of a perpetrator’s actions – and expecting a person to stay offline is not only ineffective in keeping the victim safe, it also creates additional harm by denying the victim access to support communities, economic/educational opportunities, and more.

Our lives are inextricably linked to the internet, to technology platforms, and to the devices that we use to access them. *There is No Offline.*

The fourth foundational concept that guides the Task Force’s work is:

4: You have a lot of power to improve the safety outcomes of victims being targeted through tech abuse.

The “you” of this belief describes any person or group that is willing to learn about tech abuse or advocate for people being targeted by it. This means attorneys, social workers, victims’ advocates, judges, law enforcement officers, elected officials, and lawmakers.

This Manual is just one part of our efforts to educate whoever will listen about the ways that they can specifically act to improve the safety outcomes of victims and survivors of tech abuse who they are charged with protecting and helping.

Thank you for taking the time to equip yourself with the mindset and tools to help combat the terrible modern harm that is tech abuse.

⁸ Doxing is the act of publishing private information about a person (the “target”) on the internet, usually with the intent of facilitating or encouraging third parties to harass or stalk the target.

The word “victim” is used in this manual to refer to the person who has, or still is, experiencing cyber sexual abuse. It is important to ask the person you are working with how they self identify (e.g., survivor) and respect the language they chose to use.

IV. A Discussion on Trauma Informed Understanding

Technology-facilitated gender-based violence is trauma. It is imperative to build a foundation of safety when you work with someone who has experienced technology-facilitated gender-based violence, or any form of trauma. Trauma informed care aims to establish safety and promote healing. Safety looks, feels and sounds different to those who have been victimized through technology. Digital communication can activate a person’s trauma, further impacting their access to care providers and seeking justice. As our world is increasingly lived online and through computers, it is imperative to understand how technology triggers can adversely affect vulnerable populations. Being mindful and intentional about how technology is used can help lawyers, advocates, mental health professionals and other providers to connect with clients without creating conditions that are potentially re-traumatizing. The existing minimization of how technology-facilitated gender-based violence impacts a victims mental and physical health leads to stigmatization. You can help to end this stigma through communicating with the victim and others from a trauma informed understanding.

A. Mental Health Impact

Abuse that takes place digitally can extend to all aspects of a victim's life. The negative mental health impact of being abused online and off is paramount to understanding how to work with a victim. There may be other emotional, physical and sexual abuses that the victim has experienced throughout the course of their life, or may currently be experiencing.

The mental health impact of technology-facilitated gender-based violence is both acute and chronic. Victims may experience different feelings, emotions and thoughts throughout the course of your work together. Personal recovery from abuse is individualized and nonlinear. It’s important to remember that those you work with may look and act differently as changes arise. You have the ability to promote healing with your client by being present, non judgmental, and compassionate.

Trauma fragments a person’s sense of self and they can lose trust in those around them. Ensure you are establishing and maintaining trust with the person you are working with. This involves being consistent and transparent; clear on your intent, abilities and capabilities; and limits to your scope of practice.

B. Triggers

Victims who have experienced weaponization of technology can strongly impact their daily lives, changing the ways they interact with electronics and their online needs. Re-traumatization may occur when victims use their electronic devices to connect, something that in today's world they cannot avoid doing. Alerts and pings from devices can send signals to the victim's brain and body that they are in danger, which can impact their ability to communicate with others. Hyper vigilance, hyper arousal and avoidance are common reactions.

Further, a victim collecting, cataloging, tracking and documenting their own abuse is inherently traumatic. If the victim you are working with has to engage in the documentation process of their own abuse, acknowledge there may be an emotional toll and offer support in the capacity you are able to. If you are going to help your client collect materials for evidence, have a discussion with them first about the security and confidentiality measures your workplace has established to protect the materials. This may relieve some of their anxiety about the materials being collected by someone else.

Navigating bureaucratic systems can be overwhelming and may trigger your client into re experiencing aspects of their trauma. Common emotions victims feel while moving through the legal and justice systems include powerlessness, helplessness, extreme distress and constant confusion. Help your client manage these feelings by being direct, giving concrete time frames on follow ups, and having consistent communication.

C. Consensual Communication

Trauma from technology-facilitated gender-based violence is unique due to the litany of ways victims are forced to interact with the digital world. Build your work with your client to be safety- and consent-focused through intentional dialogue on digital communication practices.

Initial steps to establishing safety include navigating communication styles, preferences and safety needs. Communication through technology may trigger your client and therefore be a space where your methods and practices can promote healing. Ask your client how they prefer to communicate, what their secondary preferred method is, and then affirm this by communicating with them in those ways. Navigate potential triggers by asking directly if they experience any negative impact when using electronics. Assess how the victim wants you to follow up with them if they have not responded to you in the agreed upon ways.

Explore and establish boundaries with communication, such as if there are things that should be not communicated over email. Do not include the victim on group messaging such as group emails, without their consent. If possible, offer end to end encrypted messaging, phone and video conferencing, as this helps the victim to understand that you are prioritizing their safety. Normalize talking about how you maintain your own digital security and protect the privacy of the victim.

When you are working with a person who has experienced technology-facilitated gender-based violence, it can be difficult for a person to communicate as stress and trauma impacts cognitive

processing and executive functioning. Be mindful that it can be hard for the victim to absorb all the information you are telling them. If possible, ask them how you can follow up with them to ensure they have all the information they need to move forward with action steps.

D. Camera Consent

Help the victim to make choices about how they use their image. Inform them ahead of time if there are scenarios where they will have to engage in image based communication, such as virtual court hearings. Video calls and video-conferencing are common venues to communicate face-to-face. For those who have been victimized with technology-facilitated gender-based violence, being on camera can create high amounts of anxiety. It is important not to minimize this fear or anxiety.

Do not assume that communications and virtual life must automatically involve camera access. Practice affirmative camera consent in your daily life by normalizing that people do not need to be on camera to connect and communicate. Let victims know that it's okay for them not to be on video, and that they can turn their camera off at any time on the occasions that they do choose to be on video.

E. Provider Self Care

Secondary trauma, vicarious trauma, compassion stress, compassion fatigue, burnout, and empathic strain refer to the effects on your own mental health that you may experience when working with trauma victims. Providers need to care for their own mental health, it is essential to this work. Be aware of new thoughts, feelings and emotions that arise over the course of your work with a person surviving image-based abuse. Build and maintain your own network of professional and personal support and engage in daily practices that promote your own wellness, care and resiliency. Seek support when you need it and do not neglect your own mental health needs.

PART 1: CRIMINAL REMEDIES FOR VICTIMS OF TECH ABUSE

The laws governing tech abuse are an imperfect web of state and federal laws. Unfortunately, there are still no federal laws that criminalize image-based sex abuse when the victim is an adult (“IBSA”). As of July 2023, forty-eight states, the District of Columbia, Puerto Rico, and Guam have laws addressing cyber sexual abuse on the books. However, both New York City and New York State have passed laws addressing IBSA dating back to 2017.

I. New York City and New York State Criminal Law

Only two (2) states have not yet passed a law making it a crime to disseminate sexual images without the depicted person’s consent. In 2019, New York State joined the vast majority of states – forty-eight states, the District of Columbia, Guam, and Puerto Rico – that criminalize this type of IBSA in some shape or form.⁹

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 a class 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.¹⁰

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, 2018.¹¹ The legislation also creates a civil cause of action that allows survivors to sue perpetrators for damages and other relief.¹² 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 IBSA summarizes the civil remedy available under the new legislation.

A. New York City 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 10-180.¹³ The NYC Unlawful Disclosure Law makes it

⁹ *48 States + DC + Two Territories Now Have Laws Against Nonconsensual Pornography*, CYBER CIVIL RIGHTS INITIATIVE <https://www.cybercivilrights.org/nonconsensual-pornography-laws/> (last visited July 8, 2023).

¹⁰ See A.0719 Text, NEW YORK STATE ASSEMBLY https://assembly.state.ny.us/leg/?default_fld=&leg_video=&bn=S01719&term=2019&Text=Y Update

¹¹ NYC Administrative Code 10-180.

¹² See NYC Administrative Code 10-180.

¹³ 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>.

unlawful to disclose, or threaten to disclose, intimate images with the intent to cause harm, where the individual depicted is or would be identifiable to another person from the image.¹⁴ Unlawful Disclosure is categorized as an unclassified misdemeanor and is punishable by up to one year in jail, a fine of \$1,000, or both.¹⁵

Elements of the Law

The elements of the NYC Unlawful Disclosure Law, labeled (a) through (g) are described below.

a. Covered Recipient

The term “covered recipient” means an individual who gains possession of, or access to, an intimate image from a depicted individual, including through the recording of the intimate image.¹⁶ The legislative history of the law indicates that the New York City Council limited liability to “covered recipients” due to concerns that liability for the recording of intimate images could be too broad. The current law’s language concerning “covered recipients” is a change from the original form of the bill:

The original version of this bill prohibited any person from distributing an intimate image, whereas the current version only prohibits a ‘covered recipient’ . . . Given the potential of images ‘going viral’ or distributed widely in a rapid fashion on the internet or social networking sites, prohibiting ‘any person’ from distributing the intimate image was too broad. It could potentially hold an individual liable or criminally responsible for sharing an image that he or she was unaware of its source. Therefore, the current version of the bill only addresses ‘covered recipients.’”¹⁷

The Committee Report also notes as an example that “the prohibition would not cover an individual who was sent an intimate image from a friend who received that image from the depicted individual.”¹⁸ The New York City Council stated this limitation would prevent unduly broad application of the law to individuals who may have no knowledge of the depicted individual's consent or lack thereof.¹⁹ In practice, advocates have found that this provision has lead to some difficulty in successful prosecution. *See infra*.

b. 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

¹⁴ 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>.

¹⁵ NYC Administrative Code 10-180 §c.

¹⁶ *Id.*

¹⁷ See New York City Council, Committee on Public Safety, Report of the Governmental Affairs Division on Proposed Int. No. 1267-A, November 1, 2017 at 19 [“Committee Report”].

¹⁸ *Id.* at 10.

¹⁹ *This cite should be directly to the City Council minutes/reports where they addressed this.*

the New York City law is important because abusers often use the threat of dissemination in order to exert control over their victims.²⁰ 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.

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.²¹ 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.”²²

c. 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.”²³

d. 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

²⁰ The threat to disseminate sexually explicit images is also treated as an offense equivalent to actual dissemination of such images under the provisions of IBSA laws in Texas and West Virginia. *See* Texas Penal Code Ann. § 21.16(c); West Virginia Code §61-8-28a(b).

²¹ NYC Administrative Code 10-180.

²² N.Y. Penal Law § 250.40.

²³ NYC Administrative Code 10-180 Importantly, an intimage image under NYC Administrative Code 10-180 does not include images such as bikini or lingerie photos, or or the uncovered rear of a victim, unless the anus is visible.

intimate image.”²⁴ 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.

e. 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.”²⁵ Arguably, 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.

f. 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.”²⁶

g. Intent Not to be Disclosed

Within the purview of N.Y.C. Admin. Code 10-180, an “intimate image” must refer to one that has been disclosed, or threatened to be disclosed, “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.*”²⁷

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

The disclosure of an intimate image is not criminalized where “[s]uch 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.”²⁸ For example, if an individual is reporting the sending of an intimate image to the police, showing the

²⁴ *Id.*

²⁵ *Id.*

²⁶ *Id.*

²⁷ *Id.*

²⁸ *Id.*

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

Similarly, disclosure is not criminalized where “[s]uch 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.”²⁹ 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 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

Finally, disclosure is not criminalized where “[s]uch 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.”³⁰ 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).³¹

d) Public Place Exception

Finally, “[a]n 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.”³² 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 would apply even if an image or video was taken as a result of coercion, under duress, or even in conjunction with a sexual assault.

Challenges

Covered Recipient Challenges

The “covered recipient” element of NYC Unlawful Disclosure Law has posed challenges for prosecutors when courts dismiss criminal complaints because they fail to plead details about

²⁹ *Id.*

³⁰ *Id.*

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

³² *Id.*

how the intimate image was recorded or how the defendant came to possess it. In *People v Ahmed*, 64 Misc 3d 601, 102 NYS3d 421, 2019 NY Slip Op 29170 (Crim Ct, Bronx County 2019), the defendant posted a video on Instagram depicting the victim, his ex-girlfriend, performing an oral sex act on him. In the criminal complaint, the victim stated that she was identifiable in the video, that the defendant named the victim in the caption of the posted video, and that he did so without her permission with the intent to cause her annoyance, alarm, and fear for her physical safety. The complaint was silent on how the video in question was recorded or how it came to be in the defendant's possession.

The defendant in *Ahmed* moved for dismissal because the People did not plead that the defendant was a “covered recipient.” The People argued that the court can reasonably infer that defendant was a “covered recipient” from the fact that “the only two individuals in the video are the defendant and the victim.” However, the court granted dismissal of the complaint, reasoning that the fact that the defendant was a participant in the act was not enough to establish the “covered recipient” element. The court stated that the complaint contained no allegations about the circumstances of the recording of the video, nor did the complaint state the defendant and the victim were the only parties involved in the sex act or in the recording. The court concluded that it will therefore not rely on unsupported assumptions both as to how the video came into being and how the defendant came to possess it.

Additionally, in the unpublished opinion, *People v E.R.*, 65 Misc 3d 1201[A], 2019 NY Slip Op 51469[U], *1-2 (Sup Ct, NY County 2019), the People’s complaint alleged that the defendant sent two intimate photos of the victim to her boyfriend, A.R., on Facebook. According to the complaint, the victim’s face and breasts were clearly visible in the photo, the victim did not give the defendant permission or authority to possess, view, or share the above-mentioned photos, and the defendant's actions caused her substantial emotional harm. The victim also stated that she knew that the defendant sent the two photos to her boyfriend because the messages came from defendant's Facebook account, which she recognized. When the defendant in *E.R.* moved to dismiss the complaint for facial insufficiency, the court granted the motion. The court found that because the complaint was silent as to how the two photos came into defendant's possession or as to who took them, the complaint failed on the “covered recipient” element.

Ex Post Facto Challenges

The NYC Unlawful Disclosure Law may face future ex post facto challenges. In *People v Mowring*, 64 Misc 3d 900, 907 (Crim Ct, Richmond County 2019), between March 2018 and September 2018, the defendant published a video recording of the defendant and the victim engaging in a sexual act on a pornographic website. The defendant admitted to the victim that he took this video between January 2013 and December 2013. The victim recognized the defendant’s username on the pornographic website as the same username that the defendant used on other social platforms. The defendant moved to dismiss the complaint arguing that it was facially insufficient and arguing unconstitutionality based on the Ex Post Facto Clause of the U.S. Constitution. However, the court found that the complaint was facially sufficient, and that the count was constitutional based upon the posting date of the video to the pornographic website, which was after the effective date of the statute.

PRACTICE TIP: Regardless of when the images were taken, if the intimate images in question were non-consensually distributed, posted or shared **before** the date that NYC Unlawful Disclosure Law went into effect, an Ex Post Facto challenge could prevail.

Intent to Cause Harm Challenges

The “intent to cause harm” element of the NYC Unlawful Disclosure Law may pose challenges in proving charges of unlawful disclosure of an intimate image, as it creates an 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.³³ 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.³⁴

First Amendment Challenges + Public Place Concerns

Additionally, advocates expect that the broad “legitimate public concern” exception may be used to deflect unlawful disclosure charges and claim First Amendment defenses under the law. Finally, 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 Unlawful Disclosure Law

In 2019, New York State passed legislation criminalizing IBSA on a state level; the law was signed by Governor Cuomo on July 23, 2019³⁵ and went into effect as of September 21, 2019. The legislation, A5981/A1719³⁶ amended the penal law, the criminal procedure law, the Family Court Act (“FCA”) and the civil rights law, by:

- Establishing the crime of unlawful dissemination or publication of an intimate image as a Class A Misdemeanor;

³³ 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.

³⁴ 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-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”).

³⁵ Press Release, Governor’s Press Office, Governor Cuomo Signs Measure Criminalizing the Publication of Revenge Porn, (July 23, 2019), <https://www.governor.ny.gov/news/governor-cuomo-signs-measure-criminalizing-publication-revenge-porn>

³⁶ See <https://www.nysenate.gov/legislation/bills/2019/s1719/amendment/c>, https://assembly.state.ny.us/leg/?default_fld=&leg_video=&bn=A05981&term=2015&Summary=Y.

- Creating the family offense of unlawful dissemination or publication of an intimate image;
- Creating a private right of action for individual to pursue injunctive relief and damages;
- Allowing a special proceeding to obtain court order to permanently remove image from internet – first in the country to do so.

For a discussion on the new family offense created under the law, please see Part 2, Section I. Family Court Orders of Protection, *infra*. For a discussion of the civil provision of the law, please see Part 2, Section II. New York State and New York City Civil Causes of Action, *infra*.

The new penal code provision, N.Y. Penal Law 245.15, creates the crime of “unlawful dissemination or publication of an intimate image.” It is now a crime to distribute an image or video showing an identifiable person’s “intimate part,” which refers to the “naked genitals, pubic area, anus or female nipple”³⁷ of that person, without such person’s consent. The law applies where the depicted person had a reasonable expectation that the image would remain private, and the defendant knew or reasonably should have known about that expectation. A violation of this provision is a Class A misdemeanor, punishable by up to a year in prison and a \$1,000 fine.

Under N.Y. Penal Law 245.15, an individual violates the law if “with intent to cause harm to the emotional, financial or physical welfare of another person, he or she intentionally disseminates or publishes a still or video image of such other person, who is identifiable from the still or video image itself or from information displayed in connection with the still or video image, without such other person’s consent” depicting “an unclothed or exposed intimate part of such other person; or such other person engaging in sexual conduct as defined in subdivision ten of section 130.00³⁸ of this chapter with another person; and such still or video image was taken under circumstances when the person depicted had a reasonable expectation that the image would remain private and the actor knew or reasonably should have known the person depicted intended for the still or video image to remain private, regardless of whether the actor was present when the still or video image was taken.”

1. Elements of the Law

(a) Intentionally disseminate or publish

N.Y. Penal Law 245.15 defines (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.³⁹ Thus, “disseminate” or “publish” means:

³⁷ N.Y. Penal Law § 245.15

³⁸ “ ‘Sexual conduct’ means sexual intercourse, oral sexual conduct, anal sexual conduct, aggravated sexual contact, or sexual contact.” N.Y. Penal Law § 130.00 (10).

³⁹ N.Y. Penal Law § 245.15(a).

- Disseminate: “To give, provide, lend, deliver, mail, send, forward, transfer or transmit, electronically or otherwise to another person;”⁴⁰ 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.”⁴¹

(b) A still or video image

A perpetrator must disseminate or publish “a still or video image of such other person.”⁴²

(c) Intimate Part

Under N.Y. Penal Law 245.15 it is unlawful to disseminate a still or video image depicting “an unclothed or exposed intimate part of such other person; or such other person engaging in sexual conduct” with another person without the individual’s consent. Intimate body parts means the naked genitals, pubic area, anus or female nipple of the person.”⁴³ Sexual conduct means “sexual intercourse, oral sexual conduct, anal sexual conduct, aggravated sexual contact, or sexual contact.”⁴⁴

(d) Without Consent

The law applies where a perpetrator disseminates or publishes an image without the depicted individual’s consent. Where a depicted individual did not intend for a photo to be disseminated or published at the time the image was taken or sent (even if the depicted individual consented to the actual taking of the image), N.Y. Penal Law 245.15 applies. It is critical to note that the consent is at the point of *dissemination*, not the point of the video recording or taking of the photograph. Therefore, even if the depicted individual consented to the taking of the photo itself (i.e., took a naked selfie and sent it to the perpetrator), that does not mean the depicted individual consented to the photo being disseminated or published.

(e) Intent to Cause Harm

The perpetrator must disseminate or publish the image with “intent to cause harm to the emotional, financial or physical welfare of another person.”⁴⁵ Arguably, this intent may be evinced through contemporaneous messages with the image or video, statements made by the

⁴⁰ N.Y. Penal Law § 250.40 (5).

⁴¹ *Id* at (6).

⁴² N.Y. Penal Law § 245.15(a).

⁴³ N.Y. Penal Law § 245.15 2.

⁴⁴ N.Y. Penal Law § 130.00.

⁴⁵ N.Y. Penal Law § 245.15 1.(a).

perpetrator to the victim, or other surrounding circumstances that would show that the perpetrator intended harm. The content of the photo or image itself could belie an intent to cause harm, along with its intended audience. For example, if a naked image was sent to a school where the victim was employed as a teacher, this could imply that the perpetrator sought to cause economic harm to the victim by getting them in trouble at work or having them fired.

(f) Identifiability

For the dissemination or publication of images, a depicted individual is “identifiable” if the victim “is identifiable from the still or video image itself or from information displayed in connection with the still or video image is or would be identifiable to another individual either from the intimate image or from the circumstances under which such image is disclosed.”⁴⁶ Even if the individual is not clearly identifiable in the still or video image, if the individual can be identified through her surroundings in the image or identified through factors associated with the image (e.g. a tattoo, or an identifiable body mark) then arguably the depicted individual is identifiable for purposes of this law. The depicted individual could also be identified by information displayed in connection with the image or video, such as a post with the name, address, phone number, or other personally identifying information of the depicted individual.

(g) Reasonable Expectation of Privacy

Under N.Y. Penal Law 245.15, the depicted individual must have “a reasonable expectation that the image would remain private and the actor knew or reasonably should have known the person depicted intended for the still or video image to remain private, regardless of whether the actor was present when the still or video image was taken.” Arguably, if a photo or video was taken and/or sent in the context of a romantic relationship between depicted individual and perpetrator, this element would be satisfied.

2. *Deep Fake Provision – Pending Governor’s Signature*

At the time this Fourth Edition of the Manual is being published (July 2023), an amendment to N. Y. Penal Law 245.15 regarding “deep fakes” has passed both the Assembly and the Senate but has not yet been signed into law by the Governor. Advocates anticipate it will be signed and will become law on the “sixtieth day after it shall have become a law.”

The new amendment to N. Y. Penal Law 245.15 would broaden the images covered by the Unlawful Dissemination law to include those “**created or altered by digitization, where such person may be reasonably identified.**”⁴⁷ For the purposes of this bill, “digitization” means “**to alter an image in a realistic manner utilizing an image or images of a person, other than the person depicted, or computer-generated images.**”⁴⁸

Because this change will update the already existing Unlawful Dissemination statute, advocates interpret this amendment as an extension to the definition of “Unlawful

⁴⁶ *Id.*

⁴⁷ https://nyassembly.gov/leg/?default_fld=%0D%0A&leg_video=&bn=S01042&term=2023&Summary=Y&Actions=Y&Floor%26nbspVotes=Y&Memo=Y&Text=Y (last viewed July 9, 2023).

⁴⁸ *Id.*

Dissemination” as a family offense under the Family Court Act. This means that a petitioner who meets the statutory requires of N. Y. Penal Law 245.15, which now includes “deep fakes” will be able to petition the Family Court for an order of protection. For a discussion on the new family offense that is expected to be created under the law, please see Part 2, Section I. Family Court Orders of Protection, *infra*. For a discussion of the civil provision of the law, please see Part 2, Section II. New York State and New York City Civil Causes of Action, *infra*.

3. *Exceptions to the law*

There are four primary exceptions to when and where the NY CPL 245.15 applies.

(a) Reporting of Unlawful Conduct and Law Enforcement Exception

Section 245.15 does not apply to “the reporting of unlawful conduct”⁴⁹ or “dissemination or publication of an intimate image made during lawful and common practices of law enforcement, legal proceedings or medical treatment.”⁵⁰ 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 N.Y. Penal Law 245.15. Similarly, if law enforcement sends the photo internally or collects the photo as a part of their law enforcement duties, this disclosure would not violate the law.

(b) Communications Decency Act (CDA) Section 230

Section 245.15 notes, “Nothing in this section shall be construed to limit, or to enlarge, the protections that 47 U.S.C § 230 confers on an interactive computer service for content provided by another information content provider, as such terms are defined in 47 U.S.C. § 230.”⁵¹ 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 or applications (i.e., Facebook, Grindr, Craigslist, and others). There is currently no liability for the content provider, only for the individuals posting on the websites or applications.

(c) Dissemination or publication of an intimate image made for a legitimate public purpose

“Dissemination or publication of an intimate image made for a legitimate public purpose”⁵² does not violate N.Y. Penal Law 245.15. Similar to the New York City law, this exception should be interpreted narrowly only to include intimate images or videos that have important public concern.

⁴⁹ N.Y. Penal Law § 245.15 3.(a).

⁵⁰ N.Y. Penal Law § 245.15 3.(b).

⁵¹ *Id.* at 4.

⁵² *Id.* at 3.(d).

(d) Voluntary exposure in a public or commercial setting

“Images involving voluntary exposure in a public or commercial setting⁵³” are not covered by Section 245.15. For example, if an image was taken of the topless New York Desnudas⁵⁴ in Times Square, then Section 245.15 would not apply to that image.

C. Differences between NY State and NY City Laws

Intent

- Intents are similar but the state law is slightly less burdensome as there is no substantial emotional harm qualifier in the state law.

Receipt of the Image

- N.Y. Admin. Code 10-180 contains a requirement that the person being prosecuted be a “covered recipient,” which means that the perpetrator gained access to the intimate image either by having received it directly from the depicted individual or have recorded it themselves. Therefore, someone who distributed or disseminated an intimate image, who did not receive it from the depicted individual or record it themselves, cannot be prosecuted under N.Y. Admin. Code 10-180.
- N.Y. Penal Law 245.15 has no such restriction – it simply states that the actor needs to have known, or reasonably should have known, that the depicted person intended for the image to remain private, regardless of whether the actor was present when the image was taken. Under the state law then, a perpetrator who distributed or disseminated an intimate image, that knew or reasonably should have known, that the depicted individual intended for the image to remain private, could be prosecuted under the state law, even if they did not gain access to the image by recording it themselves or having received it from the depicted individual.

Threat Provision

- Threats to disseminate images are only explicitly criminalized under the city law, N.Y. Admin. Code 10-180.

Identifiability

- N.Y. Admin. Code 10-180 requires that the depicted individual is or *would be* identifiable to another individual either from the intimate image or from the circumstances under which such image is disclosed.

⁵³ N.Y. Penal Law § 245.15 3.(c).

⁵⁴ See, e.g., Colleen Wright, *The Desnudas of Times Square, Topless but for the Paint*, N.Y. TIMES (August 14, 2015), available at <https://www.nytimes.com/2015/08/16/nyregion/the-desnudas-of-times-square-topless-but-for-the-paint.html>.

- N.Y. Penal Law 245.15 does not have the *to another individual* provision, it only requires the depicted individual “is identifiable from the image itself or from information displayed in connection with the image.”⁵⁵

Intent to Remain Private

- Under N.Y. Penal Law 245.15, the perpetrator needs to have known or reasonably should have known that the person depicted had a reasonable expectation that the image would remain private. *See supra*.
- Under N.Y. Admin. Code 10-180, the image that is being distributed and/or disseminated, or being threatened to be disseminated/distributed, must be one that has been disclosed or threatened to be disclosed 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.

Public Place

- Unlike the New York city law, there is no “public place” exception for the NY state law.

(New as of 2023! Pending Governor signature) Deep Fake or “Digitized Image” Provision

- As described above, the legislature amended N.Y. Penal Law 245.15 in June 2023 (pending the Governor’s signature) to include harms caused by “digitized” images, where the intimate image depicts an image or video that was altered to appear as the depicted person – but in fact is not the depicted person.
- N.Y. Admin. Code 10-180 does not contain language that covers deep fakes or “digitized” images.

D. Suffolk County Criminal Law

On December 17, 2018, Suffolk County signed a bill similar to New York City’s Unlawful Disclosure Law that makes sharing revenge porn a misdemeanor punishable up to a year in jail and \$1,000 fine. The Suffolk County Unlawful Disclosure Law also holds violators subject to civil penalties, holding them liable for compensatory damages, punitive damages, and attorney’s costs and fees.⁵⁶

E. Nassau County Criminal Law

On February 25, 2019 Nassau County voted to pass a bill similar to the one of Suffolk County. The law makes non-consensual disclosure of intimate images (revenge porn) a misdemeanor punishable with up to one year in jail, \$1000 fine and other civil penalties.⁵⁷

⁵⁵ N.Y. Penal Law § 245.15 1.(a).

⁵⁶ See <https://www.longislandpress.com/2018/12/18/suffolk-makes-revenge-porn-a-crime/>.

⁵⁷ See <https://www.longislandpress.com/2019/02/26/nassau-pols-pass-revenge-porn-bill/>.

F. Common New York Penal Code Provisions Addressing Tech Abuse

Since New York State’s new IBSA law was only passed relatively recently, prosecutors formerly deployed a mixture of criminal laws to address behavior like stalking, coercion, witness tampering and harassment in the context of IBSA, which are still useful today.⁵⁸ There may be circumstances where the elements of the unlawful dissemination statutes may not be met. However, the below listed sections of the New York State Penal Code could potentially address tech abuse and image-based sex abuse, depending on the specific facts of the case. Each statute will be described in term.

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*
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 — N.Y. Penal Law §§ 250.45, 250.50*

“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.⁵⁹ 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.”⁶⁰ Dissemination of an

⁵⁸ See, e.g. *People v. Barber*, 992 N.Y.S.2d 159 (N.Y.C. Crim. Ct. N.Y. Cty. 2014) Defendant 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 IBSA, 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.” The case was dismissed.

⁵⁹ N.Y. Penal Law § 250.45.

⁶⁰ *Id.*

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. However, if the elements are met, Unlawful Surveillance is a serious crime in New York, constituting a Felony.

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 IBSA, 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 post, which means that stand-alone incidents of IBSA would likely not fall under this section of the penal code.

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

A person is guilty of coercion in the second degree when the person either: “compels or induces [the victim] to engage in conduct which [the victim] has a legal right to abstain from engaging in, compels or induces [the victim] to abstain from engaging in conduct in which he or she has a legal right to engage in ,or compels or induces [the victim] to join a group, organization or criminal enterprise which [the] person has a right to abstain from joining in”⁶¹

Importantly, the statute requires that the defendant have compelled or induced 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, including, but not limited to: “causing physical injury to a person;” “causing damage to property;” accusing a person of a crime or causing criminal charges to be instituted against him or her, “[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;” testifying or providing information, or withholding testimony or information, “with respect to another’s legal claim or defense;” performing “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;” or any other conduct that constitutes a crime.⁶²

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

⁶¹ N.Y. Penal Law § 135.60.

⁶² N.Y. Penal Law §§ 135.60.

with the abuser, does not come back to the abuser, does not give the abuser custody of their shared child, or does not engage in sexual activity with other persons for money. 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*

A person is guilty of stalking in the fourth degree, P.L. § 120.45, when he or she intentionally and for no legitimate purpose, engages in a “course of conduct,” directed at a specific person, that he or she knows or reasonably should know that such conduct:

(1) is likely to cause reasonable fear of material harm to the “physical health, safety, or property of such person, a member of such person’s immediate family, or a third party with whom such person is acquainted;”⁶³

(2) “causes material harm to the mental or emotional health of such person, where such conduct consists of following, telephoning, initiating communication or contact with such person, a member of such person’s immediate family, or a third party with whom such person is acquainted, *and the actor was previously clearly informed to cease the conduct;*”⁶⁴ or

(3) “is likely to cause such person to reasonably fear that his or her employment, business or career is threatened, where such conduct consists of appearing, telephoning or initiating communication or contact at such person’s place of employment or business, and the actor was previously clearly informed to cease that conduct.”⁶⁵

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.”⁶⁶ While the “course of conduct” must be directed at harming the victim, such conduct can include harmful communications made to third parties.⁶⁷

It is important to note that for a defendant to be prosecuted under subsection (2) or (3) of P.L. 120.45, they must have been previously informed to cease the conduct. Such a requirement is not necessary for a prosecution under subsection (1), however, that subsection requires that the conduct be “likely to cause reasonable fear of material harm” to the physical health of the victim, their family, or a third party with whom they are acquainted. *See supra*.

Where an abuser has engaged in repeated acts of threats to post or release intimate images, stalking may be applicable. IBSA may also fall under subsection (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” (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

⁶³ N.Y. Penal Law § 120.45(1).

⁶⁴ N.Y. Penal Law § 120.45(2) (emphasis added).

⁶⁵ N.Y. Penal Law § 120.45(3).

⁶⁶ *People v. Payton*, 161 Misc. 2d 170 (N.Y.C. Crim. Ct. Kings Cty. 1994).

⁶⁷ *See* N.Y. Penal Law § 120.45(2).

victim's standing in the community). Additionally, stalking may be an applicable crime in cases where a person is repeatedly communicating with a victim, via online platforms, e-mail, etc.

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. This type of conduct may also be able to be prosecuted under the coercion statute. *See* P.L. 135.60.

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.

G. Supporting Victims of Tech Abuse Who Report to Law Enforcement (New York)

Victims of tech 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 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 tech abuse who are considering reporting and/or who choose to report their abuse to law enforcement.

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

It is important to discuss with your client the pros and cons of reporting tech 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.

Obtaining a Criminal Order of Protection

Obtaining an order of protection is a key benefit to reporting tech 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. Although New York advocates have not found this provision to be 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. *See infra* for sample language in the Index.

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 New York 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 previously in an intimate relationship.⁶⁸ Civil orders of protection are explored in much more detail in [Section I of Part 2- Civil Legal Remedies for Victims of IBSA](#). 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.⁶⁹

⁶⁸ *See* N.Y. Family Court Act § 812.

⁶⁹ 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.

Keep in mind that due to the jurisdictional restraints of Family Court: if the tech abuse did not occur in the context of a covered relationship for Family Court jurisdiction, then pursuing a criminal case will be your client's only option to secure an order of protection.

Control of the Case

Once your client reports the tech abuse, the police and the District Attorney's office will decide how to move the case forward, if at all. If they are interested in having the criminal case progress, advocates and clients can 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 (often referred to as “evidence-based prosecution”). 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. 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 criminal 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 ICE⁷⁰ 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

⁷⁰ 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>.

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.

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 tech 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 a venue 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.

Helping Your Client Report Tech Abuse

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

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 tech 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.

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 tech abuse.⁷¹

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 tech abuse cases. When a complaint of domestic violence/tech 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

⁷¹ *Family Justice Centers*, MAYOR'S OFFICE TO END GENDER-BASED VIOLENCE, <https://www.nyc.gov/site/ocdv/programs/family-justice-centers.page> (last visited July 18, 2023)

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 tech abuse to the NYPD.

Special Victims Unit, Family Court Division, New York City Law Department, Office of the Corporation Counsel. The Office of the Corporation Counsel investigates, and prosecutes where appropriate, matters involving youth between the ages of 7 and 17 years old who have been arrested for juvenile delinquency offenses (misdemeanors and felonies) and referred to the Law Department for prosecution in Family Court. Further, juveniles 16- and 17-years of age arrested for any misdemeanor offense (including any misdemeanor sex offenses) will automatically be treated as a juvenile, the matter will be handled by the Family Court, and their cases will be assigned to an attorney.

Any 16- and 17-year-old arrested for a felony (including sex offenses) is considered an Adolescent Offender (AO) and is subject to the jurisdiction of the Youth Part in Supreme Court where the case is prosecuted by the county's District Attorney's Office. Youth arrested for felony offenses may also be treated as juveniles but are subject to initial processing in the Youth Part as Adolescent Offenders. Transfer or removal to the Family Court from the Youth Part will depend on the severity of the felony charges and other factors considered by the court. Adolescent Offenders whose cases are removed from the Youth Part in Supreme Court to Family Court will then be considered Juvenile Delinquents. One of the relevant factors that can result in a case remaining in the Youth Part is if the Respondent is alleged to have engaged in unlawful sexual conduct. Another factor may be the existence of extraordinary circumstances in the particular case.

Some juveniles 14- and 15-years of age who are arrested for certain violent felonies (including sex offenses) are considered Juvenile Offenders (JO) and are also subject to the jurisdiction of the Youth Part in Supreme Court. Removal to the Family Court from the Youth Part will depend on an analysis of several "interest of justice" factors. These factors include, but are not limited to, whether or not the youth used a firearm or deadly weapon, whether the offense was a sex crime, or whether or not the youth caused significant physical injury. In sexual offense cases and cases involving image-based sex abuse, the Office of the Corporation Counsel often works with the District Attorney's office to coordinate the handling of the case. In general, the Office of the Corporation Counsel receives cases after an arrest has been made but is sometimes involved in pre-arrest investigations with the police department.

Once a youth is arrested and before a case is referred to the Law Department, the law allows for the Department of Probation to address the case through what is termed adjustment services. Adjustment services are an early means of resolving a case outside of the court system. Survivors should expect a phone call from a probation officer asking their opinion regarding adjustment of the delinquency case. This means that the probation officer will ask whether the survivor is seeking court intervention, or whether they would like for the youth to be offered services outside of court. However, the decision to adjust a case lies solely with the Department of Probation. If a case is not "adjusted" the Department of Probation refers the case to the Law Department for investigation and prosecution.

The Special Victims Unit (“SVU”) within the Family Court Division of the NYC Law Department, Office of the Corporation Counsel, is comprised of specialized attorneys called Assistant Corporation Counsels (ACCs), victim advocates, and investigators, who handle any juvenile arrested for and charged with an Article 130 sexual offense and any case involving teen dating violence or intimate partner abuse, including crimes such as stalking and dissemination of intimate images. Like most of the DA’s offices, our office is one of vertical prosecution so the same Assistant Corporation Counsel should handle the case from beginning to end (barring any change in employment). SVU attorneys are uniquely qualified to handle and investigate these sensitive cases, from pre-arrest investigations to interviewing and taking statements from child, teen and adult victims to final disposition. Further, SVU attorneys are certified in forensic interviewing of children. Complaining witnesses in juvenile delinquency proceedings can receive orders of protection just as they would in Criminal or Supreme Court and our Office’s victim advocates will assist them with any service referrals they may need.

Similar to the District Attorney’s office, during the initial investigation of the case, your client should expect the ACC to want to spend at least an hour, if not more, with them to discuss the facts of the case, gather evidence, assess their credibility, and discuss possible outcomes. In order to proceed with a juvenile delinquency case, the ACC will need to take a supporting deposition from the complainant. This document states the facts of the incident in order to support the charges. In order to proceed, the ACC will have to prove the case beyond a reasonable doubt, as in the adult system. However, unlike Criminal and Supreme Court, there are no jury trials in juvenile delinquency proceedings held in Family Court. Juvenile delinquency hearings and fact-findings are instead heard by the assigned judge at a bench trial. Additionally, the speedy trial time-frames in delinquency proceedings are expedited. Your client should expect the case to proceed to trial within 60 days (unless there is a waiver of speedy trial) on cases where the juvenile is paroled and in either 3 or 14 days if the juvenile is remanded. Because of these timeframes, it is essential that your client stay in contact with the ACC.

The Family Court system is meant to be rehabilitative, not punitive. The process seeks to ensure that youth who commit offenses that would be considered crimes if they were adults are held accountable for their actions and receive services that will contribute to their rehabilitation. It is at the dispositional phase (similar to sentencing) when a judge determines if a juvenile requires supervision, treatment or confinement. There are a number of different options for a juvenile at this stage, including but not limited to, supervision by the Department of Probation for a period of up to 24 months, which can include curfew checks and mandated enrollment in services. Some services relevant to sex offenses and/or image-based sex abuse include Problematic Sexual Behavior therapy or participation in programs focused on teen dating violence and internet abuse. Another possibility during the dispositional phase is placement of a juvenile in a facility away from home, such as a group home or a secure facility, depending on the needs of the juvenile, for a period of up to 18 months. Dispositions may differ based on whether the youth has a finding to a misdemeanor or felony offense, but there are no crime specific sentences that are found in the adult system.

Preparing to Report

Unfortunately, tech abuse crimes 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 tech 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 tech 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 tech 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 tech 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 tech 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 Unlawful Dissemination which is described in more detail in Part 1-Criminal Legal Remedies for Victims of IBSA, Section I.A., and which makes Unlawful Dissemination 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 IBSA 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 tech abuse or image-based sex abuse (“IBSA”). In an effort to fill the current gap in federal and state law, victims of tech 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 criminal laws that could potentially be used to combat tech abuse at the federal level. In Part III., infra, the Manual will cover the newly created Federal civil cause of action relating to Unlawful Dissemination.

A summary of caselaw interpreting these sections is included in the Appendix, *infra*.

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.⁷² While it may seem obvious that computers connected to the Internet are “used in or affecting interstate or foreign commerce or communication,”⁷³ this jurisdictional element still needs to be established by the evidence.

⁷² See 18 U.S.C. § 1030(c)(2)(B)(ii).

⁷³ 18 U.S.C. § 1030(e)(2)(B)

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 identity theft will receive a two-year term of imprisonment to run consecutively with the sentence imposed for other offenses.⁷⁴

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

As discussed *infra* at Part 2-Civil Legal Remedies for Victims of IBSA 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.⁷⁵

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 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.⁷⁶

A person violates § 875(d) “if he transmits a communication containing any threat to injure the reputation of a person with intent to extort a ‘thing of value’ from that person.”⁷⁷ In his motion to dismiss count two, the defendant argued that he could not have demonstrated the requisite intent to extort because a request to drop out of an election was not a “thing of value.” Rejecting this argument, the court determined that under § 875(d), a “thing of value” could include tangible or intangible things, and that “the focus of the . . . term is to be placed on the

⁷⁴ 18 U.S.C. § 1030.

⁷⁵ See 18 U.S.C. § 2511(4)(a).

⁷⁶ See 18 U.S.C. § 2261(b).

⁷⁷ *United States v. Hobgood*, 868 F.3d 744, 747 (8th Cir. 2017).

value which the defendant subjectively attaches” to what he seeks.⁷⁸ For example, a sexual relationship may be an intangible thing of value under § 875(d).⁷⁹ The defendant’s belief that his victim would not make a good candidate for office and his threats to embarrass his ex-wife and the victim’s other family member demonstrated that the victim’s candidacy was a “thing of value” to him.

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.

F. Obscene or Harassing Telephone Calls in Interstate or Foreign Communications, 47 U.S.C. § 233

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).

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 jurisdiction-less 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.

18 U.S.C. § 2422(b) (2021) makes it a criminal offense to use the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States, to knowingly persuade, induce, entice, or coerce a minor to engage in, *inter alia*, any sexual activity for which any person can be charged with a criminal offense. Any person who does so or attempts to do so shall be fined and imprisoned for a minimum of ten years or for life.

⁷⁸ *Id.* (quoting *United States v. Petrovic*, 701 F.3d 849, 858 (8th Cir. 2012)).

⁷⁹ *United States v. Petrovic*, 701 F.3d 849, 858 (8th Cir. 2012).

PART 2: CIVIL REMEDIES FOR VICTIMS OF TECH ABUSE

I. Civil Orders of Protection – New York

Victims of tech 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.⁸⁰ A victim does not need to go to the police and make a report before seeking a civil order of protection. They can initiate the process themselves (or with an attorney) by filing a Family Offense Petition in court. The following section describes the requirements and the process for seeking a civil order of protection.

1. Jurisdiction: Determining Who can File for a Civil Order of Protection in Family Court.

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 formerly, 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.

In determining whether a relationship is an “intimate relationship,” courts consider factors such as 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. 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.

2. Family Offenses

In order to obtain an order of protection, the petitioner needs to allege at least one family offense in their petition. The Family Court Act defines a family offense as: acts which would constitute disorderly conduct, unlawful dissemination or publication of an intimate image, 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,

⁸⁰ A civil protective order may also be obtained in New York Supreme Court as part of a divorce already pending there.

grand larceny in the fourth degree, grand larceny in the third degree or coercion in the second degree”⁸¹

In other words, the Family Court Act designates certain crimes from the penal code as family offenses, providing a basis for seeking a civil order of protection in Family Court. New York State’s relatively new Unlawful Dissemination law establishes N.Y. Penal Law 245.15, “unlawful dissemination or publication of an intimate image” (hereinafter “Unlawful Dissemination”) as a family offense. *See infra* Part 1, Criminal Legal Remedies for Victims of IBSA, Section I.A, thereby allowing a petitioner to secure a civil order of protection if they can meet the elements (discussed above) of N.Y. Penal Law 245.15.

Additionally, the Unlawful Dissemination experienced by the victim may qualify as one or more other family offenses, such as harassment, coercion, stalking, or a sexual offense. For example, if an abuser repeatedly threatens to disclose intimate images, or actually does post images repeatedly, their 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.

3. *Procedure for Obtaining a Civil Order of Protection (“OP”)*

a. Venue.

A petitioner seeking a civil order of protection may go to the New York Family Court in the county or borough: 1) where the victim lives, 2) where the abuser lives, or 3) where the abuse took place. If the abuse is solely cyber, the place of abuse can be the borough where the images, digital threats, etc. originated (if known) and the borough in which they were received and where the harm occurred.

b. Jurisdiction

Given the virtual nature of cyber abuse it is possible that an abuser lives outside of New York and the harmful activity is originating outside of New York. This may result in perpetrators arguing that New York does not have jurisdiction for the order of protection case. That is not correct. **If the harm occurred in New York and/or the victim lives in New York, the family offense petition can be filed in New York.**

PRACTICE TIP: Since the COVID-19 pandemic, parties are now typically able to file a Family Offense Petition through the Electronic Document Delivery System (“EDDS”) and request to appear virtually via Microsoft Teams video conference. Check with the appropriate

⁸¹ N.Y. Fam. Ct. §812(1); *see also* N.Y. Penal Law 245.15.

venue to determine if virtual appearance is available, so you can present your client with the option.

c. First Day of Court: Filing *Ex Parte* Petition in Pursuit of a Temporary OP.

To initiate an order of protection case the victim or advocate should go to the petition room of the appropriate Family Court and file a Family Offense Petition that alleges at least one family offense.⁸² Virtual filing is also available in many boroughs and counties due to the COVID-19 pandemic.⁸³

If the victim does not have attorney assistance, they will get limited *pro se* assistance from the petition room clerk, who should help them create and file a family offense petition. The victim must include as much detail as possible in the petition about the incidents of abuse, including details about the tech abuse and approximate dates that incidents happened (*see* Appendix for a sample Family Offense Petition including language addressing technology-facilitated abuse). Upon completing the petition, petitioners will make an *ex parte* appearance before an intake judge where they will ask the judge to issue a Temporary Order of Protection. The judge should grant the request for the Temporary Order of Protection directly from the bench on the same day if good cause is shown.

Available Relief

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:

- 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, including through third-parties;
- refrain from committing any family offenses against the victim.

In cases where the petition alleges tech abuse, family court adjudicators should 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 (e.g., “stay away” provisions), law enforcement officials often do not consider tech abuse to be a violation of the Order of Protection.

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

⁸² Petitioners 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.

⁸³ Electronic Document Delivery Service, NY STATE COURTS, <https://iappscontent.courts.state.ny.us/NYSCEF/live/edds.htm> (last visited July 18, 2023).

should be made both in writing in the petition and orally at the appearance before the judge. Examples include:

- **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 tech abuse specific language are included in this Manual in the Appendix.

Prior to the adoption of the Unlawful Dissemination family offense, some Family Court judges were resistant to including these tech abuse-specific protections. To the extent a judge continues to resist including this type of protective language in an order of protection, the advocate or victim should be prepared to respectfully remind the judge that Unlawful Dissemination is now an enumerated family offense and therefore protective provisions related to that offense are highly relevant and appropriate. Advocates/victims can also point to the court’s authority to craft appropriate protective provisions related to tech abuse, including:

- Section 842(c) of the Family Court Act, which allows the Court to enter an Order of Protection ordering a respondent to “refrain from harassing, intimidating or threatening” conduct; and
- Section 842(k) of the Family Court Act, which states that the Court may require a respondent “to observe such other conditions as are necessary to further the purposes of protection.”⁸⁴

Based on this authority, and the inclusion of Unlawful Dissemination as an enumerated family offense, numerous family court judges have been willing to include the IBSA-specific provisions in both temporary and final orders of protection.

Continuing the Case

Following the initial *ex parte* appearance, in addition to deciding whether to grant a Temporary Order of Protection and what relief to include therein, the Judge will issue a summons for the abuser to appear in court on a specific date. The abuser must be served with the summons, Family Offense Petition, and Temporary Order of Protection at least 24 hours before the next set court date. When the respondent’s address is known, the court will typically send these papers directly to the Sheriff who will serve the Respondent without a fee.

⁸⁴ 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.”)

PRACTICE TIP: Before leaving the *ex parte* appearance you should confirm with the Court that the Court will be sending the papers to the Sherriff's office for service.

On the next 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 offenses alleged 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 established by the petitioner.⁸⁵

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 tech abuse from the beginning is crucial. (*See* [Part 4- Evidence Collection](#)).

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

A. New York City Civil Causes of Action

As discussed *supra* at [Criminal Legal Remedies for Victims of IBSA 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 Unlawful Dissemination for damages and other 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.”⁸⁶ A civil suit under this section does not preclude the victim from also seeking criminal justice remedies for the same behavior.⁸⁷ 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 may pass similar laws that create specific causes of action for Unlawful Dissemination victims.⁸⁸

At least two civil lawsuits have been filed under the New York City Unlawful Disclosure Law. Both cases raised claims against both an individual and a corporation. In both cases, the

⁸⁵ 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.

⁸⁶ NYC Administrative Code 10-180 §d.

⁸⁷ *See id.*

⁸⁸ *See* [IR 1756-2018](#). A Suffolk County 2018 Resolution prohibiting the disclosure of intimate images, which closely resembles the NYC law.

complaints against the corporations were dismissed, because the text of the law does not allow for the company to be considered a “covered recipient, as presently defined.”⁸⁹

In *Waterbury v. New York City Ballet, Inc.*, the claim against the individual who distributed the intimate images was permitted to proceed.⁹⁰ In this case, the individual defendant Finlay secretly recorded, saved, and shared photographs and videos of romantic partner, plaintiff Waterbury, without clothing and engaging in sexual activity with him. While Finlay was employed by the NYC Ballet (NYCB) and Waterbury was a student of the School of American Ballet, Finlay shared these images with coworkers along with lewd text messages. Waterbury brought suit against NYC Ballet for its “fraternity-like environment that allowed, condoned, encouraged, and permitted its male dancers to abuse, assault, degrade, demean, dehumanize, and mistreat its female dancers and other women.”⁹¹ The court allowed the NYC Unlawful Disclosure claim against Finlay to proceed, but dismissed the claim against NYC Ballet, as it did not meet the definition as a “covered recipient.”⁹²

In *Litwin v. Hammond Hanlon Camp, LLC*, both plaintiff Litwin and defendant Michael Hammond were employed by Hammond Hanlon Camp, LLC (HHC) when entering into a romantic relationship where plaintiff shared intimate images with Michael Hammond, instructing him the images were for him alone. After the relationship terminated, Michael Hammond sent the images to his brother and defendant Gregory Hammond, who then proceeded to widely distribute the images to HHC employees “via a known channel of HHC communications.”⁹³ Plaintiff brought suit against Michael Hammond, Gregory Hammond, and HHC under the NYC Unlawful Disclosure Law. Relying on legislative intent, the court determined that the NYC Unlawful Disclosure Law does not afford Plaintiff a remedy against Gregory Hammond nor HHC, neither of whom received the images directly from Plaintiff.⁹⁴ As Michael Hammond is included in the definition of a covered recipient under the law, the claim against him was allowed to proceed to summary judgement.

B. New York State Civil Causes of Action

New York State civil cause of action for Unlawful Dissemination.

New York passed legislation permitting a civil cause of action for victims of Unlawful Dissemination. The new legislation, A5981/A1719, went into effect on September 21, 2019, and permits a victim to file a civil lawsuit against the individual who posted the content⁹⁵. To file a civil suit, the victim must meet the following elements:

⁸⁹ NYC Administrative Code 10-180 §a. See *Litwin v Hammond Hanlon Camp, LLC*, 2019 NY Slip Op 51475 (N.Y. Sup. Ct. 2020); see also *Waterbury v New York City Ballet, Inc.*, 2020 NY Slip Op 33132 (N.Y. Sup. Ct. 2020).

⁹⁰ *Waterbury v New York City Ballet, Inc.*, 2020 NY Slip Op 33132 (N.Y. Sup. Ct. 2020).

⁹¹ *Id.* at 6 (internal quotation marks omitted).

⁹² NYC Administrative Code 10-180 §d.

⁹³ *Litwin at 1.*

⁹⁴ See New York City Council, Committee on Public Safety, Report of the Governmental Affairs Division on Proposed Int. No. 1267-A, Nov. 1 2017 at 10 (“the prohibition does not cover an individual who received or accesses an intimate image indirectly” and “the prohibition would not cover an individual who was sent an intimate image from a friend who received that image from the depicted individual”).

⁹⁵ See N.Y. Civ. R. §52-b 1.

- (a) Disseminate or Publish OR Threaten to Disseminate or Publish a still or video image. Similar to N.Y. Penal Law 245.15., N.Y. Civil Rights Law 52-b requires that the perpetrator “disseminate or publish,” a still of video image of the depicted individual. Importantly, the civil cause of action also applies to perpetrators who *threaten* to disseminate or publish such image or video.⁹⁶
- (b) For the Purpose of Harassing, Annoying, or Alarming Such Person. Critically, N.Y. Civil Rights Law 52-b has a less onerous intent requirement than N.Y. Penal Law 245.15 – it only requires that the perpetrator have disseminated or published an image, or threatened to do so, “for the purpose of harassing, annoying or alarming such person.”⁹⁷
- (c) Intimate Part. Under N.Y. Civil Rights Law 52-b it is unlawful to disseminate a still or video image depicting “an unclothed or exposed intimate part of such other person; or such other person engaging in sexual conduct”⁹⁸ with another person without the individual’s consent.
- (d) Without Consent. The law applies where a perpetrator disseminates or publishes an image, OR threatens to do so, without the depicted individual’s consent. Where a depicted individual did not intend for a photo to be disseminated or published at the time the image was taken or sent (even if the depicted individual consented to the actual taking of the image), N.Y. Civil Rights Law 52-b applies. It is critical to note that the consent is at the point of *dissemination*, not the point of the video recording or taking of the photograph. Therefore, even if the depicted individual consented to the taking of the photo itself (i.e. took a naked selfie and sent it to the perpetrator), that does not mean the depicted individual consented to the photo being disseminated or published.

There are four primary exceptions to when and where the law applies.

- (a) Reporting of Unlawful Conduct and Law Enforcement Exception — The law does not apply to “the reporting of unlawful conduct”⁹⁹ or “dissemination or publication of an intimate image made during lawful and common practices of law enforcement, legal proceedings or medical treatment.”¹⁰⁰ 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 N.Y. Penal Law 245.15. Similarly, if law enforcement sends the photo internally or collects the photo as a part of their law enforcement duties, this disclosure would not violate the law.
- (b) Communications Decency Act (CDA) Section 230— The law notes, “Nothing in this section shall be construed to limit, or to enlarge, the protections that 47 U.S.C § 230 confers on an interactive computer service for content provided by another information content provider, as such terms are defined in 47 U.S.C. § 230.”¹⁰¹ This exception merely restates

⁹⁶ *Id.*

⁹⁷ *Id.*

⁹⁸ *Id.* at 1.b.

⁹⁹ N.Y. Civ. R. §52-b 3.a.

¹⁰⁰ N.Y. Civ. R. §52-b 3.b.

¹⁰¹ *Id.* at 10.

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

- (c) Dissemination or publication of an intimate image made for a legitimate public purpose — “Dissemination or publication of an intimate image made for a legitimate public purpose”¹⁰² does not violate N.Y. Penal Law 245.15. similar to the New York City law, this exception should be interpreted narrowly only to include intimate images or videos that have important public concern.
- (d) Voluntary exposure in a public or commercial setting — “Images involving voluntary exposure in a public or commercial setting¹⁰³” are not covered by this law. For example, if an image was taken of the topless New York Desnudas¹⁰⁴ in Times Square, then this law would not apply to that image.

Plaintiffs bringing the suit under the law are not required to file a criminal complaint in order to maintain their civil lawsuit¹⁰⁵. Finally, a image-based sex abuse victim can seek a court-ordered injunction to have the image(s) or video(s) removed from a website,¹⁰⁶ a provision that is a first in the nation.¹⁰⁷

For the civil actions, a victim can file one no later than three years after the dissemination or publication of an image or one year from the date a person discovers the image had been distributed or posted online¹⁰⁸.

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.

Intentional Infliction of Emotional Distress (“IIED”)

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

1. extreme and outrageous conduct;
2. intent to cause, or disregard of a substantial probability of causing, severe emotional distress;
3. a causal connection between the conduct and injury; and
4. severe emotional distress.

¹⁰² *Id.* at 3.d.

¹⁰³ *Id.* at 3.c.

¹⁰⁴ See, e.g., Colleen Wright, *The Desnudas of Times Square, Topless but for the Paint*, N.Y. TIMES (August 14, 2015), available at <https://www.nytimes.com/2015/08/16/nyregion/the-desnudas-of-times-square-topless-but-for-the-paint.html>.

¹⁰⁵ N.Y. Civ. R. §52-b 7.

¹⁰⁶ N.Y. Civ. R. §§52-b 4., 5.

¹⁰⁷ See, e.g., April Glaser, *New York's New Revenge Porn Bill Is a Bittersweet Victory*, SLATE (July 25, 2019), available at <https://slate.com/technology/2019/07/revenge-porn-law-new-york.html>

¹⁰⁸ N.Y. Civ. R. §52-b 6.

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”.¹⁰⁹ Note, however, that it 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.”¹¹⁰ Moreover, IIED is unavailable where damages resulting from the conduct at issue are available via another recognized tort.¹¹¹

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:

1. breach of the duty of care; and
2. breach of the duty of care results directly in the emotional harm.

Unlike IIED, NIED does not require “extreme and outrageous” conduct.¹¹² 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.”¹¹³ Identifying a duty that was breached appears to be the biggest hurdle in bringing an NIED claim in image-based sex abuse cases, as there is no common-law right to privacy in New York.¹¹⁴ However, an NIED claim may be premised on a statutory duty.¹¹⁵ 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.¹¹⁶ The court found that the owner 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.¹¹⁷

¹⁰⁹ *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).

¹¹⁰ *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).

¹¹¹ *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”).

¹¹² *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”).

¹¹³ *Id.*

¹¹⁴ *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”).

¹¹⁵ *See id.*

¹¹⁶ *See id.*

¹¹⁷ *See id.*

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 image-based sex abuse.

III. Federal Causes of Action

A. NEW (2022) Civil Cause of Action for Disclosure of Intimate Images

In 2022, the Violence Against Women Act was amended to add a federal civil cause of action for dissemination of an intimate image without consent to such dissemination. The new legislation, codified at 15 U.S.C. § 6851, took effect on October 1, 2022, and permits a victim to file a civil lawsuit against the individual who posted the content.¹¹⁸

This action provides strong relief, including statutory damages of \$150,000 in addition to attorneys' fees, as well as injunctive relief against perpetrators (though not platforms) and use of pseudonyms. Further, the statute covers a broader range of conduct than some state or local actions, to include perpetrators who act not just knowingly but also with reckless disregard for lack of consent to dissemination, and it prohibit imputing consent to subsequent dissemination from the victim's prior consent to initial creation or voluntary initial dissemination. Moreover, the law's exceptions and carve-out appear narrowly tailored.

However, one weakness of the federal civil action relative to the New York City law is that the federal statute does not prohibit mere threats to disseminate absent actual dissemination.

Following are summaries of the claim elements, damages and other relief, and exceptions:

1. Elements of the Law

(a) Disclosure. The law requires that the victim's intimate visual depiction "is disclosed" by the perpetrator.¹¹⁹ The statute provides that " 'disclose' means transfer, publish, distribute, or make accessible."¹²⁰

(b) Intimate Visual Depiction. The law requires the disclosure at issue to be of the victim's "intimate visual depiction."¹²¹ The statute provides that "'intimate visual depiction'

¹¹⁸ See "Federal Civil Action for Disclosure of Intimate Images: Free Speech Considerations," Cong. Research Svc. (Apr. 1, 2022), *available at* <https://crsreports.congress.gov/product/pdf/LSB/LSB10723#:~:text=Effective%20October%201%2C%202022%2C%20Section, person%20who%20made%20the%20disclosure>

¹¹⁹ 15 U.S.C. § 6851(b)(1)(A).

¹²⁰ *Id.* § 6851(a)(4). The statute does not define the terms "transfer," "publish," "distribute," or "make accessible." *Id.*

¹²¹ 15 U.S.C. § 6851(b)(1)(A).

means a visual depiction as that term is defined in 18 U.S.C. § 2256(5) [relating to child pornography] that depicts:

- (i) the uncovered genitals, pubic area, anus, or post-pubescent female nipple of an identifiable individual; or
- (ii) the display or transfer of bodily sexual fluids—
 - (I) on to any part of the body of an identifiable individual;
 - (II) from the body of an identifiable individual; or
 - (III) an identifiable individual engaging in sexually explicit conduct¹²²....¹²³

(c) Without Consent. The law requires the disclosure to be “without the consent of the individual,”¹²⁴ and it defines “consent” as “an affirmative, conscious, and voluntary authorization made by the individual free from force, fraud, misrepresentation, or coercion.”¹²⁵ Helpfully, the statute expressly provides that the depicted person’s consent to the depiction’s *creation* “shall not establish that the person consented to its *distribution*,” and the victim’s *disclosure to someone else shall not establish that the person consented to the further disclosure*” by the perpetrator.¹²⁶

(d) Knowledge or Reckless Disregards of Lack of Consent to Such Disclosure. The law provides that a violation occurs where the “disclosure was made by a person who knows that, or recklessly disregards whether, the individual has not consented to such disclosure.”¹²⁷

(e) In or Using Interstate or Foreign Commerce, or Any Means or Facility Thereof. The perpetrator’s disclosure must be “in or affecting interstate or foreign commerce or using any means or facility of interstate or foreign commerce.” The statute does not define interstate or foreign commerce. At the time of writing this draft of the manual, case law was not available interpreting this statute; however, the courts have long interpreted identical language in other statutes such as federal child pornography laws broadly to include any transmission via the internet.¹²⁸

2. Damages and Other Relief

The law offers strong relief, permitting recovery of damages – either “liquidated damages in the amount of \$150,000” or “actual damages sustained” – “and the cost of the action,

¹²² The statute defines “sexually explicit conduct” by reference to 18 U.S.C. § 2256(2) (relating to child pornography). 15 U.S.C. § 6851(b)(6). The referenced law contains both a general definition (18 U.S.C. § 2256(2)(A)) and a separate definition for sexually explicit conduct in “child pornography” (18 U.S.C. § 2256(2)(B)). The general definition provides that “sexually explicit conduct” means actual or simulated—(i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the anus, genitals, or pubic area of any person...” 18 U.S.C. § 2256(2)(A).

¹²³ 15 U.S.C. § 6851(b)(5)(A).

¹²⁴ 15 U.S.C. § 6851(b)(1)(A).

¹²⁵ 15 U.S.C. § 6851(a)(2).

¹²⁶ 15 U.S.C. § 6851(b)(2) (emphasis added).

¹²⁷ 15 U.S.C. § 6851(b)(1)(A).

¹²⁸ See, e.g., *United States v. Wesson*, 426 F. Supp. 3d 822 (D. Kan. 2019) (citing Fourth Circuit and Eighth Circuit precedent holding that “use of the internet in the transmission of child pornography satisfies the interstate commerce element of the offense” under 18 U.S.C. § 2252A, which uses language identical to 15 U.S.C. § 6851).

including reasonable attorneys' fees and other litigation costs reasonably incurred.¹²⁹ Moreover, the statute provides that the court “may, in addition to any other relief available at law, order equitable relief, including a temporary restraining order, a preliminary injunction, or a permanent injunction ordering the defendant to cease display or disclosure of the visual depiction.”¹³⁰

The law also provides that, in ordering the foregoing relief, the court “may grant injunctive relief maintaining the confidentiality of the plaintiff using a pseudonym.”¹³¹

3. *Exceptions to the Law*

Where the depicted individual was “in a public place” when the depiction was created, it is covered by the statute “only if the individual did not—(i) voluntarily display the content depicted; or (ii) consent to the sexual conduct depicted.”¹³²

The statute also carves out four other express exceptions for consensual commercial pornography; good faith disclosures by or for law enforcement, legal proceedings, medical or treatment uses, and reporting; matters of public interest; and disclosures reasonably intended to assist the victim.¹³³

B. Cases Against Governmental Entities

A summary of case law interpreting these statutes is included in the Appendix.

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.¹³⁴ Sexual harassment is encompassed within its prohibition of discrimination on the basis of sex.¹³⁵ 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.¹³⁶ Title VII of the Act prohibits sexual harassment or other forms of discrimination at work.¹³⁷ Title IX of the Education Amendments Act of 1972 prohibits discrimination in an education program that receives funding from the federal government.¹³⁸ Title VII and Title IX do not provide plaintiffs with a cause of action against individuals, only against employers and educational institutions.

¹²⁹ *Id.* § 6851(b)(3)(A)(i).

¹³⁰ *Id.* § 6851(b)(3)(A)(ii).

¹³¹ *Id.* § 6851(b)(3)(B).

¹³² 15 U.S.C. § 6851(a)(5)(B).

¹³³ Specifically: “An identifiable individual may not bring an action for relief under this section relating to—(A) an intimate image that is commercial pornographic content, unless that content was produced by force, fraud, misrepresentation, or coercion of the depicted individual; (B) a disclosure made in good faith—(i) to a law enforcement officer or agency; (ii) as part of a legal proceeding; (iii) as part of medical education, diagnosis, or treatment; or (iv) in the reporting or investigation of—(I) unlawful content; or (II) unsolicited or unwelcome conduct; (C) a matter of public concern or public interest; or (D) a disclosure reasonably intended to assist the identifiable individual.” 15 U.S.C. § 6851(b)(4).

¹³⁴ Pub. L. No. 88-352, 78 Stat. 241 (1964); 42 U.S.C. § 2000e-2 (Title VII).

¹³⁵ 29 C.F.R. pt. 1604.11.

¹³⁶ See Civil Rights Attorney’s Fees Award act, codified at 42 U.S.C. § 1988.

¹³⁷ 42 U.S.C. § 2000e-2 (Title VII).

¹³⁸ 20 U.S.C. § 1681 (Title IX).

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 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.”¹³⁹

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.¹⁴⁰ Title VII claims by federal employees must be brought against the head of the relevant department, agency, or unit.¹⁴¹

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 program or activity receiving Federal financial assistance”¹⁴² 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.¹⁴³

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.

C. Cases Against Non-Governmental Entities

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

One successful (but unorthodox) tactic used by victims of image-based sex 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

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

¹⁴⁰ 42 U.S.C. § 2000e-5(e)(1).

¹⁴¹ 42 U.S.C. § 2000e-16(c).

¹⁴² 20 U.S.C. § 1681 (Title IX)(a)

¹⁴³ See *Davis v. Monroe County Bd. of Educ.*, 526 U.S. 629, 631-632 (1999).

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 image-based sex abuse.¹⁴⁴ 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.¹⁴⁵

Additionally, if there was a copyrighted song accompanying the online post containing the intimate video, the image-based sex 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.¹⁴⁶

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.¹⁴⁷ In particular, damages may be available against a person who obtains information 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.¹⁴⁸ 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.

¹⁴⁴ 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>.

¹⁴⁵ See 17 U.S.C.A. § 201(a).

¹⁴⁶ 17 U.S.C. § 501.

¹⁴⁷ 18 U.S.C. § 1030(g)

¹⁴⁸ See § 1030(e)(2)(B)

Government to promote national security.¹⁴⁹ If the CFAA violation causes only loss of money, then the damages are also only limited to economic damages.¹⁵⁰ The statute of limitations for the CFAA is two years.¹⁵¹

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.¹⁵² 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).¹⁵³

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.¹⁵⁴

Stored Communication Act, 18 U.S.C. § 2701 (2021)

The Stored Communications Act (SCA), with certain exceptions,¹⁵⁵ punishes intentionally accessing without authorization or intentionally exceeding an authorization to access a facility through which an electronic communication service is provided, and thereby obtaining, altering, or preventing authorized access to a wire or electronic communication while it is in electronic storage in such system.¹⁵⁶ Therefore, “the SCA applies to (1) electronic communications (2) that were transmitted through an electronic communication service, (3) that are in electronic storage, and (4) that are not public.”¹⁵⁷

¹⁴⁹ See §§ 1030(g), (c)(4)(A)(i)(I)-(IV).

¹⁵⁰ *Id.*

¹⁵¹ *Id.*

¹⁵² 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).

¹⁵³ 18 U.S.C. § 2520

¹⁵⁴ See, e.g., *United States v. Steiger*, 318 F.3d 1039, 1050 (11th Cir. 2003).

¹⁵⁵ 18 U.S.C. § 2701(c) (2021).

¹⁵⁶ *Id.* § 2701(a).

¹⁵⁷ *Billiter v. SP Plus Corp.*, 329 F. Supp. 3d 459, 469 (M.D. Tenn. 2018) (citing *Combier v. Portelos*, 17-CV-2239 (MKB), 2018 WL 3302182, at *11 (E.D. N.Y. July 5, 2018)).

IV. RECENT SETTLEMENTS OF CIVIL CAUSES OF ACTION

Helm v. City of Las Vegas

In March 2019, Sadie Helm, a paramedic firefighter, sued the City of Las Vegas (Las Vegas), the City of Henderson (Henderson), and several other defendants who worked for Las Vegas Fire and Rescue (LVFR).¹⁵⁸ She claimed, *inter alia*, sex discrimination and retaliation in violation of Title VII¹⁵⁹ and discrimination in violation of 42 U.S.C. § 1983 (2021).¹⁶⁰ Helm and one of the individual defendants, Nathan Hannig, were romantically involved, but the relationship ended because of the latter's obsessive and possessive behavior.¹⁶¹ In June, 2018, Helm found out that Hannig had circulated a private intimate video, which Helm had sent him during their relationship, amongst other personnel of LVFR and Henderson Fire Department.¹⁶² The video was widely viewed, discussed and distributed on LVFR and Henderson Fire Department property, by their employees, and during working hours.¹⁶³ Helm alleged that because LVFR failed to act, incompetently handled the investigation, and tried to sweep the matter under the rug, she was subject to continued sexual harassment and trauma.¹⁶⁴

On December 2, 2019, Henderson filed its Motion for Determination of Good Faith Settlement.¹⁶⁵ The parties agreed to resolve the claims against Henderson in the amount of \$1,000.¹⁶⁶ On December 16, 2019, Helm filed her Notice of Limited Non-Opposition to Henderson's motion.¹⁶⁷ Although she disagreed with Henderson's characterization of its culpability and her likelihood of success on the merits, she did not oppose the request that the court certify the settlement between them.¹⁶⁸ On September 2, 2020, Helm and Las Vegas participated in a settlement conference.¹⁶⁹ It was reported that the Las Vegas City Council subsequently approved a \$280,000 settlement with Helm as part of the council's Consent

¹⁵⁸ Complaint, *Helm v. City of Las Vegas*, No. 2:19-cv-00382-GMN-BNW (D. Nev. Mar. 5, 2019).

¹⁵⁹ Second Amended Complaint and Jury Demand at 169, *Helm v. City of Las Vegas*, No. 2:19-cv-00382-GMN-BNW (D. Nev. Dec. 17, 2019).

¹⁶⁰ *Id.* at 23–24, 26.

¹⁶¹ *Id.* at 5.

¹⁶² *Id.* at 6.

¹⁶³ *Id.* at 6, 8.

¹⁶⁴ *Id.* at 17–18.

¹⁶⁵ City of Henderson's Motion for Determination of Good Faith Settlement at 2, *Helm v. City of Las Vegas*, No. 2:19-cv-00382-GMN-BNW (D. Nev. Dec. 2, 2019).

¹⁶⁶ *Id.* at 2–3.

¹⁶⁷ Notice of Limited Non-Opposition to Defendant City of Henderson's Motion for Determination of Good Faith Settlement at 2, *Helm v. City of Las Vegas*, No. 2:19-cv-00382-GMN-BNW (D. Nev. Dec. 16, 2019).

¹⁶⁸ *Id.*

¹⁶⁹ Order Scheduling Settlement Conference at 1, *Helm v. City of Las Vegas*, No. 2:19-cv-00382-GMN-BNW (D. Nev. July 24, 2020).

Agenda.¹⁷⁰ The parties stipulated and agreed to dismiss with prejudice Henderson and Las Vegas from Helm’s civil action in January 2020 and October 2020 respectively.¹⁷¹

EEOC v. United Airlines

In August 2018, the Equal Employment Opportunity Commission sued United Airlines under Title VII and Title I to correct unlawful employment practices on the basis of sex and to provide appropriate relief to Jane Doe.¹⁷² In November 2018, Jane Doe intervened in the action.¹⁷³ The plaintiffs claimed that United Airlines discriminated against Doe by subjecting her to sexual harassment for several years and placing her in a sexually hostile environment.¹⁷⁴ More specifically, they alleged that United Airlines failed to prevent and take action against one of its pilots, Mark Uhlenbrock, who repeatedly posted, over several years, private sexually explicit photos, videos, and stories about Doe online while working for United Airlines.¹⁷⁵ He had obtained them while he and Doe were in a consensual intimate relationship.¹⁷⁶ Plaintiffs claimed that United Airlines did not take necessary action because it treated the incidents as a “personal matter between two adults.”¹⁷⁷ Even after Uhlenbrock pleaded guilty to cyberstalking, United Airlines was alleged to have continued to keep him employed and allowed him to retire with full benefits and an award to celebrate his thirty-one years of service.¹⁷⁸

The parties agreed to engage in good-faith efforts to settle.¹⁷⁹ In December 2019, the court found that all issues in the complaints had been resolved and that the Consent Decree should be entered.¹⁸⁰ The parties agreed to settle the action pursuant to the terms of the Consent Decree.¹⁸¹ United Airlines agreed to, *inter alia*, pay Doe \$321,000 plus an additional amount for attorney’s fees, modify and implement its Antidiscrimination/Antiharassment Policy and

¹⁷⁰ Joe Bartels, *Update: Revenge Porn Lawsuit Involving Las Vegas Fire and Rescue Set for Settlement*, KTNV LAS VEGAS (Oct. 7, 2020, 1:36 PM), <https://www.ktnv.com/13-investigates/revenge-porn-lawsuit-involving-las-vegas-fire-and-rescue-set-for-settlement>.

¹⁷¹ Stipulation and Order for Dismissal with Prejudice at 2, *Helm v. City of Las Vegas*, No. 2:19-cv-00382-GMN-BNW (D. Nev. Oct. 15, 2020); Stipulation and Order for Dismissal with Prejudice at 2, *Helm v. City of Las Vegas*, No. 2:19-cv-00382-GMN-BNW (D. Nev. Jan. 30, 2020).

¹⁷² Complaint and Demand for Jury Trial, *EEOC v. United Airlines, Inc.*, No. 5:18-cv-817 (W.D. Tex. Aug. 9, 2018).

¹⁷³ Motion of Jane Doe to Intervene as of Right as Party Plaintiff at 1, *Equal Employment Opportunity Commission v. United Airlines, Inc.*, No. 5:18-cv-00817-DAE (W.D. Tex. Nov. 26, 2018).

¹⁷⁴ Complaint and Demand for Jury Trial at 1, *EEOC v. United Airlines, Inc.*, No. 5:18-cv-817 (W.D. Tex. Aug. 9, 2018).

¹⁷⁵ Complaint in Intervention at 3, *EEOC v. United Airlines, Inc.*, No. 5:18-cv-00817-DAE (W.D. Tex. Feb. 28, 2019).

¹⁷⁶ Complaint and Demand for Jury Trial at 3–4, *EEOC v. United Airlines, Inc.*, No. 5:18-cv-817 (W.D. Tex. Aug. 9, 2018).

¹⁷⁷ Complaint in Intervention at 4–5, *EEOC v. United Airlines, Inc.*, No. 5:18-cv-00817-DAE (W.D. Tex. Feb. 28, 2019).

¹⁷⁸ *Id.* at 9.

¹⁷⁹ Parties’ Alternative Dispute Resolution Report at 1, *EEOC v. United Airlines, Inc.*, No. 5:18-cv-00817-XR (W.D. Tex. Mar. 25, 2019).

¹⁸⁰ Final Judgment and Order Entering Consent Decree at 1, *EEOC v. United Airlines, Inc.*, No. 5:18-cv-00817-XR (W.D. Tex. Dec. 19, 2019).

¹⁸¹ Consent Decree at 1, *EEOC v. United Airlines, Inc.*, No. 5:18-cv-00817-XR (W.D. Tex. Jan. 03, 2020).

distribute it to its current employees, provide refresher Equal Employment Opportunity training to flight operations and inflight management employees, maintain a copy of all complaints of sex discrimination and/or harassment, designate the director of its Ethics & Compliance Office to ensure compliance with the Decree, Title VII, and to respond to any claims by Doe of retaliation, and to not discriminate against any employee on the basis of sex.¹⁸² The Decree was set to last for two years.¹⁸³ In January 2020, the court dismissed with prejudice Doe’s complaint.¹⁸⁴

Ann Seifullah v. City of New York

In September 2017, Ann Seifullah’s suit against the City of New York, the New York City Department of Education (DOE) and its Chancellor was removed to federal court.¹⁸⁵ She alleged that the DOE raided her office, seized her computers, escorted her out of the building, and demoted her in response to her being allegedly framed by her ex-partner, Robert Sofia, for having intimate photos on her DOE-issued computer.¹⁸⁶ He had also claimed that she “had sex on school property with other DOE staff, parents of students, and former students.”¹⁸⁷

Although Seifullah was eventually cleared of these charges, the DOE justified its actions by claiming that she had broken other, unrelated, rules.¹⁸⁸ However, according to Seifullah, three male employees who were also involved in these infractions were never disciplined.¹⁸⁹ She was eventually suspended for one year without pay.¹⁹⁰ She claimed that, as a result, the defendants, *inter alia*, discriminated against her on the basis of her gender in violation of both Title VII and the Equal Protection Clause of the Fourteenth Amendment to the U.S. Constitution.¹⁹¹

It was subsequently reported that the city settled Seifullah’s suit for an undisclosed sum in September 2018.¹⁹² In September 2018, the parties stipulated and agreed to withdraw, discontinue, and dismiss with prejudice Seifullah’s civil action.¹⁹³

¹⁸² *Id.* at 2–6.

¹⁸³ *Id.* at 8.

¹⁸⁴ Order of Dismissal with Prejudice, *EEOC v. United Airlines, Inc.*, No. 5:18-cv-00817 (W.D. Tex. Jan. 03, 2020).

¹⁸⁵ Notice of Removal, *Seifullah v. City of New York*, No. 17-CV-5394 (NGG)(ST) (E.D.N.Y. Sept. 14, 2017).

¹⁸⁶ First Amended Complaint and Jury Demand at 1–2, 7–10, *Seifullah v. City of New York*, No. 17-CV-5394 (NGG)(ST) (E.D.N.Y. Apr. 23, 2018).

¹⁸⁷ *Id.* at 2.

¹⁸⁸ *Id.*

¹⁸⁹ *Id.* at 2–3.

¹⁹⁰ *Id.* at 3.

¹⁹¹ *Id.* at 17, 20–21.

¹⁹² Ben Chapman, *Former Principal Who Accused City of Revenge Porn Wins Settlement*, DAILY NEWS (Oct. 1, 2018, 6:00 PM), <https://www.nydailynews.com/new-york/education/ny-metro-former-principal-who-accused-city-of-revenge-porn-wins-settlement-20181001-story.html>.

¹⁹³ Stipulation of Dismissal with Prejudice, *Seifullah v. City of New York*, No. 17-CV-5394 (NGG)(ST) (E.D.N.Y. Oct. 2, 2018).

PART 3: RELEVANT SOCIAL MEDIA AND TECH PLATFORMS ASSOCIATED WITH TECH ABUSE

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

This is intended as a summary of social media platforms, but these platforms are constantly changing and updating and advocates and survivors are strongly encouraged to continually check for updates. Additional resources for safety planning and social media/tech platforms are available through additional resources recommended below (also linked in the Index).

- Cornell Tech’s Clinic to End Tech Abuse, *available at* <https://www.ceta.tech.cornell.edu/resources>
- Cyber Civil Rights Initiative Safety Center, *available at* <https://cybercivilrights.org/ccri-safety-center>
- Right To Be Social Media Guide, *available at* <https://righttobe.org/guides/how-to-use-social-media-safely/>

I. Social Media

A. Facebook

Facebook, owned by parent company Meta,¹⁹⁴ 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.¹⁹⁵ 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.¹⁹⁶ 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.

¹⁹⁴ *Introducing Meta: A Social Technology Company*, <https://about.fb.com/news/2021/10/facebook-company-is-now-meta/> (October 28, 2021).

¹⁹⁵ 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>.

¹⁹⁶ *What is public information?* FACEBOOK, <https://www.facebook.com/help/203805466323736> (last visited Jan. 8, 2019).

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.”¹⁹⁷ Facebook also uses “photo-matching technologies to help thwart further attempts to share the image on Facebook, Messenger and Instagram.”¹⁹⁸ Facebook has created its own Cyber Rights guide, called “Not Without My Consent.”¹⁹⁹

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.

In 2021, Meta supported the launch of the website StopNCII.org, which allows victims to create a case through the site when they are concerned their intimate images have been posted or might be posted to online platforms like Facebook or Instagram.²⁰⁰ A summary of the StopNCII.org is included below:

“The tool features hash-generating technology that assigns a unique hash value (a numerical code) to an image, creating a secure digital fingerprint. Tech companies participating in StopNCII.org receive the hash and can use that hash to detect if someone has shared or is trying to share those images on their platforms.

While participating companies use the hash they receive from StopNCII.org to identify images that someone has shared or is trying to share on their platforms, the original image never leaves the person’s device. Only hashes, not the images themselves, are shared with StopNCII.org and participating tech platforms. This feature prevents further circulation of that NCII content and keeps those images securely in the possession of the owner.”

Per Meta, “StopNCII.org is for adults over 18 years old who think an intimate image of them may be shared, or has already been shared, without their consent. For people who are under 18, there are other resources and organizations that can offer support, including the National Center for Missing & Exploited Children (NCMEC).”

¹⁹⁷ *Community Standards: Adult Nudity and Sexual Activity*, FACEBOOK, https://www.facebook.com/communitystandards/adult_nudity_sexual_activity (last visited July 17, 2023)

¹⁹⁸ 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 July 17, 2023)

¹⁹⁹ *Not Without My Consent*, FACEBOOK, <https://fbnewsroomus.files.wordpress.com/2017/03/not-without-my-consent.pdf> (last visited July 17, 2023)

²⁰⁰ Antigone Davis, *Strengthening Our Efforts Against the Spread of Non-Consensual Intimate Images*, FACEBOOK NEWSROOM (December 2, 2021), <https://about.fb.com/news/2021/12/strengthening-efforts-against-spread-of-non-consensual-intimate-images/> (last visited July 17, 2023)

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.²⁰¹

Users can report within Instagram either directly from a photo or 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.²⁰² Instagram has information available about reporting and seeking help for nonconsensual sharing of intimate images.²⁰³

C. 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 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 image-based sex 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))."²⁰⁴ Additionally, LinkedIn prohibits the posting of "deepfake" images or videos of others or otherwise posting content that has been manipulated to deceive.²⁰⁵

To report inappropriate, abusive, or spam content, follow the instructions on LinkedIn's Help center.²⁰⁶

²⁰¹ *Instagram: Community Guidelines*, INSTAGRAM, https://help.instagram.com/477434105621119?helpref=faq_content (last visited Jan. 8, 2019).

²⁰² The form can be found here: https://help.instagram.com/contact/383679321740945?helpref=faq_content.

²⁰³ *See What should I do if someone shares an intimate photo of me on Instagram without my permission?*, INSTAGRAM HELP CENTER <https://help.instagram.com/1769410010008691> (last visited July 17, 2023); *see also Building a Safer Community: Protecting Intimate Images*, INSTAGRAM HELP CENTER, <https://about.instagram.com/blog/announcements/protecting-intimate-images-on-instagram>, (last visited July 17, 2023)

²⁰⁴ *User Agreement*, LINKEDIN, <https://www.linkedin.com/legal/user-agreement> (last visited July 17, 2023).

²⁰⁵ *Professional community politics*, LINKEDIN, <https://www.linkedin.com/legal/professional-community-policies> (last visited July 17, 2023).

²⁰⁶ *Recognize and report spam, inappropriate, and abusive content*, LINKEDIN, <https://www.linkedin.com/help/linkedin/answer/a1344213/recognize-and-report-spam-inappropriate-and-abusive-content?lang=en> (last visited July 17, 2023)

D. 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.²⁰⁷

Snapchat has been used to share sexually explicit content and has become a popular platform for “sexting.”²⁰⁸ 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.²⁰⁹ 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 image-based sex abuse should try to

²⁰⁷ *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).

²⁰⁸ 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).

²⁰⁹ *Community Guidelines & Rules* SNAPCHAT, <https://support.snapchat.com/en-US/a/guidelines> (last visited July 16, 2023), <https://values.snap.com/privacy/transparency/community-guidelines/harassment-and-bullying> (last visited July 16, 2023), <https://values.snap.com/privacy/transparency/community-guidelines/harassment-and-bullying> (last visited July 16, 2023).

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.

E. TikTok

TikTok is a social media platform TikTok is a video-sharing app that allows users to create and share short-form videos on any topic. TikTok is a newer app whose users skew younger, but it has become increasingly popular with age groups across the spectrum.²¹⁰ Video creators can utilize filters and search for sound to include on the video. Users engage with other videos by commenting, liking, and responding, or “dueting” where users duplicate videos and add themselves alongside. Similar to Twitter (described *infra*) you can search TikTok via “hashtags” (a word or phrase preceded by a “#” symbol), which are often used to identify all posts associated with a particular “challenge,” such as eating a certain food or doing a specific dance move. *Id.*

TikTok bans the below (non-exhaustive list):²¹¹

- “Content that risks the safety of others, including pranks like swatting.
- Content that attacks or incites violence against an individual or a group of individuals on the basis of protected attributes.
- Expressions of abuse, including but not limited to violent threats, sexual harassment, disparaging statements regarding appearance, intellect, personality traits, and hygiene.
- Content that depicts, commits, or incites non-consensual sexual acts. Content that commits, promotes, or glorifies sexual solicitation or sexual objectification.
- Nudity and sexual exploitation involving minors”

Users can report abusive content through the TikTok Support center.²¹²

F. 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

²¹⁰John Herman, *How TikTok Is Rewriting the World*, NY TIMES, <https://www.nytimes.com/2019/03/10/style/what-is-tik-tok.html> (March 10, 2019).

²¹¹ *Community Guidelines*, TIKTOK, <https://www.tiktok.com/community-guidelines/> (last visited July 17, 2023).

²¹² *Report a Problem*, TIKTOK, <https://support.tiktok.com/en/safety-hc/report-a-problem> (last visited July 17, 2023).

for Twitter Blue subscribers, who can tweet up to 4,000 characters)²¹³. 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 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.”²¹⁴ Twitter gives these examples that are not permitted in its Terms of Use:

- hidden camera content featuring nudity, partial nudity, and/or sexual acts;
- creepshots or upskirts - images or videos taken of people's buttocks, up an individual's skirt/dress or other clothes that allows people to see the person's genitals, buttocks, or breasts;
- images or videos that superimpose or otherwise digitally manipulate an individual's face onto another person's nude body;
- images or videos that are taken in an intimate setting and not intended for public distribution; and
- offering a bounty or financial reward in exchange for intimate images or videos.

To report an image or photo, follow the guidelines on how to “Report Violations” through the Twitter Help Center.²¹⁵

Per its policy, 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. However, since the purchase of Twitter by Elon Musk, a litany of changes have been made to the app and user experience.²¹⁶ In December 2022, Musk disbanded the Twitter Trust and Safety Council, leading to advocate outcry and concern about the lack of response from harassment on the platform.²¹⁷

²¹³ Nicholas Reimann, *Twitter Boosts Character Limit to 4,000 for Twitter Blue Subscribers*, FORBES <https://www.forbes.com/sites/nicholasreimann/2023/02/08/twitter-boosts-character-limit-to-4000-for-twitter-blue-subscribers/#:~:text=Key%20Facts,outside%20of%20the%20United%20States> (February 8, 2023).

²¹⁴ *Help Center: Twitter Rules and policies: About intimate media on Twitter*, TWITTER, <https://help.twitter.com/en/rules-and-policies/intimate-media> (last visited July 16, 2023).

²¹⁵ *Report Violations*, TWITTER HELP CENTER, <https://help.twitter.com/en/rules-and-policies/twitter-report-violation> (last visited July 17, 2023).

²¹⁶ Kate Conger, *How Elon Musk is Changing the Twitter Experience*, NY TIMES, <https://www.nytimes.com/2023/04/07/technology/elon-musk-twitter-changes.html> (April 7, 2023).

²¹⁷ Rebecca Kern, *Advocacy groups warn of harassment on Twitter after Musk kills safety board*, POLITICO, <https://www.politico.com/news/2022/12/13/twitter-harassment-musk-kills-safety-board-00073684> (last visited July 17, 2023).

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). As of July 2023, there are more than 579 million blogs on the platform.²¹⁸ 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 (“Absolutely do not post unauthorized nude imagery—that is, private photos or videos taken or posted without the subject’s consent”).²¹⁹ Tumblr does allow “nudity and other kinds of adult material” but ask that users “add a Community Label to your mature content so that people can choose to filter it out of their Dashboard if they prefer.” *Id.* However, Tumblr bans “visual depictions of sexually explicit acts (or content with an overt focus on genitalia)” however, “[h]istorically significant art that you may find in a mainstream museum and which depicts sex acts—such as from India’s Śūnga Empire—are now allowed on Tumblr with proper labeling.” *Id.*

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.²²⁰ Tumblr users can report abusive content through the steps identified in Tumblr’s Help Center.²²¹

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 image-based sex abuse if a user uploads pornographic or intimate videos of a subject without their consent.

YouTube does not permit the posting of “any...content that depicts someone in a sexualized manner without their consent.”²²² however YouTube prohibits content that is “explicit content meant to be sexually gratifying.” *Id.* It also prohibits “content that threatens individuals”

²¹⁸ *top ten facts*, TUMBLR, <https://about.tumblr.com/#quick-facts> (last visited July 17, 2023)

²¹⁹ *Community Guidelines*, TUMBLR, <https://www.tumblr.com/policy/en/community> (last updated November 1, 2022).

²²⁰ *Online Removal Guide*, CYBER CIVIL RIGHTS INITIATIVE, <https://www.cybercivilrights.org/online-removal/#tumblr> (last visited Jan. 8, 2019).

²²¹ *Reporting Content*, TUMBLR HELP CENTER <https://help.tumblr.com/hc/en-us/articles/226270628-Reporting-Content> (last visited July 17, 2023).

²²² *Nudity & sexual content policy*, YOUTUBE HELP, <https://support.google.com/youtube/answer/2802002?hl=en> (last visited July 17, 2023).

or “content that targets an individual with prolonged or malicious insults based on intrinsic attributes.”²²³

To report a video that violates the Community Guidelines, you may follow the directions found in the YouTube Help center.²²⁴

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.²²⁵

WhatsApp does not have a specific policy on image-based sex 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.”²²⁶

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.”²²⁷ 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 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.

²²³ *Harassment and cyberbullying policy*, YOUTUBE, <https://support.google.com/youtube/answer/2802268?hl=en> (last visited July 17, 2023).

²²⁴ *Report inappropriate videos, channels, and other content on YouTube*, YOUTUBE, <https://support.google.com/youtube/answer/2802027?hl=en-GB&co=GENIE.Platform%3DDesktop> (last visited July 17, 2023).

²²⁵ *End-to-end encryption*, WHATSAPP, <https://faq.whatsapp.com/en/android/28030015/> (last visited July 17, 2023).

²²⁶ *WhatsApp Legal Info*, WHATSAPP, <https://www.whatsapp.com/legal/> (last visited July 17, 2023).

²²⁷ *See id.*

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/nonconsensualintimateimagery> (last accessed July 16, 2023). 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.

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.²²⁸ WeChat is known as a “super app” because of its wide range of functions.²²⁹ 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.

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

²²⁸ 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>.

²²⁹ 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>.

“information containing any sexual content or sexual connotation” or other information that “contradicts to social morality.”²³⁰

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.²³¹

For users outside China, a different Terms of Service applies.²³² According to WeChat’s Acceptable Use Policy, it is prohibited for users to upload or transmit content that is “sexual exploitation of adults – e.g., acts or photos involving non-consenting adults, paid sexual services, and other types of pornography (whether its public distribution was consented to or otherwise)”²³³

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, WeChat “attempt[s] to eliminate false news, disinformation, misinformation, false advertising, fraud and security breaches on WeChat” and therefore prohibit the following content:

- Spam content – including using fake accounts or compromising other people's accounts to message people or otherwise create connections or content; and attempting to engage with other users under false pretenses (e.g., falsely using login credentials, or distributing fake information).
- Any manipulation or disruption of WeChat – including manipulating or disrupting other users' use of WeChat.
- Coordinating, spreading, distributing or participating in inauthentic behavior, including in relation to false news, disinformation or misinformation and in relation to a topic or individual).
- Using WeChat on behalf of governmental entities, without full disclosure.
- Synthetic or manipulated content that may deceive, confuse or harm others (including deepfakes)”.

WeChat also has a specific Copyright Policy which details how the service deals with intellectual property-related complaints in accordance with the DMCA.²³⁴

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.

²³⁰ *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 July 16, 2023)

²³¹ *Id.*

²³² *WeChat Terms of Service*, WECHAT, https://www.wechat.com/en/service_terms.html (last modified March 1, 2023)

²³³ *WeChat Acceptable Use Policy*, WECHAT, https://www.wechat.com/en/acceptable_use_policy.html (last updated March 1, 2023)

²³⁴ *Protection of Intellectual Property in Action*, WECHAT, <https://www.tencent.com/legal/html/en-us/index.html> (last visited July 16, 2023) y 1

III. Discussion Boards/Servers

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.²³⁵ 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).”²³⁶ Moreover, Reddit prohibits users from posting fake explicit content, such as “lookalike pornography.”

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

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> (NSFW²³⁷). 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](#)).

²³⁵ 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-gyfcap>.

²³⁶ *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 updated July 5, 2023).

²³⁷ NSFW means “Not Safe for Work,” a reference used when a link likely contains pornographic images.

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 image-based sex 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 image-based sex 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, or illegal material, or any material that infringes or violates another person’s rights (including intellectual property rights, and rights of privacy and publicity).”²³⁸

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.”²³⁹ 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

²³⁸ *Match.com Terms of Use Agreement*, MATCH.COM (last revised Dec. 28, 2017), <https://www.match.com/registration/membagr.aspx>.

²³⁹ *Id.*

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 image-based sex 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.”²⁴⁰

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 any available legal action in response to illegal and/or unauthorized uses of [Tinder], including termination of your account.”²⁴¹

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.²⁴² 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;

²⁴⁰ Terms of Use, TINDER, <https://www.gotinder.com/terms/us-2018-05-09> (last revised May 9, 2018).

²⁴¹ *Id.*

²⁴² 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.

- 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.”²⁴³

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 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.²⁴⁴

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 Arrangements

Seeking Arrangements is a “Sugar Baby” and “Sugar Daddy” membership-based networking site.²⁴⁵ 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.²⁴⁶ “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.

Image-based sex 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.

²⁴³ *Grindr Terms and Conditions of Service*, GRINDR, <https://www.grindr.com/terms-of-service/> (last visited Jan. 8, 2019).

²⁴⁴ 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/>.

²⁴⁵ 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).

²⁴⁶ 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.

Seeking Arrangement will remove photos of a victim posted on the site without consent.²⁴⁷

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>.

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 image-based sex 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."²⁴⁸ 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 image-based sex 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 image-based sex 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

²⁴⁷ *Terms of Use*, SEEKING ARRANGEMENT (Oct. 30, 2018), <https://www.seeking.com/terms>.

²⁴⁸ 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.

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
- The subject did not consent to the act and the imagery was made publicly available without their consent.²⁴⁹

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.

²⁴⁹ *Remove unwanted & explicit personal images from Google*, GOOGLE, <https://support.google.com/websearch/answer/6302812?hl=en> (last visited Jan. 8, 2019).

PART 4: TECH ABUSE EVIDENCE & TRIAL ADVOCACY

I. Prior to Litigation: Active Steps to Preserve

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](#) 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 image-based sex 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.²⁵⁰
- The search results that lead to the nonconsensual pornography;
- 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's name. This ensures proper admission into evidence at later

²⁵⁰ 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 tech abuse).

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.²⁵¹

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 image-based sex 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.

²⁵¹ PAGE VAULT, <https://www.page-vault.com/>.

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 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.²⁵² 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.²⁵³ 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 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.”²⁵⁴

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).²⁵⁵

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

²⁵² See 18 U.S. Code § 2511.

²⁵³ 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.”).

²⁵⁴ *Id.*

²⁵⁵ 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.

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.

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;

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

Tech 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 tech 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

Admissibility

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.²⁵⁶
- 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 content of text messages, and the ones that do often keep the data only for a short period of time.²⁵⁷
- 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.

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.²⁵⁸
- **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.²⁵⁹

²⁵⁶ *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>.

²⁵⁷ 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/>.

²⁵⁸ See FED. R. EVID. 401.

²⁵⁹ See FED. R. EVID. 901.

- 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?²⁶⁰
- **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).²⁶¹
- **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?²⁶²
- **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.²⁶³

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.²⁶⁴

However, New York uses the most common approach, known as the Texas Standard:²⁶⁵

- 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.

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.

²⁶⁰ See FED. R. EVID. 801.

²⁶¹ See FED. R. EVID. 1003.

²⁶² See FED. R. EVID. 403.

²⁶³ 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/>.

²⁶⁴ *Griffin v. State*, 19 A.3d 415 (Md. 2011).

²⁶⁵ *Tienda v. State*, 358 S.W.3d 633 (Tex. Crim. App. 2012)

- 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 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.

Hearsay Rules / How to Introduce ESI

Most social media posts that will be relevant in the tech 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.²⁶⁶
- Others may fall under a hearsay exception such as a present sense impression, an excited utterance, a then-existing condition, or a recorded recollection,²⁶⁷ or if the creator of the post is unavailable to testify.²⁶⁸
- 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.²⁶⁹
- ESI may also become relevant with regard to character evidence;²⁷⁰ however, they may not be used solely to show bad character.²⁷¹

The Best Evidence Rule is commonly misunderstood and should not be a significant issue for using ESI (FRE 1001-1008).²⁷² The BER solely means that evidence should be

²⁶⁶ See FED. R. EVID. 801.

²⁶⁷ See FED. R. EVID. 803.

²⁶⁸ See FED. R. EVID. 804.

²⁶⁹ See FED. R. EVID. 806.

²⁷⁰ See FED. R. EVID. 404, *see also* FED. R. EVID. 405.

²⁷¹ *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).

²⁷² See FED. R. EVID. 1001-1008.

provided 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);²⁷³ 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).²⁷⁴

²⁷³ See also FED. R. EVID. 1003.

²⁷⁴ Available at https://www.americanbar.org/groups/litigation/publications/litigation_journal/2012_13/winter/the_admissibility_social_media_evidence/.

PART 5: COPYRIGHTING & 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.²⁷⁵ Where a “selfie” is at issue and thus the author of the image becomes a victim of image-based sex abuse,²⁷⁶¹⁶⁶ 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.²⁷⁷ 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.²⁷⁸

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 fee and faster processing time, and there are status tracking capabilities. In addition, where the

¹⁶⁴ 17 U.S.C. § 102(a).

²⁷⁵ 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)

²⁷⁶ 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.

²⁷⁷ 17 U.S.C. § 101 (emphasis added).

²⁷⁸ *Garcia*, 786 F.3d at 741.

copyrighted work is a video or an image, it is easier and cheaper 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 copy (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. Once registered, the copyright will last for the lifetime of the author plus 70 years. The process of registration takes several months, and the work will only be usable for litigation once registration is finalized by the Copyright office. Electronic claims are processed the fastest. In 2019 the Supreme Court decided that simply submitting application materials is no longer enough.²⁷⁹ There is opportunity for an expedited registration process called “special handling” which is available for a “compelling need related to pending or prospective litigation...” and other reasons.²⁸⁰ This process costs an \$800 nonrefundable fee. The Copyright office will try to complete its examination within 5 days in which it will determine whether the legal and formal requirements have been met. Then it will issue a Certificate of Registration effective from the date it received all the required elements of the application (acceptable application, acceptable copy of the work, and full filing fee).

To request special handling registration for litigation, the request should state whether the litigation is actual or prospective, whether the claimant is for the plaintiff or the defendant, and the names of the parties and the court involved in the prospective or actual litigation.

PRACTICE TIP: In cases of image-based sex 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. All or part of a copyright owner’s rights can be transferred to a new party.

²⁷⁹ Fourth Est. Pub. Benefit Corp. v. Wall-Street.com, LLC, 139 S. Ct. 881 (2019)

²⁸⁰ *Expedited Services and Special Handling*, Circular 4: Copyright Office Fees, 4, UNITED STATES COPYRIGHT OFFICE, <https://www.copyright.gov/circs/circ04.pdf>

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. Works can be copyrighted before they are publicized. Noncitizens are able to register for copyright protection. Minors may be eligible for protection pursuant to their state’s business regulations.

Claimants can use third-party information (P.O boxes; business addresses; business phone numbers etc.) rather than use their own personal information on their registration application. They may also have the option of registering anonymously or pseudonymously in certain situations. Claimants can request certain information like home addresses and phone numbers be removed from the Copyright office’s internet-accessible public catalogue, however the information will still be available on the offline record. Other information like driver’s license numbers, social security numbers, banking information, and credit card information will be removed by the office’s volition or upon request.²⁸¹

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.

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 image-based sex 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. The U.S. Copyright Office states during online registration only the registration specialist who examines the application will be able to view any photographs. Afterwards, the photos do become part of the public record and can be requisitioned from storage by the public. This typically only happens when a work is involved in a legal copyright suit. Section 2407.1(A) of the Copyright Compendium states that electronic registration records are available to the public via [the public catalog](#) to view and duplicate. This includes “certificates of registration, completed applications, and any written communications between the applicant and the Office.”²⁸²

²⁸¹ Section 2407.1(A), Compendium of U.S Copyright Office Practices, UNITED STATES COPYRIGHT OFFICE, Jan 28, 2021. Third Edition. <https://www.copyright.gov/comp3/docs/compendium.pdf>

²⁸² Section 2407.1(B)(1) Compendium of U.S Copyright Office Practices, UNITED STATES COPYRIGHT OFFICE, Jan 28, 2021. Third Edition. <https://www.copyright.gov/comp3/docs/compendium.pdf>

Physical deposit copies of works that have been copyrighted or refused by the office can be viewed by anyone with a reader registration card if they are available.²⁸³ A reader registration card provides access to certain Copyright Office records and is available through the Library of Congress through an application and valid photo identification.²⁸⁴ Duplications of physical deposit copies are only available to claimants, exclusive copyright holders, attorneys involved in litigation regarding the work, or through a court order.²⁸⁵

Copyrights are not very powerful in international cases. There is no international copyright law. Instead, the U.S has copyright agreements with certain countries which result in a mutual respect for each state's copyright laws. The U.S does not have an agreement with every country, so copyright protection may be ineffective in certain situations.²⁸⁶ Many victims have successfully utilized copyright to combat image-based sex abuse as websites and servers are often quick to remove copyrighted material from their sites.²⁸⁷

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”).²⁸⁸ Section 512 limits liability for ISPs in copyright infringement cases in exchange for the swift removal of infringing content.

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.

²⁸³ Section 2407.1(B)(2), Compendium of U.S Copyright Office Practices, UNITED STATES COPYRIGHT OFFICE, Jan 28, 2021. Third Edition. <https://www.copyright.gov/comp3/docs/compendium.pdf>

²⁸⁴ Section 2405.1, Compendium of U.S Copyright Office Practices, UNITED STATES COPYRIGHT OFFICE, Jan 28, 2021. Third Edition. <https://www.copyright.gov/comp3/docs/compendium.pdf>

²⁸⁵ Section 2406.3, Compendium of U.S Copyright Office Practices, UNITED STATES COPYRIGHT OFFICE, Jan 28, 2021. Third Edition. <https://www.copyright.gov/comp3/docs/compendium.pdf>

²⁸⁶ See *Circular 38A: International Copyright Relations of the United States*, 1, UNITED STATES COPYRIGHT OFFICE, <https://www.copyright.gov/circs/circ38a.pdf>

²⁸⁷ 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.

²⁸⁸ 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/>.

- (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.
- (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.²⁸⁹

Takedown Notice templates and help can be found online.

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.”²⁹⁰ A DMCA takedown notification should include a “a statement that the copyright holder believes in good faith the infringing material “is not authorized by the copyright owner, its agent, or the law.” *Id at 1151*. Accordingly, it is important that the party demanding the takedown actually have lawful authority as (or from) the copyright owner. Websites are not obligated to comply with a DMCA notice.

The DMCA also requires any ISP seeking the protection of Section 512 to include the contact details of its designated agent on the DMCA Designated Agent Directory which is available on the U.S Copyright Office’s website. The directory can be filtered by website name or by service provider. Thus, to the extent the information cannot be found on the ISP’s website, a victim may request it from the Copyright Office. There is also another free resource called the [WHOIS Tool](#) available on Whois.com, Digital.com, Icann.lookup.org, and other sites. It is meant to find domain owners. The WHOIS Tool will provide the hosting provider, I.P address, contact information, nameservers, and more.

The DMCA is a U.S law and does not apply internationally. However, non-U.S websites may still comply with the DMCA, especially if the host nation is participating in a copyright treaty with the U.S. Compliance will protect them from possible liability in case of a U.S lawsuit. If a foreign website does not comply with a DMCA takedown, it may be worth it to pursue the host countries copyright laws and solutions.²⁹¹

²⁸⁹ 17 U.S.C. § 512.

²⁹⁰ *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).

²⁹¹ See *Section 512 of Title 17: Resources on Online Service Provider Safe Harbors and Notice-and-Takedown System*, U.S Copyright Office, <https://www.copyright.gov/512/>

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.²⁹²

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.

[Lumen](#) is a DMCA transparency database. It may be a potential concern for victims. It is an independent database of DMCA notices and counternotices. The information is sourced from websites or individuals who voluntarily submit them to Lumen. Lumen only displays whatever information was sent to them. This may include the names of the people involved in the DMCA notice, URLs involved in the DMCA claim, a description of the issue leading to the complaint, or a description of the original copyrighted material and its URL.²⁹³

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;²⁹⁴ the process is known as “de-indexing.” In theory, de-indexing is a useful tool for addressing image-based sex 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 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.²⁹⁵

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

²⁹² 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”).

²⁹³ See *About Us*, Lumen, <https://www.lumendatabase.org/pages/about>

²⁹⁴ See *Site removed from the Google Index*, Help Center, GOOGLE, <https://support.google.com/webmasters/answer/40052?hl=en>.

²⁹⁵ Contact a site's webmaster, Help Center, GOOGLE, <https://support.google.com/websearch/answer/9109>.

- *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.²⁹⁶

1. *Legal Removals*

Under its Legal Removals policy,²⁹⁷ 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 image-based sex 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 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, Google states that it “*may*” (rather than “*will*”) de-list content containing “certain types of sensitive personal information.” *Id.* This includes involuntarily uploaded intimate images, involuntarily uploaded faked (or edited) intimate images, and personal information that was non-consensually released (doxxing).

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

²⁹⁶ 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>.

²⁹⁷ *Removal policies*, Help Center, GOOGLE, <https://support.google.com/websearch/answer/2744324>.

- Confidential, personal medical records.

Google has created a specific page for ‘doxxing’ or contact information that has been released for malicious reasons and is usually accompanied by “threatening behavior and calls to engage in harassment.” Google *may* remove the information as long as an examination will show:

- Presence of contact information, and
- Presence of:
 - Explicit or implicit threats, or
 - Explicit or implicit calls to action for others to harm or harass

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?

Google may also preserve to preserve certain information or photos if the content is newsworthy or is found to benefit the public interest. For personal images this may occur when there is information alongside the image that is important to the public interest, though the image without context may be removed. In rare cases, personal photos may be preserved if there is a strong public interest to keep it available. For doxxed information the public interest element is also considered and it includes:

- Professional contact information shared in the context of allegations of professional wrongdoing such as fraud, scams, etc.
- Government records
- Criminal conduct
- Other public interest content pertaining to topics such as active civic participation and public officials

3. Personal Image Removal

In response to growing public concerns about image-based sex abuse and “revenge porn,” Google introduced a dedicated “Unwanted and Explicit Personal Images” policy in 2015.¹⁸¹ That policy has since been updated to address increasingly changing privacy concerns. 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:

1. The imagery shows the complainant nude, in a sexual act or an intimate state
-AND-
2. The complainant didn't consent to the imagery, or the act and it was made publicly available

-OR-

The complainant intended the content to be private and the imagery was made publicly available without complainant's consent, like "revenge porn"

Google has similar policy regarding involuntarily uploaded "fake porn" such as photoshopped or deepfaked content. Google will only remove images or videos that meet specific requirements:

- The complainant is identifiably depicted in the imagery,
- The imagery in question is fake and falsely depicts the complainant nude or in a sexually explicit situation, and
- The imagery was distributed without the complainant's 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.

Whois.com is a free website that allows users to look up IP addresses and trace the ownership and tenure of a domain name. The "database contains details such as the registration date of the domain name, when it expires, ownership and contact information, nameserver information of the domain, the registrar via which the domain was purchased, etc."²⁹⁸ Whois may be useful for identifying ownership of a website.

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. It is encouraged to digitally obscure the sexually explicit portions of the content, as long as the content will still be useful for identifying the content that needs to be removed.

In short, victims of image-based sex 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.

²⁹⁸ <https://www.whois.com/whois/>

G. Impact of Court Orders

While it may be possible for victims of image-based sex abuse to obtain Family Court orders requiring an abuser to remove content from a website,²⁹⁹ those orders are not binding on third parties to the proceeding, such as webmasters, ISPs, Google, or other search engines.³⁰⁰ In addition, such companies traditionally enjoy immunity from liability for image-based sex abuse taking place on their platforms due to the CDA Section 230 exemption discussed *supra* in this Manual.³⁰¹

The New York State Unlawful Dissemination law (*see supra* Part 1- Criminal Legal Remedies for Victims of IBSA, Section I.A.) contains a provision allowing a victim to seek a court order of removal from a website hosting or transmitting a unlawfully disseminated intimate 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.³⁰² 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.

²⁹⁹ See Part 5 - Copyrighting and Removing Images and Videos from the Web, Sections I.F-G of the Manual.

³⁰⁰ See, e.g., *Hassell v. Bird*, 420 P.3d 776 (Cal. 2018).

³⁰¹ See Part 5 - Copyrighting and Removing Images and Videos from the Web, Sections I.F-G of the Manual.

³⁰² *FTC v LeadClick Media LLC*, 838 F.3d 158 (2d Cir. 2016).

PART 6: BEST PRACTICES FOR SAFETY PLANNING IN THE CONTEXT OF TECH ABUSE

If you are working with a client who has already been a victim of tech 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 the Resources portion 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.

A. 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).³⁰³
- 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

³⁰³ 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).

hard to remember so many different random and unique passwords. Instead, a free online password manager allows you to create one secure, unique password to log into the manager, and then the manager creates and saves random passwords for every other site.³⁰⁴

- 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* [Technology Safety Planning](#). Your client can also take the computers/devices to a professional to have them analyzed.
- Have your client secure their home WiFi network by resetting their password.
- 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?

B. 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

³⁰⁴ 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.

monitor your client, but even without spyware, your client's cell phone can broadcast a lot of dangerous information about them.

- 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.

- Disable “Find my Friends” feature.
- Ensure text message forwarding is turned off and texts are not being forwarded to another phone number.
- Remove any “trusted devices” you do not recognize.
- 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.³⁰⁵

C. 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.³⁰⁶

³⁰⁵ For more detailed iPhone safety tips, see *iPhone Privacy & Security Guide*, Technology Safety, NATIONAL NETWORK TO END DOMESTIC VIOLENCE, <https://www.techsafety.org/iphoneguide/>.

³⁰⁶ A reputable and free antivirus program for both PC and Mac is Avast, www.avast.com.

- When reading e-mail, do not open attachments from unknown senders. When browsing, do not visit unknown websites or click on unknown links.
- 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.

D. 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.

E. 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.³⁰⁷

F. 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>.

³⁰⁷ 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/>.

- 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 IBSA and Part 2- Civil Legal Remedies for Victims of IBSA and evidence collection and preservation is discussed in Part 4- Evidence Collection of this Manual.

G. 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 and applications exist that allow users to track another person’s whereabouts, take photos, record ambient audio, and remotely wipe or lock the device.³⁰⁸

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.³⁰⁹

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.

³⁰⁸ RAHUL CHATTERJEE ET AL., *The Spyware Used in Intimate Partner Violence* 9 (2018), <https://www.ipvtechresearch.org/pubs/spyware.pdf>.

³⁰⁹ 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>.

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.)

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

I. Directory of Useful Websites (Written Resources)

Field Guides and Manuals

- **Chayn and End Cyber Abuse, Orbits Field Guide**, <https://endcyberabuse.org/orbits/> - Guide co-created by two nonprofit organizations guide on how to design interventions to tech abuse that are intersectional, survivor-centered, and trauma-informed. The guide focuses on three areas that are vital for effectively tackling tech abuse: technology, research, and policy. It explores how systems are failing survivors and how we can design interventions that leave no survivor behind.
- **“How Communities Can Support Survivors of Stalking,”** <https://www.survivorguides.org/> This guide, co-created by Thriving Through and menses centers survivors, builds the strength and knowledge of survivors’ support networks, and relieves some of the burden on people experiencing this form of abuse.
- **Intel Techniques** - <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.
- **Pen America**, <https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/> - Online Harassment Field Manual with helpful glossary of technology-facilitated abuse terms.

Documents, guides, and other written resources

- **NNEDV Safety Net Project** - <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.
- **Hackblossom** - <https://hackblossom.org/domestic-violence/> – An online scenario and strategy guide for domestic violence victims of technology abuse.
- **Cyber Civil Rights Initiative** - <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 image-based sex abuse content found online.

- **Clinic to End Tech Abuse**, <https://www.ceta.tech.cornell.edu> - Provides guides and resources to help end tech abuse for survivors, including 1:1 assistance and safety planning guides and information.
 - <https://www.ceta.tech.cornell.edu/gethelp>
 - <https://www.ceta.tech.cornell.edu/resources>
- **Copyright Alliance** - <https://copyrightalliance.org/education/copyright-law-explained/> – Overview of copyright law.
 - **Copyright.gov** - <https://www.copyright.gov/help/faq/faq-general.html> - General FAQ regarding copyright laws.
- **Federal Trade Commission** - <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.
- **Right to Be** - <https://stories.righttobe.org/>– Right To Be's storytelling platform is a safe space where you can share your harassment story, get support, and help others experiencing harassment. Sharing your story contributes to the collective building of a better world where everyone has the Right To Be who they are, wherever they are. They also have a resource guide on different social media + tech platforms and reporting options.

II. Directory of Service Organizations

Organization	Mission and Services	Contact Information	Location
Access Now	24/7 Digital Security Helpline; free	E-mail: help@accessnow.org https://www.accessnow.org/help/	Global
Arab American Family Support Center	Settlement house, mission to empower immigrants and refugees.	150 Court Street, 3d floor, Brooklyn, New York 11201 (718) 643-8000.	New York
Association Concerning Sexual Violence Against Women	Established on 8 March 1997, Association Concerning Sexual Violence Against Women (ACSVAfW) is a non-government charitable organisation that works to raise awareness of sexual violence against women and promotes a gender equal environment.	https://rainlily.org.hk/	Hong Kong
CA Goldberg	Victim's rights Law Firm specializing in helping those who are under attack to restore their safety and privacy. Provides resources and guides for those who have been impacted by stalking, sextortion, nonconsensual photography and intimate partner violence.	646 - 666 - 8908 https://www.cagoldberglaw.com/	New York and California

Chayn	Addresses gender based violence through survivor lead resources. Toolkits and global resources	https://chayn.co/	Global (based in UK)
Clinic to End Tech Abuse	Services to help end tech abuse for survivors, including 1:1 and resource guides.	https://www.ceta.tech.cornell.edu/gethelp https://www.ceta.tech.cornell.edu/resources	New York
CCM (Community Counseling and Mediation)	Counseling services with a focus on teen dating violence; additional services offered for mental health, alcohol and substance abuse, education and youth development, and preventative services. (for ages 7-24)	Phone: 718-802-0666 https://ccmny.org	New York
Covenant House	Provides housing and supportive services to youth facing homelessness.	https://www.covenanthouse.org/	Global (United States, Canada, Guatemala, Honduras)
Crash Override Network	Crisis helpline, advocacy network & resource center for those experiencing online abuse. Digital security guides available.	http://www.crashoverridenetwork.com/ Email: help@crashoverridenetwork.com	United States

<p>Cyber Civil Rights Initiative</p>	<p>Pro bono legal assistance. Also provides a free, confidential support available 24/7 for victims of image-based sex abuse</p>	<p>https://www.cybercivilrights.org/professionals-helping-victims/</p> <p>Call: 844-878-2274</p> <p>https://www.cybercivilrights.org/ccri-crisis-helpline/</p>	<p>United States</p>
<p>Day One</p>	<p>Day One partners with youth to end dating abuse and domestic violence through community education, supportive services, legal advocacy, and leadership development.</p>	<p>Toll-free hotline: 800-214-4150</p> <p>Text line – 646-535-DAY1 (3291)</p> <p>https://www.dayoneny.org/</p>	<p>New York</p>
<p>DMCA Defender</p>	<p>Reputation management and DMCA takedown specialists</p>	<p>http://dmcadefender.com/</p>	<p>United States (based in Missouri)</p>
<p>The Door</p>	<p>Providing mental health counseling, housing, addiction treatment, legal services, and teen dating violence services. (12-24 years old.</p>	<p>Call (212)-453-0222, and Text (646)-392-8563. Monday - Friday 10am to 8pm</p> <p>https://door.org</p>	<p>New York</p>

End Cyber Abuse	End Cyber Abuse is a global collective of lawyers and human rights activists working to tackle technology-facilitated gender-based violence (TGBV) by raising awareness of rights, advocating for survivor-centered systems of justice, and advancing equitable design of technology to prevent gendered harms.	https://endcyberabuse.org/	Global
EndTab	Trainings & resource guides to address online harassment, digital intimate partner violence.	https://endtab.org/	United States (based in California)
Family Legal Care	The mission of Family Legal Care (formerly 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.familylegalcare.org	New York

Garden of Hope	Serving, caring, and rebuilding the lives of people who have been exposed to domestic violence, sexual assault, and human trafficking; specifically for the growing Chinese communities in the NYC region.	Flushing New York Office (718)- 990-8862 HelpLine (718)-321-8862	Global (New York and Taiwan)
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/	New York
iPredator:	Internet safety and cyber crime psychology resource. Risk assessments, checklists, guides for how to identify and address cyber crimes	https://www.ipredator.co/	New York
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 https://www.klgates.com/pro-bono	United States, Asia, Australia, Europe
Korean American Family Service Center	Provide crisis intervention, counseling, support, culturally specific education for survivors of domestic violence, sexual assault, and human trafficking.	Flushing, New York , (718) 460-3801 24hr hotline (718)460-3800	New York

<p>Legal Momentum</p>	<p>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.</p>	<p>https://www.legalmomentum.org/</p> <p>Helpline request form available at: https://www.legalmomentum.org/get-help-form</p>	<p>New York</p>
<p>Legal Services NYC</p>	<p>Legal Services NYC fights poverty and seeks racial, social, and economic justice for low income New Yorkers.</p>	<p>Call 917-661-4500 for the Legal Assistance Hotline, Monday through Friday from 10 a.m. to 4 p.m.</p> <p>https://www.legalservicesnyc.org/</p>	<p>New York</p>
<p>Love is Respect</p>	<p>Engage, educate and empower young people to prevent and end abusive relationships. Advocates offer support, information and advocacy to young people who have questions or concerns about their dating relationships. Provide information and support to concerned friends and family members, teachers, counselors, etc. (Project of National Domestic Violence Hotline, below)</p>	<p>1-(866)-331-9474</p> <p>https://www.loveisrespect.org</p>	<p>United States</p>

McAllister Olivarius	International civil litigators with offices in the UK and US who have built an international reputation for providing skillful and supportive representation to people unfairly treated by employers, universities, online harassers, government bodies and others.	https://mcolaw.com/	Global (United States, UK and Europe)
National Domestic Violence Hotline	24/7 hotline; provides connections to local domestic violence agencies	Call: 1-800-799-7233 www.thehotline.org	United States (based in Texas)
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/	New York
Operation Safe Escape	Organization of security professionals assisting victims of domestic violence with escaping and remaining free of abusive relationships. Educate and train victims in various methods of personal, physical, and digital safety, help them to erase their digital footprint and protecting themselves in the real world.	https://safeescape.org	United States

RAINN	24/7 hotline; provides connections to local sexual violence agencies	Call: 1-800-656-HOPE (4673) www.rainn.org .	United States
Sanctuary for Families	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.	For crisis intervention, shelter, and counseling , please call 1.212.349.6009 x1367 or text 929.335.9922 For legal services including orders of protection, divorce, immigration, and child custody, visitation and support, please call 1.212.349.6009 x8000 or text 646.692.0300 www.sanctuaryforfamilies.org	New York
Safe Horizon	24/7 hotline; provides support with crisis counseling, safety planning, assistance finding a shelter, information about resources. Assistance available in any language.	www.safehorizon.org For help with domestic violence, call: 1-800-621-HOPE (4673) For help with all crimes, call 866-689-HELP (4357) For help with rape and sexual assault, call 212-227-3000 For hearing impaired clients, call TDD line at 866-604-5350	New York

Sakhi for South Asian Women	Represent the South Asian diaspora in survivor-led movement for gender-justice. Offer direct services, advocacy and organizing, technical assistance, and community outreach.	Office number (212)714-9153 Helpline M-F 10-5 (212)-868-6741 or text (305)-204-1809	New York
Thriving Through	Provide therapy, court services, consultations, and engagement and training services for survivors of technology-facilitated abuse.	thrive@thrivingthrough.com 347.841.6499 Brooklyn, NY 11201	New York
Turning Point for Women and Families	Confidential services in a culturally and religiously sensitive environment. We focus on issues related to domestic violence, child safety. Counseling, crisis intervention, support groups, advocacy, mentoring.	https://tpny.org/ Helpline (718)-262-8722.	New York
Urban Justice Center	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.	www.urbanjusticecenter.org Call the intake line 718-875-5062 on M, W, Fri (9am-5pm). For domestic violence services, visit www.dvp.urabnjustice.org	
VAWnet	Online Resource Library on Gender Based Violence, project of National Resource Center on Domestic Violence	https://vawnet.org/sc/technology-assisted-abuse /	

<p>WomanKind (formerly New York Asian Women’s Center)</p>	<p>Resources and cultural competency to help survivors find refuge, recovery, and renewal from domestic violence, human trafficking, and sexual violence.</p>	<p>24hour hotline (888)-888-7702 Office number (212)732-0054.</p>	
---	---	--	--

III. Teen Dating Violence Hotline Numbers:

Resource	Contact information
Day One Helpline	1-800-214-4150
Covenant House Helpline:	1-800-999-9999 (7 days a week 1pm to 5pm) https://www.covenanthouse.org
The Network/La Red’s 24-hour hotline provides confidential emotional support, information, referrals, safety planning, and crisis intervention for lesbian, gay, bisexual, queer and/or transgender (LGBTQ+) folks, as well as folks in kink and polyamorous communities who are being abused or have been abused by a partner.	1-800-832-1901
LGBT National Hotline	1-800-246-7743
Hetrick Martin Institute	LGTBQI+ youth 1-(212)-674-2400.
Love is Respect Hotline	1-866-331-9974 (24/7) or text “loveis” 22522
NYC Youth line:	Or Youth Connect 1-(800)-246-4646. TDD 1-(800)-246-4699.
The Anti-Violence Project	1-212-714-1141 (LGBTQ Teens). Bilingual; 24/7.

PART 8: APPENDICES

APPENDIX	DOCUMENT
A.	Ten 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 technology-facilitated abuse language on Orders of Protection
D.	Family Offense Petitions alleging technology-facilitated abuse
E.	Family Court Orders of Protection including provisions prohibiting technology-facilitated abuse
F.	Case law interpreting federal criminal and civil statutes
G.	New York City Administrative Code § 10-180
H.	New York Penal Law § 245.15
I.	New York Family Court Act § 812
J.	New York Criminal Procedure Law § 530.11
K.	New York Civil Rights Law § 52-b
L.	Apple Guide: Device and Data Access when Safety is at Risk

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[ititione]r’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].;

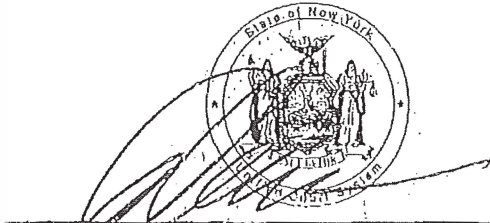
[99] Observe such other conditions as are necessary to further the purposes of protection: [REDACTED];

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];

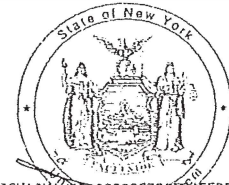
[99] Observe such other conditions as are necessary to further the purposes of protection: no accessing social media accounts owned by [REDACTED]; No impersonating [REDACTED] online; NO distributing, disseminating, publishing intimate photographs, images, texts, videos of [REDACTED];



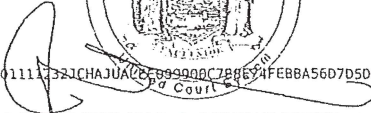
It is further ordered that this order of protection shall remain in force until and including August 01, 2019.

Dated: August 01, 2018

ENTER



201808011112321CHAJUAC669900C788674FE8BA56D7D506FC215F



[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]: _____



Appendix F – Case law interpreting federal criminal and civil statutes

Cases Interpreting Federal Criminal Law

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

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. 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.”¹ 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).²

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.

An unpublished case in the Army Court of Criminal Appeals, *United States v. Meredith*, ARMY 20170178, 2018 WL 3770392 (A. Ct. Crim. App. Aug. 7, 2018) provides some guidance related to the application of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2) (2021). In that case, appellant, then a Sergeant, was assigned as the Non-Commissioned Officer-in-Charge at one of the clinics at a joint military medical facility. He had befriended his victims, a Hospitalman and her husband. Because they trusted him, they would sometimes ask him to dog-sit and stay at their apartment when they were away. On one such occasion, using the pretext of watching movies on Netflix, he obtained his victims’ computer password and accessed their external hard drive, searched through their private folders, and located private sex videos that they had recorded of themselves. He downloaded copies of those videos onto three of his electronic devices and tried to share them with other subordinates. The Army court determined that a military judge had erred in convicting the appellant of one specification of violating § 1030(a)(2) by intentionally accessing a protected computer “without authorization” and obtaining the private sex videos of his victims. The court held that this conviction was legally and factually insufficient. It reasoned that § 1030(a)(2)(C) provides for two different theories of criminal liability: intentionally accessing a computer without authorization *or* exceeding authorized access and thereby obtaining information from a protected computer. “Without authorization” means “without any permission”;³ whereas “exceeds authorized access” means “to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter.”⁴ Because the appellant’s victims had granted him access to their computer, he did not access the computer “without

¹ 18 U.S.C. § 1030(e)(2)(B).

² See [Part 1- Criminal Legal Remedies for Victims of IBSA, Section II. E](#), *infra*, for a discussion of criminal charges related to interstate threats or extortion under 18 U.S.C. § 875.

³ *Amphenol Corp. v. Paul*, 993 F. Supp. 2d 100, 109 (D. Conn. 2014).

⁴ 18 U.S.C. § 1030(e)(6) (2021).

authorization,” but exceeded the access granted. Therefore, the government had “[chosen] the wrong theory in pursuing [the] charge.”⁵

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

In *Ledgard*, discussed *supra*, 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. Cases Interpreting Federal Wiretap Act, 18 U.S.C. § 2520

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

In an unpublished opinion in *United States v. Lloyd*, 809 Fed. App’x 750 (11th Cir. 2020), the court affirmed a defendant’s sentence following his conviction for threatening, over the internet, someone he believed to be a minor, in violation of 18 U.S.C. § 2261A(2)(B) (2021). In that case, the defendant had threatened to email topless photos of his victim to her parents and friends and thereby “ruin her ‘good girl’ image” unless she continued to supply him with similar photos. The court rejected the defendant’s argument that his offense was not a sex offense that required him to register as a sex offender under the Sex Offender Registration and Notification Act (SORNA).

In *United States v. Ackell*, 907 F.3d 67 (1st Cir. 2018), the court expressly rejected the defendant’s First Amendment challenge to the federal anti-stalking statute, 18 U.S.C. § 2261A(2)(B) (2021) and affirmed the district court’s judgment. In that case, the defendant formed a relationship with his victim, a sixteen-year-old high school sophomore, online. About five months into the relationship, the defendant proposed that they enter into a “dominant-

⁵ *United States v. Meredith*, ARMY 20170178, 2018 WL 3770392, at *2 n.5 (A. Ct. Crim. App. Aug. 7, 2018).

submissive” relationship, in which his victim would be “the submissive,” which she agreed to. After they commenced this relationship, the defendant would frequently demand that she send him sexually explicit photos of herself. When the victim tried to end the relationship, the defendant told her that she could not, and threatened to disseminate the photos she had sent him to her friends, classmates, and family if she stopped sending such photos to him. When she pleaded with him to delete the photos, he refused. The defendant was convicted under § 2261A(2)(B) and sentenced to thirty-three months of imprisonment.

In his appeal, the defendant argued that § 2261A(2)(B) violated the First Amendment because (1) the statute was facially overbroad even though it was constitutionally applied to him, and (2) it was an impermissible content-based restriction on speech that did not survive strict scrutiny. The court disagreed. Construing the elements of the statute, the court held that § 2261A(2)(B) regulates, not speech, but “course[s] of conduct.” Although sufficiently expressive conduct may enjoy First Amendment protection, the concern that protected speech may be chilled attenuates as the otherwise unprotected behavior moves from pure speech toward conduct. The court held that, while § 2261A(2)(B) could reach expressive conduct, its plain language covered countless amounts of unprotected conduct. Although a statute that does not facially regulate speech could still be facially overbroad under the First Amendment, the court found that the defendant failed to sufficiently demonstrate that the statute could apply to a substantial amount of protected speech, both in an absolute sense and in relation to its many legitimate applications. Therefore, with regard to the defendant’s first argument, although the court acknowledged that § 2261A(2)(B) could have an unconstitutional application, it held that the statute did not, on its face, regulate protected speech or sufficiently expressive conduct. If the statute ever did implicate protected expression, as-applied challenges would suffice to properly safeguard First Amendment rights. The court also rejected the defendant’s contention that § 2261A(2)(B) was an impermissible content-based restriction on speech. Because it had already determined that § 2261A(2)(B) did not target protected speech, it held that the statute could not be an impermissible content- or viewpoint-based restriction on speech.

The defendant also brought four different challenges to the district court’s jury instructions. Two were merely a repetition of his First Amendment challenge to § 2261A(2)(B) and were dismissed by the court. The remaining two were that the district court erred in: (1) failing to instruct the jury to decide unanimously which specific acts formed his “course of conduct,” and (2) instructing the jury that a course of conduct can “attempt to cause” substantial emotional distress. Responding to his first challenge, the court held that, although unanimity was necessary in determining both guilt and that the prosecution had proved each element of the charged offense, it was not necessary with regard to “brute facts” that constitute those elements. Because the specific acts were “brute facts” and not elements of the offense, a unanimity instruction was unnecessary. In terms of his second challenge, the court acknowledged that because it was unusual to think of “courses of conduct” as having volition, the statute’s provision that a defendant may be convicted for engaging in a course of conduct that “attempts to cause . . . substantial emotional distress,” was quite peculiar. However, it noted that the defendant only challenged the district court’s rejection of his proposed instructions; he did not, for example, challenge the statute’s wording on due process or void-for-vagueness grounds. As such, his challenge failed because the court found that the district court did not abuse its discretion when it gave jury instructions that precisely tracked the statute’s language.

Finally, the defendant challenged the district court's denial of his motion for acquittal. The court rejected this challenge as well because it found that the defendant could not demonstrate that the government had failed to introduce sufficient evidence to prove the intent and harm elements of § 2261A(2)(B).

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.⁶

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

⁶ 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.

In *United States v. Sryniawski*, 8:19-CR-394, 2020 WL 5422814 (D. Neb. Sept. 10, 2020), the defendant moved to dismiss the second count in his indictment that charged him with making interstate extortionate threats in violation of 18 U.S.C. § 875(d) (2021). The court adopted the magistrate judge’s recommendation that the motion be denied. The victim had announced that he would be seeking office in the Nebraska Unicameral, and became eligible as a candidate for the November 2018 general election. The defendant, the ex-husband of the victim’s wife, sent anonymous emails containing a photograph of the victim’s wife and a photograph of an immediate family member of the victim performing sexual acts. The photograph of the victim’s wife (the defendant’s ex-wife) had been taken when the defendant was married to her; the photograph of the victim’s family member was a digital manipulation. The defendant threatened to make these pictures public unless the victim dropped out of the race.

A person violates § 875(d) “if he transmits a communication containing any threat to injure the reputation of a person with intent to extort a ‘thing of value’ from that person.”⁷ In his motion to dismiss count two, the defendant argued that he could not have demonstrated the requisite intent to extort because a request to drop out of an election was not a “thing of value.” Rejecting this argument, the court determined that under § 875(d), a “thing of value” could include tangible or intangible things, and that “the focus of the . . . term is to be placed on the value which the defendant subjectively attaches” to what he seeks.⁸ For example, a sexual relationship may be an intangible thing of value under § 875(d).⁹ The defendant’s belief that his victim would not make a good candidate for office and his threats to embarrass his ex-wife and the victim’s other family member demonstrated that the victim’s candidacy was a “thing of value” to him.

In *United States v. Torres*, 20cr608 (DLC), 2021 WL 1947503 (S.D.N.Y. May 13, 2021), the court denied the defendant’s motion to dismiss the indictment against him, for charges including stalking in violation of 18 U.S.C. § 2261A(2) (2021). In that case, Torres had sent a

⁷ *United States v. Hobgood*, 868 F.3d 744, 747 (8th Cir. 2017).

⁸ *Id.* (quoting *United States v. Petrovic*, 701 F.3d 849, 858 (8th Cir. 2012)).

⁹ *United States v. Petrovic*, 701 F.3d 849, 858 (8th Cir. 2012).

series of threatening text messages to his romantic partner and threatened to kill her minor son if they did not accompany him to a motel that he forced his victim to rent, where he then forcibly confined his victims and assaulted them. When they escaped, Torres sent a series of threatening text messages to his romantic partner including threats that he would post a nude photograph of her on the internet.

Seeking to dismiss his indictment in court, Torres argued that it failed to allege an adequate basis for federal jurisdiction as required by § 2261A and, alternatively, that § 2261A was unconstitutional because it exceeded Congress's power under the Commerce Clause. The court rejected both arguments. The indictment alleged an adequate jurisdictional basis because it alleged that Torres had used a cellular telephone during the commission of the crimes charged in the indictment. Where a telephone network was used in the commission of a crime, a facility of interstate commerce was used, even if only intrastate communications were made using the telephone network.¹⁰ Torres's Commerce Clause challenge failed because a telephone network is an instrumentality of interstate commerce, and Congress can criminalize certain intrastate uses of the telephone network, such as Torres' alleged use of the telephone network to commit the crimes alleged in the indictment. For these reasons Torres's motion to dismiss the indictment for stalking in violation of § 2261A(2) was denied.

In *United States v. Hollingberry*, No. 20-03058MJ-001-PHX-MTM, 2020 WL 2771773 (D. Ariz. May 28, 2020), the defendant, who was charged with violating 18 U.S.C. § 2261A(2) (2021) and was detained pending trial, moved, pursuant to 18 U.S.C. § 3145(b) (2021), to revoke the Magistrate Judge's detention order. The court denied his motion. The defendant had been cited for trespassing after he repeatedly videotaped in the lobby of the Arizona Attorney General's Office (AGO) despite being told that this was prohibited. His victim, an AGO employee, provided the police with a copy of the surveillance video capturing the defendant's behavior. The defendant then retaliated against the victim using a combination of the internet, telephones, and in-person contact to harass and threaten her. He shared the victim's name, picture, home address and email address in videos he uploaded to his YouTube channel, and on numerous occasions directed his approximately 3,000 followers to harass her. In one video, the defendant threatened to send nude photos of the victim to the AGO and states in another that he emailed nude photos of her to one hundred people. He also sent numerous emails to AGO employees, government officials, and local news outlets, one of which was titled "Nude Photos" and stated that nude photos of the victim in a compromising position could be found on the internet.

The court found that the Government had made a threshold showing that the defendant was eligible for a detention hearing. Under the Bail Reform Act, the United States may move for pretrial detention if it can show by a preponderance of the evidence that the defendant is charged with a crime of violence¹¹ or that the case involves obstruction of justice, witness tampering, or jury tampering.¹² The court held that cyberstalking is a crime of violence under the Bail Reform Act because there is a substantial risk that physical force against the person or property of

¹⁰ See *United States v. Perez*, 414 F.3d 302, 304–05 (2d Cir. 2005).

¹¹ See § 3142(f)(1).

¹² *Id.* § 3142(f)(1)(D), (2).

another may be used in the course of committing the offense. Moreover, there was a serious risk that, if released, Defendant would continue to threaten or intimidate the victim (or attempt to do so). The court next considered certain factors to determine whether the defendant should be detained pending trial: (1) the nature and circumstances of the offense; (2) the weight of the evidence against the defendant; (3) the history and statutorily specified characteristics of the defendant; and (4) the nature and seriousness of the danger to any person or the community that would be posed by the defendant's release. The court held that these factors weighed in favor of detention.

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

In an unpublished decision in *United States v. Gomez*, 801 Fed. App'x 715 (11th Cir. 2020), the appellate court rejected defendant's challenge to her conviction for, *inter alia*, conspiracy to transmit an interstate extortionate communication, in violation of 18 U.S.C. §§ 371 & 875(d) (2021) and for transmission of extortionate communications, in violation of § 875(d). The victim in this case was the son of a famous, now-deceased Mexican singer, who had frequently engaged in conduct including partying with a group of women (including the defendant), having affairs, and exchanging sexually explicit photos with various women. The defendant and another woman sent the victim text messages threatening to reveal the photos and videos to the media unless he paid them \$50,000. They also spoke with the victim's lawyer (who recorded these conversations) on the phone to arrange for delivery of the money. Ultimately, the victim and his lawyer alerted the FBI who arrested the defendant when she flew to Miami to collect the \$50,000. The FBI were able to find extensive written and audio communications between the two women establishing the conspiracy that spanned several months. The court held that the text messages and recorded calls establishing the extortionate plot and the defendant's willing participation in it constituted overwhelming evidence of her guilt at trial.

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 IBSA 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. Cases Interpreting Obscene or Harassing Telephone Calls in Interstate or Foreign Communications, 47 U.S.C. § 233

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

In *United States v. Harris*, 991 F.3d 552 (4th Cir. 2021), the defendant challenged his conviction under 18 U.S.C. § 2422(b) (2021). He had met his minor victim, who resided in Virginia, on Facebook, and had coerced her into performing sexual acts on video chats with him and sending him sexually explicit images. He threatened to publish these explicit images on the internet or send them to her school if she did not accede to his continued demands. The conduct in question occurred when he was serving in the United States Navy at a military facility in Japan and continued while he was in Guam and then in the United States. He was convicted under § 2422(b), and sentenced to a total of fifty years' imprisonment and a life term of supervised release.

The defendant argued that his conviction constituted an impermissible extraterritorial application of § 2422(b). The court held that it need not reach this issue since his conviction involved a permissible domestic application of § 2422(b). The court looked at whether the conduct relevant to the statute's focus occurred in the United States. It held that § 2422(b)'s focus is on the coercion of children into sexual activity. The conduct relevant to this statutory focus occurred in the United States because the minor victim was in Virginia when she received the defendant's coercive messages and was forced to assent to his demands for sexual activity, which § 2422(b) seeks to prevent. Moreover, he was present in the United States when he engaged in at least some of the proscribed activity.

Cases Interpreting Federal Civil Law

A. Title VII (Employment Setting)

In an unpublished decision, *Ortiz v. Waste Mgmt., Inc.*, 808 Fed. App'x 1010 (11th Cir. 2020), the appellate court affirmed the district court's (Middle District of Florida) dismissal of the plaintiff-employee's Title VII civil action against his former employer, where the plaintiff's Employment Opportunity Commission ("EEOC") charge of discrimination failed to make allegations related to sex discrimination. In that case, the plaintiff—a route driver—alleged in his Title VII complaint against his employer that a co-worker had followed him into the men's restroom and filmed him as he was sitting on the toilet with his genitalia exposed. The co-worker then showed the video recording to several other employees. The plaintiff's employment was terminated because he persisted in his refusal to disclose the identity of the individual who informed him that the video was being shown in the workplace. Notably, the EEOC charge of discrimination had contained allegations that the co-worker had recorded and circulated the video of the plaintiff on the toilet, but did not allege that he was "treated differently or discriminated against because of his sex." Accordingly, for failing to allege sex discrimination in the EEOC charge, the Title VII complaint was dismissed.

In another unpublished decision, *Wilson v. New Jersey*, Civil No. 16-7915 (RBK/JS), 2019 WL 5485395 (D.N.J. Oct. 25, 2019), the plaintiff was employed as an Operator at a government-operated male prison in New Jersey. Around March 2014, the plaintiff began assisting a Senior Corrections Officer (SCO) at the prison with the latter's complaint about gender-based discriminatory practices she endured. Starting in June 2014, plaintiff claimed to have suffered retaliatory actions by some of her co-workers. After she reported these incidents, she suffered several more retaliatory actions. She also found out that an anonymous sender had mailed sexually suggestive nude photographs of her through interoffice mail to some of her co-workers' homes and office. The plaintiff filed a complaint with the EEOC, which determined that there was insufficient evidence of sexual harassment. She then filed her judicial complaint in which she alleged, *inter alia*, that they had unlawfully discriminated and retaliated against her in violation of Title VII, and that the retaliatory conduct included, in part, the dissemination of the nude photographs of her. The defendants moved for summary judgment.

The court granted the defendants' motion for summary judgment on the gender discrimination claim under Title VII because the plaintiff could not establish that she suffered an adverse employment action giving rise to an inference of unlawful gender discrimination. However, the court denied the defendants' motion for summary judgment on the retaliation claim under Title VII (and her sexual harassment hostile work environment claim under state law). The court held that (1) the record disclosed a factual dispute as to whether the retaliatory actions started after and in response to the plaintiff assisting the SCO with her gender discrimination complaint; and (2) the plaintiff's claims would not fail as a matter of law if a jury found that the retaliatory actions, such as the naked pictures, were a result of her aiding the SCO's complaint. The plaintiff's claims would not fail as a matter of law because (a) the plaintiff's assistance constituted a protected activity under Title VII. It was a protected activity because her assistance constituted opposition to discrimination made unlawful by Title VII. (b) The retaliatory actions

taken against her constituted adverse employment action. They constituted adverse employment action because they “well might have dissuaded a reasonable worker from making or supporting a charge of discrimination.”¹³ Finally, because a jury could determine that the plaintiff assisted the SCO prior to the start of the adverse actions against her, she had made a prima facie showing of a causal link between the protected activity and the adverse actions.

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.

B. Title IX (Educational Setting)

T.C. v. Metro. Gov’t of Nashville, No. 3:17-cv-01098; 3:17-cv-01159; 3:17-cv-01209; 3:17-cv-01277, 2020 U.S. Dist. LEXIS 179281 (M.D. Tenn. Sept. 29, 2020), concerned allegations that, in 2016 and 2017, the plaintiffs, all minors at the time, were videotaped by other students while engaged in sexual encounters with male students on the premises of their respective Metropolitan Government of Nashville and Davidson County (MNPS) schools. These videos were circulated electronically among the students’ peers. The plaintiffs, through their parents, sued MNPS. They argued that the defendant’s handling of the matters and general approach to harassment at its schools led to the deprivation of the plaintiffs’ rights under, *inter alia*, Title IX. A school system may be liable for Title IX damages related to student-on-student

¹³ *Yatzus v. Appoquinimink Sch. Dist.*, 458 F. Supp. 2d 235, 243 (citing *Burlington N. & Santa Fe Ry. Co. v. White*, 548 U.S. 53, 54 (2006)).

harassment if the school system’s “deliberate indifference . . . , at a minimum, ‘caused[d] [the student] to undergo’ harassment or ‘ma[d]e [the student] liable or vulnerable’ to it.”¹⁴

The court’s decision considered five sealed Motions for Summary Judgment. Four were filed by the defendant, MNPS. The plaintiffs, Sally Doe, Jane Doe, S.C., and Mary Doe, collectively filed a Motion for Partial Summary Judgment regarding a portion of their claims. All four plaintiffs brought “before” and “after” claims. The “before” claims focused on the defendant’s actions before the underlying incident occurred. The “after” claims focused on the defendant’s response after it learned of the underlying incident. The court granted the defendant’s motion for summary judgment on the “before” claims of all four plaintiffs. Following *Kollaritsch v. Mich. State Univ. Bd. of Trs.*, 944 F.3d 613 (6th Cir. 2019), the court held that if “a student experiences sexual harassment, and the school becomes aware of [it], ‘at least one more (*further*) incident of harassment’—attributable to the school’s improper response to the original harassment—‘is necessary to state a claim.’”¹⁵ Therefore, a claim could not be premised on the defendant’s failure to address the risk of sexual harassment against students other than the plaintiff.¹⁶ Because “before” claims could not satisfy all of these elements, they were precluded by the holding. Therefore, the defendant was entitled to summary judgment on those claims.

The court also granted defendant’s motion for summary judgment with regard to the “after” claims of Sally Doe and Jane Doe. In Sally Doe’s case, the school administrators treated the incident as serious and maintained ongoing communication with her parents, and the initial perpetrator faced significant consequences, including criminal prosecution. Because the school was not deliberately indifferent, the defendant was granted summary judgment in relation to Sally Doe’s “after” claim. In Jane Doe’s case, she transferred to another school nearly immediately after the school officials were informed of the incident and conceded that she was not subject to further harassment after the video was brought to the school’s attention. The mere fact that after she had left the school her peers had referred to her using derogatory names was not enough to meet the test for actionable harassment under *Kollaritsch*.

However, the court refused to grant the defendant’s motion for summary judgment with respect to the “after” claims of S.C. and Mary Doe. In S.C.’s case, she was initially suspended for three days from the school immediately after the incident and she did not return to the physical campus of the school after that because she received violent physical threats from other students related to her participation in the school’s investigation of the incident. The threats and gendered insults continued throughout her suspension and until her withdrawal from the school, and the video of her was uploaded to a publicly accessible pornography website. The court found that for a period of at least two weeks while S.C. was still enrolled in the school, the defendant was aware of the harassment being waged against her and failed to adequately address it. Although S.C. was not physically on campus during this period, the court held that this did not preclude her claim. First, a variety of facts demonstrated a nexus between the school’s authority

¹⁴ *Davis v. Monroe Cty. Bd. of Educ.*, 526 U.S. 629, 645 (1999).

¹⁵ *T.C. v. Metro. Gov’t of Nashville*, Civil No. 3:17-cv-01098; 3:17-cv-01159; 3:17-cv-01209; 3:17-cv-01277, 2020 U.S. Dist. LEXIS 179281, at *42 (M.D. Tenn. Sept. 29, 2020).

¹⁶ *Kollaritsch*, 944 F.3d at 621–22.

and interests and the harassment S.C. experienced. Second, the defendant's disciplinary authority to protect its investigation into the incident involving S.C. translated to sufficient control over off-campus attempts made by students to thwart it. Because the defendant treated S.C. as a perpetrator and downplayed the unique problems associated with the circulation of such a video, it caused the situation to spiral out of control. Therefore, defendant's motion for summary judgment was denied.

In Mary Doe's case, the school failed to interdict the video and grudgingly accepted the practice of students circulating sexual videos of other students as "a game . . . seniors play." Although Mary Doe complained to school personnel about the bullying she experienced as a result of the incident, the school did nothing. It merely verbally disciplined the students involved in the sexual activity and videotaping. Because Mary Doe was harassed, the school was made aware of it, her humiliation was aggravated by the school's inaction, and the discipline meted out to the perpetrators arguably reflected deliberate indifference to the risk of future harassment, defendant's motion for summary judgment was denied.

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.

1. *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. In *Kane v. Barger*, 902 F.3d 185 (3rd Cir. 2018), the plaintiff filed a civil rights action under 42 U.S.C. § 1983 (2021) alleging that the defendant—a police officer--violated her substantive due process right to bodily integrity under the Fourteenth Amendment during his investigation into whether she was the victim of a sexual assault. When the plaintiff arrived at the police station, the defendant, contrary to department policy, met alone with her in a back room of the station, closed the hallway door, pulled her shorts and top down, and used his personal cell phone to photograph intimate areas of her body. After photographing the plaintiff, the defendant failed to document the clothing evidence that the plaintiff provided.

While the district court had granted summary judgment in favor of the officer, based on qualified immunity, the appellate court reversed. In its analysis, the court first determined that (1) the plaintiff's right to not have her bodily integrity violated by a police officer investigating her potential sexual assault was protected by the Due Process Clause of the Fourteenth Amendment, and (2) viewing the evidence in the light most favorable to the plaintiff for purposes of summary judgment, the defendant's conduct shocked the conscience. Whether conduct shocks the conscience generally depends on the context in which the action takes place. Unlike in a hyperpressurized environment, because the defendant had time for "actual deliberation," the standard of "deliberate indifference" applied, which requires a "conscious disregard of a substantial risk of serious harm."¹⁷

Applying this standard, the court held that the defendant's conduct underscored a conscience-shocking disregard for the plaintiff's bodily integrity and that he had acted for his own personal gratification, rather than investigative ends. Therefore, the defendant was held to have violated the plaintiff's right to bodily integrity. Second, the court determined that the individual's right not to be sexually fondled and illicitly photographed by a police officer investigating her case was clearly established even without materially similar cases. The court held that the defendant's conduct resembled the crime of indecent assault and that, at the time of the conduct, he was on notice that he acted unconstitutionally. Because the law provided fair warning that his sexual misconduct toward the plaintiff was unlawful, the plaintiff's right was clearly established for purposes of qualified immunity. Accordingly, the matter was remitted for further proceedings consistent with the opinion.

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 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.

¹⁷ *L.R. v. Sch. Dist. of Phila.*, 836 F.3d 235, 246 (3d Cir. 2016).

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.*

C. 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 image-based sex 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 image-based sex abuse.¹⁸ 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.¹⁹

Additionally, if there was a copyrighted song accompanying the online post containing the intimate video, the image-based sex 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.²⁰

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

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

¹⁸ 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>.

¹⁹ See 17 U.S.C.A. § 201(a).

²⁰ 17 U.S.C. § 501.

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 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.

Hall v. Sargeant, No. 18-80748-CIV-ALTMAN/Reinhart, 2020 WL 1536435 (S.D. Fla. Mar. 30, 2020), concerned, *inter alia*, Sargeant’s malicious prosecution of Hall, a private investigator. Hall had been retained to locate Sargeant’s assets because the latter was defaulting on a judgment. During his investigations, Hall learned that, although Sargeant had left his family business, his emails remained on the business server. Hall was able to obtain more than 168,000 of these emails, some of which contained several hundred private photographs, messages, and sex videos of Sargeant. When Sargeant discovered Hall’s receipt of his personal emails, he sued Hall alleging, *inter alia*, that Hall had conspired to violate the federal Computer Fraud and Abuse Act (CFAA). Sargeant eventually dismissed this claim voluntarily. Hall then sued Sargeant claiming that the latter’s suit constituted malicious prosecution. The court had to determine, *inter alia*, whether to grant summary judgment on this claim in favor of Hall, which, in turn, required the court to examine the CFAA and whether Hall intentionally accessed a protected computer, without authorization or exceeding authorized access, and thereby obtained information, resulting in Sargeant suffering damage or loss of at least \$5,000.

The court held that Sargeant had probable cause to believe that each of these elements were met when he filed the complaint against Hall. First, the server on which Sargeant’s personal emails were located fit comfortably within the statutory definition of a “protected computer.” The email account itself may have constituted a “protected computer” under the CFAA. Although not technically a “device” or “facility,” at least one federal judge had suggested that

Yahoo! And Facebook accounts may qualify as “protected computer[s]” under the CFAA.²¹ For the court, such online accounts were indistinguishable from the email account at issue in the case. Second, Sargeant had reasonable grounds to believe both that Hall obtained the emails with his brother’s assistance and that his brother accessed either the server or the email account “without authorization.” Third, Sargeant had reason to believe that Hall obtained the information at issue in this case through a conspiracy with his brother. Finally, Sargent suffered losses greater than \$5,000 as a result of the alleged violation, through the hiring of a forensic analyst to respond to the violation. The court noted that Sargeant need not have suffered an interruption of service to allege losses suffered in responding to the violation.

3. *Stored Communication Act, 18 U.S.C. § 2701 (2021)*

In *Billiter v. SP Plus Corp.*, 329 F. Supp. 3d 459 (M.D. Tenn. 2018), the plaintiff sued her former employer and a former co-worker, asserting claims for intentional infliction of emotional distress, negligent hiring, invasion of privacy, and violations of the federal SCA.

The plaintiff had been provided with a company laptop computer while employed by the defendant-employer. She used the laptop for work and, on occasion, to access her personal email and other accounts. She alleged that when she returned her company laptop, the defendant-co-worker accessed the plaintiff’s private information, photographs, and videos in her private electronic accounts (including an email account and Dropbox account), downloaded these personal files, and removed them from her private electronic devices without her knowledge and consent. Some of these personal files included the plaintiff’s nude photos and videos. She alleged that the defendant-co-worker shared these photos and videos with other employees of the defendant-employer. Denying the defendants’ motion for summary judgment with respect to the plaintiff’s SCA claims, the court held that whether the SCA applied to photos in a Dropbox account was an issue that required additional facts (other than what Wikipedia and the Dropbox website provided in connection with the summary judgment motion) to determine whether Dropbox “meets the definitions of the SCA”²²

²¹ See *Mahoney v. DeNuzzio*, No. 13–11501–FDS, 2014 WL 347624, at *5 (D. Mass. Jan. 29, 2014).

²² The court did not specify which elements of the SCA required further factual development.

Appendix G – New York City Administrative Code § 10-180

Print

The New York City Administrative Code

§ 10-180 Unlawful disclosure of an intimate image.

a. *Definitions.* As used in this section, the following terms have the following meanings:

Consent. The term “consent” means permission that is knowingly, intelligently and voluntarily given for the particular disclosure at issue.

Covered recipient. The term “covered recipient” means an individual who gains possession of, or access to, an intimate image from a depicted individual, including through the recording of the intimate image.

Depicted individual. The term “depicted individual” means 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.

Disclose. The term “disclose” means to disseminate as defined in subdivision 5 of section 250.40 of the penal law, or to publish as defined in subdivision 6 of section 250.40 of the penal law.

Intimate body parts. The term “intimate body parts” means 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.

Intimate image. The term “intimate image” means a photograph, film, videotape, recording or any other reproduction of an image of a depicted individual that has been disclosed or threatened to be disclosed 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. An intimate image does not include any image taken in a public place as defined in section 240.00 of the 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.

Sexual activity. The term “sexual activity” means sexual intercourse as defined in subdivision 1 of section 130.00 of the penal law, oral sexual conduct or anal sexual conduct as those terms are defined in subdivision 2 of section 130.00 of the penal law, touching of the sexual or other intimate parts of a person for the purpose of gratifying sexual desire, sexual penetration with any object or the transmission or appearance of semen upon any part of the depicted individual's body.

b. *Unlawful disclosure of an intimate image.*

1. It is unlawful for a covered recipient to disclose an intimate image, without the depicted individual's consent, with the intent to cause economic, physical or substantial emotional harm to such depicted individual, where such depicted individual is or would be identifiable to another individual either from the intimate image or from the circumstances under which such image is disclosed.

2. It is unlawful for a covered recipient to make a threat to violate paragraph 1 of this subdivision, provided that for the purposes of this paragraph a depicted individual shall be considered to be identifiable where the covered recipient states or implies that such person would be so identifiable.

c. *Criminal penalty.* Any individual who violates subdivision b of this section shall be guilty of a misdemeanor punishable by up to one year in jail, or a fine of up to \$1,000, or both.

d. *Civil cause of action.*

1. Any individual who suffers harm from a violation of subdivision b of this section shall have a civil cause of action in any court of competent jurisdiction against the individual who violated that subdivision.

2. The defendant may be held liable to the plaintiff for any or all of the following relief:

(a) Compensatory and punitive damages;

- (b) Injunctive and declaratory relief;
- (c) Attorneys' fees and costs; and
- (d) Such other relief as a court may deem appropriate.

3. This subdivision shall not be construed to require that a criminal charge be brought, or a criminal conviction be obtained, as a condition of bringing a civil action or receiving a civil judgment pursuant to this subdivision.

e. *Provisos.* The prohibitions contained in subdivision b do not apply if:

1. 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;

2. 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; or

3. 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.

(L.L. 2017/242, 12/17/2017; Am. L.L. 2018/192, 12/1/2018, eff. 3/1/2019)

Appendix H – New York Family Court Act § 812

[The Laws Of New York \(/LEGISLATION/LAWS/ALL\)](#) / [Court Acts \(/LEGISLATION/LAWS/COURTACTS\)](#) / [Family Court \(/LEGISLATION/LAWS/FCT\)](#) / [Article 8: Family Offenses Proceedings \(/LEGISLATION/LAWS/FCT/A8\)](#) / [Part 1: Jurisdiction \(/LEGISLATION/LAWS/FCT/A8P1\)](#) /

[UP ONE LEVEL](#)

[PART 1](#)

[Jurisdiction \(/Legislation/laws/FCT/A8P1\)](#)

[NEXT](#)

[SECTION 813](#)

[Transfer To Criminal Court \(/Legislation/laws/FCT/813/\)](#)

Section 812

Procedures for family offense proceedings

Family Court (FCT)

SHARE



1. Jurisdiction. The family court and the criminal courts shall have concurrent jurisdiction over any proceeding concerning acts which would constitute disorderly conduct, unlawful dissemination or publication of an intimate image, 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 as set forth in subdivision one of section 130.60 of the penal law, 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, coercion in the second degree or coercion in the third degree as set forth in subdivisions one, two and three of section 135.60 of the penal law between spouses or former spouses, or between parent and child or between members of the same family or household except that if the respondent would not be criminally responsible by reason of age pursuant

to section 30.00 of the penal law, then the family court shall have exclusive jurisdiction over such proceeding. Notwithstanding a complainant's election to proceed in family court, the criminal court shall not be divested of jurisdiction to hear a family offense proceeding pursuant to this section. In any proceeding pursuant to this article, a court shall not deny an order of protection, or dismiss a petition, solely on the basis that the acts or events alleged are not relatively contemporaneous with the date of the petition, the conclusion of the fact-finding or the conclusion of the dispositional hearing. For purposes of this article, "disorderly conduct" includes disorderly conduct not in a public place. For purposes of this article, "members of the same family or household" shall mean the following:

(a) persons related by consanguinity or affinity;

(b) persons legally married to one another;

(c) persons formerly married to one another regardless of whether they still reside in the same household;

(d) persons who have a child in common regardless of whether such persons have been married or have lived together at any time; and

(e) persons who are not related by consanguinity or affinity and who are or have been in an intimate relationship regardless of whether such persons have lived together at any time. Factors the court may consider in determining whether a relationship is an "intimate relationship" include but are not limited to: 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. Neither a casual acquaintance nor ordinary fraternization between two individuals in business or social contexts shall be deemed to constitute an "intimate relationship".

2. Information to petitioner or complainant. The chief administrator of the courts shall designate the appropriate persons, including, but not limited to district attorneys, criminal and family court clerks, corporation counsels, county attorneys, victims assistance unit staff, probation officers, warrant officers, sheriffs, police officers or any other law enforcement officials, to inform any petitioner or complainant bringing a proceeding under this article, before such proceeding is commenced, of the procedures available for the institution of family offense proceedings, including but not limited to the following:

(a) That there is concurrent jurisdiction with respect to family offenses in both family court and the criminal courts;

(b) That a family court proceeding is a civil proceeding and is for the purpose of attempting to stop the violence, end the family disruption and obtain protection. Referrals for counseling, or counseling services, are available through probation for this purpose;

(c) That a proceeding in the criminal courts is for the purpose of prosecution of the offender and can result in a criminal conviction of the offender;

(d) That a proceeding or action subject to the provisions of this section is initiated at the time of the filing of an accusatory instrument or family court petition, not at the time of arrest, or request for arrest, if any;

(f) That an arrest may precede the commencement of a family court or a criminal court proceeding, but an arrest is not a requirement for commencing either proceeding; provided, however, that the arrest of an alleged offender shall be made under the circumstances described in subdivision four of section 140.10 of the criminal procedure law;

(g) That notwithstanding a complainant's election to proceed in family

court, the criminal court shall not be divested of jurisdiction to hear a family offense proceeding pursuant to this section.

3. Official responsibility. No official or other person designated pursuant to subdivision two of this section shall discourage or prevent any person who wishes to file a petition or sign a complaint from having access to any court for that purpose.

4. Official forms. The chief administrator of the courts shall prescribe an appropriate form to implement subdivision two of this section.

5. Notice. Every police officer, peace officer or district attorney investigating a family offense under this article shall advise the victim of the availability of a shelter or other services in the community, and shall immediately give the victim written notice of the legal rights and remedies available to a victim of a family offense under the relevant provisions of the criminal procedure law, the family court act and the domestic relations law. Such notice shall be available in English and Spanish and, if necessary, shall be delivered orally and shall include but not be limited to the following statement:

"If you are the victim of domestic violence, you may request that the officer assist in providing for your safety and that of your children, including providing information on how to obtain a temporary order of protection. You may also request that the officer assist you in obtaining your essential personal effects and locating and taking you, or assist in making arrangement to take you, and your children to a safe place within such officer's jurisdiction, including but not limited to a domestic violence program, a family member's or a friend's residence, or a similar place of safety. When the officer's jurisdiction is more than a single county, you may ask the officer to take you or make arrangements to take you and your children to a place of safety in the county where the incident occurred. If you or your children are in need of medical treatment, you have the right to

request that the officer assist you in obtaining such medical treatment. You may request a copy of any incident reports at no cost from the law enforcement agency. You have the right to seek legal counsel of your own choosing and if you proceed in family court and if it is determined that you cannot afford an attorney, one must be appointed to represent you without cost to you.

You may ask the district attorney or a law enforcement officer to file a criminal complaint. You also have the right to file a petition in the family court when a family offense has been committed against you. You have the right to have your petition and request for an order of protection filed on the same day you appear in court, and such request must be heard that same day or the next day court is in session. Either court may issue an order of protection from conduct constituting a family offense which could include, among other provisions, an order for the respondent or defendant to stay away from you and your children. The family court may also order the payment of temporary child support and award temporary custody of your children. If the family court is not in session, you may seek immediate assistance from the criminal court in obtaining an order of protection.

The forms you need to obtain an order of protection are available from the family court and the local criminal court (the addresses and telephone numbers shall be listed). The resources available in this community for information relating to domestic violence, treatment of injuries, and places of safety and shelters can be accessed by calling the following 800 numbers (the statewide English and Spanish language 800 numbers shall be listed and space shall be provided for local domestic violence hotline telephone numbers).

Filing a criminal complaint or a family court petition containing allegations that are knowingly false is a crime."

The division of criminal justice services in consultation with the state

office for the prevention of domestic violence shall prepare the form of such written notice consistent with the provisions of this section and distribute copies thereof to the appropriate law enforcement officials pursuant to subdivision nine of section eight hundred forty-one of the executive law. Additionally, copies of such notice shall be provided to the chief administrator of the courts to be distributed to victims of family offenses through the family court at such time as such persons first come before the court and to the state department of health for distribution to all hospitals defined under article twenty-eight of the public health law. No cause of action for damages shall arise in favor of any person by reason of any failure to comply with the provisions of this subdivision except upon a showing of gross negligence or willful misconduct.

UP ONE LEVEL**PART 1**[Jurisdiction \(/Legislation/laws/FCT/A8P1\)](/Legislation/laws/FCT/A8P1)**NEXT****SECTION 813**[Transfer To Criminal Court \(/Legislation/laws/FCT/813/\)](/Legislation/laws/FCT/813/)

Appendix I – New York Criminal Procedure Law § 530.11

[The Laws Of New York \(/LEGISLATION/LAWS/ALL\)](#) / [Consolidated Laws \(/LEGISLATION/LAWS/CONSOLIDATED\)](#) / [Criminal Procedure \(/LEGISLATION/LAWS/CPL\)](#) / [Part 3: Special Proceedings And Miscellaneous Procedures \(/LEGISLATION/LAWS/CPL/P3\)](#) / [Title P: Procedures For Securing Attendance At Criminal Actions And Proceedings Of Defendants And Witnesses Under Control Of Court--recognizance, Bail And Commitment \(/LEGISLATION/LAWS/CPL/P3TP\)](#) / [Article 530: Orders Of Recognizance Or Bail With Respect To Defendants In Criminal Actions And Proceedings--when And By What Courts Authorized \(/LEGISLATION/LAWS/CPL/A530\)](#) /

[PREV](#)[SECTION 530.10](#)[Order Of Recognizance Or Bail; In General \(/Legislation /laws/CPL/530.10/\)](#)[NEXT](#)[SECTION 530.12](#)[Protection For Victims Of Family Offenses \(/Legislation /laws/CPL/530.12/\)](#)

Section 530.11

SHARE

Procedures for family offense matters

Criminal Procedure (CPL)



1. Jurisdiction. The family court and the criminal courts shall have concurrent jurisdiction over any proceeding concerning acts which would constitute disorderly conduct, unlawful dissemination or publication of an intimate image, 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 as set forth in subdivision one of section 130.60 of the penal law, 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, strangulation in the first degree, strangulation in the second degree, criminal obstruction of breathing or blood circulation, 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, coercion in the second degree or coercion in the third degree as set forth in subdivisions one, two and three of section 135.60 of the penal law

between spouses or former spouses, or between parent and child or between members of the same family or household except that if the respondent would not be criminally responsible by reason of age pursuant to section 30.00 of the penal law, then the family court shall have exclusive jurisdiction over such proceeding. Notwithstanding a complainant's election to proceed in family court, the criminal court shall not be divested of jurisdiction to hear a family offense proceeding pursuant to this section. For purposes of this section, "disorderly conduct" includes disorderly conduct not in a public place. For purposes of this section, "members of the same family or household" with respect to a proceeding in the criminal courts shall mean the following:

(a) persons related by consanguinity or affinity;

(b) persons legally married to one another;

(c) persons formerly married to one another regardless of whether they still reside in the same household;

(d) persons who have a child in common, regardless of whether such persons have been married or have lived together at any time; and

(e) persons who are not related by consanguinity or affinity and who are or have been in an intimate relationship regardless of whether such persons have lived together at any time. Factors the court may consider in determining whether a relationship is an "intimate relationship" include but are not limited to: 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. Neither a casual acquaintance nor ordinary fraternization between two individuals in business or social contexts shall be deemed to constitute an "intimate relationship".

2. Information to petitioner or complainant. The chief administrator of the courts shall designate the appropriate probation officers, warrant officers, sheriffs, police officers, district attorneys or any other law enforcement officials, to inform any petitioner or complainant bringing a proceeding under this section before such proceeding is commenced, of the procedures available for the institution of family offense proceedings, including but not limited to the following:

(a) That there is concurrent jurisdiction with respect to family offenses in both family court and the criminal courts;

(b) That a family court proceeding is a civil proceeding and is for the purpose of attempting to stop the violence, end family disruption and obtain protection. That referrals for counseling, or counseling services, are available through probation for this purpose;

(c) That a proceeding in the criminal courts is for the purpose of prosecution of the offender and can result in a criminal conviction of the offender;

(d) That a proceeding or action subject to the provisions of this section is initiated at the time of the filing of an accusatory instrument or family court petition, not at the time of arrest, or request for arrest, if any;

(f) That an arrest may precede the commencement of a family court or a criminal court proceeding, but an arrest is not a requirement for commencing either proceeding.

(h) At such time as the complainant first appears before the court on a complaint or information, the court shall advise the complainant that the complainant may: continue with the proceeding in criminal court; or have the allegations contained therein heard in a family court proceeding; or proceed concurrently in both criminal and family court. Notwithstanding a

complainant's election to proceed in family court, the criminal court shall not be divested of jurisdiction to hear a family offense proceeding pursuant to this section;

(i) Nothing herein shall be deemed to limit or restrict complainant's rights to proceed directly and without court referral in either a criminal or family court, or both, as provided for in section one hundred fifteen of the family court act and section 100.07 of this chapter;

2-a. Upon the filing of an accusatory instrument charging a crime or violation described in subdivision one of this section between members of the same family or household, as such terms are defined in this section, or as soon as the complainant first appears before the court, whichever is sooner, the court shall advise the complainant of the right to proceed in both the criminal and family courts, pursuant to section 100.07 of this chapter.

3. Official responsibility. No official or other person designated pursuant to subdivision two of this section shall discourage or prevent any person who wishes to file a petition or sign a complaint from having access to any court for that purpose.

* 4. When a person is arrested for an alleged family offense or an alleged violation of an order of protection or temporary order of protection or arrested pursuant to a warrant issued by the supreme or family court, and the supreme or family court, as applicable, is not in session, such person shall be brought before a local criminal court in the county of arrest or in the county in which such warrant is returnable pursuant to article one hundred twenty of this chapter. Such local criminal court may issue any order authorized under subdivision eleven of section 530.12 of this article, section one hundred fifty-four-d or one hundred fifty-five of the family court act or subdivision three-b of section two hundred forty or subdivision two-a of section two hundred fifty-two of the domestic relations law, in

addition to discharging other arraignment responsibilities as set forth in this chapter. In making such order, the local criminal court shall consider the bail recommendation, if any, made by the supreme or family court as indicated on the warrant or certificate of warrant. Unless the petitioner or complainant requests otherwise, the court, in addition to scheduling further criminal proceedings, if any, regarding such alleged family offense or violation allegation, shall make such matter returnable in the supreme or family court, as applicable, on the next day such court is in session.

* NB Effective until January 1, 2020

* 4. When a person is arrested for an alleged family offense or an alleged violation of an order of protection or temporary order of protection or arrested pursuant to a warrant issued by the supreme or family court, and the supreme or family court, as applicable, is not in session, such person shall be brought before a local criminal court in the county of arrest or in the county in which such warrant is returnable pursuant to article one hundred twenty of this chapter. Such local criminal court may issue any order authorized under subdivision eleven of section 530.12 of this article, section one hundred fifty-four-d or one hundred fifty-five of the family court act or subdivision three-b of section two hundred forty or subdivision two-a of section two hundred fifty-two of the domestic relations law, in addition to discharging other arraignment responsibilities as set forth in this chapter. In making such order, the local criminal court shall consider de novo the recommendation and securing order, if any, made by the supreme or family court as indicated on the warrant or certificate of warrant. Unless the petitioner or complainant requests otherwise, the court, in addition to scheduling further criminal proceedings, if any, regarding such alleged family offense or violation allegation, shall make such matter returnable in the supreme or family court, as applicable, on the next day such court is in session.

* NB Effective January 1, 2020

5. Filing and enforcement of out-of-state orders of protection. A valid order of protection or temporary order of protection issued by a court of competent jurisdiction in another state, territorial or tribal jurisdiction shall be accorded full faith and credit and enforced as if it were issued by a court within the state for as long as the order remains in effect in the issuing jurisdiction in accordance with sections two thousand two hundred sixty-five and two thousand two hundred sixty-six of title eighteen of the United States Code.

(a) An order issued by a court of competent jurisdiction in another state, territorial or tribal jurisdiction shall be deemed valid if:

(i) the issuing court had personal jurisdiction over the parties and over the subject matter under the law of the issuing jurisdiction;

(ii) the person against whom the order was issued had reasonable notice and an opportunity to be heard prior to issuance of the order; provided, however, that if the order was a temporary order of protection issued in the absence of such person, that notice had been given and that an opportunity to be heard had been provided within a reasonable period of time after the issuance of the order; and

(iii) in the case of orders of protection or temporary orders of protection issued against both a petitioner, plaintiff or complainant and respondent or defendant, the order or portion thereof sought to be enforced was supported by: (A) a pleading requesting such order, including, but not limited to, a petition, cross-petition or counterclaim; and (B) a judicial finding that the requesting party is entitled to the issuance of the order which may result from a judicial finding of fact, judicial acceptance of an admission by the party against whom the order was issued or judicial finding that the party against whom the order was issued had given knowing, intelligent and voluntary consent to its issuance.

(b) Notwithstanding the provisions of article fifty-four of the civil practice law and rules, an order of protection or temporary order of protection issued by a court of competent jurisdiction in another state, territorial or tribal jurisdiction, accompanied by a sworn affidavit that upon information and belief such order is in effect as written and has not been vacated or modified, may be filed without fee with the clerk of the court, who shall transmit information regarding such order to the statewide registry of orders of protection and warrants established pursuant to section two hundred twenty-one-a of the executive law; provided, however, that such filing and registry entry shall not be required for enforcement of the order.

6. Notice. Every police officer, peace officer or district attorney investigating a family offense under this article shall advise the victim of the availability of a shelter or other services in the community, and shall immediately give the victim written notice of the legal rights and remedies available to a victim of a family offense under the relevant provisions of the criminal procedure law, the family court act and the domestic relations law. Such notice shall be prepared in Spanish and English and if necessary, shall be delivered orally, and shall include but not be limited to the following statement:

"If you are the victim of domestic violence, you may request that the officer assist in providing for your safety and that of your children, including providing information on how to obtain a temporary order of protection. You may also request that the officer assist you in obtaining your essential personal effects and locating and taking you, or assist in making arrangements to take you, and your children to a safe place within such officer's jurisdiction, including but not limited to a domestic violence program, a family member's or a friend's residence, or a similar place of safety. When the officer's jurisdiction is more than a single county, you may ask the officer to take you or make arrangements to take you and your children to a place of safety in the county where the incident occurred. If

you or your children are in need of medical treatment, you have the right to request that the officer assist you in obtaining such medical treatment. You may request a copy of any incident reports at no cost from the law enforcement agency. You have the right to seek legal counsel of your own choosing and if you proceed in family court and if it is determined that you cannot afford an attorney, one must be appointed to represent you without cost to you.

You may ask the district attorney or a law enforcement officer to file a criminal complaint. You also have the right to file a petition in the family court when a family offense has been committed against you. You have the right to have your petition and request for an order of protection filed on the same day you appear in court, and such request must be heard that same day or the next day court is in session. Either court may issue an order of protection from conduct constituting a family offense which could include, among other provisions, an order for the respondent or defendant to stay away from you and your children. The family court may also order the payment of temporary child support and award temporary custody of your children. If the family court is not in session, you may seek immediate assistance from the criminal court in obtaining an order of protection.

The forms you need to obtain an order of protection are available from the family court and the local criminal court (the addresses and telephone numbers shall be listed). The resources available in this community for information relating to domestic violence, treatment of injuries, and places of safety and shelters can be accessed by calling the following 800 numbers (the statewide English and Spanish language 800 numbers shall be listed and space shall be provided for local domestic violence hotline telephone numbers).

Filing a criminal complaint or a family court petition containing allegations that are knowingly false is a crime."

The division of criminal justice services in consultation with the state office for the prevention of domestic violence shall prepare the form of such written notice consistent with provisions of this section and distribute copies thereof to the appropriate law enforcement officials pursuant to subdivision nine of section eight hundred forty-one of the executive law.

Additionally, copies of such notice shall be provided to the chief administrator of the courts to be distributed to victims of family offenses through the criminal court at such time as such persons first come before the court and to the state department of health for distribution to all hospitals defined under article twenty-eight of the public health law. No cause of action for damages shall arise in favor of any person by reason of any failure to comply with the provisions of this subdivision except upon a showing of gross negligence or willful misconduct.

7. Rules of court regarding concurrent jurisdiction. The chief administrator of the courts, pursuant to paragraph (e) of subdivision two of section two hundred twelve of the judiciary law, shall promulgate rules to facilitate record sharing and other communication between the criminal and family courts, subject to applicable provisions of this chapter and the family court act pertaining to the confidentiality, expungement and sealing of records, when such courts exercise concurrent jurisdiction over family offense proceedings.

[PREV](#)

[SECTION 530.10](#)

[Order Of Recognizance Or Bail; In General \(/Legislation/laws/CPL/530.10/\)](#)

[NEXT](#)

[SECTION 530.12](#)

[Protection For Victims Of Family Offenses \(/Legislation/laws/CPL/530.12/\)](#)

Appendix J – New York Civil Rights Law § 52-b

[The Laws Of New York \(/LEGISLATION/LAWS/ALL\)](#) / [Consolidated Laws \(/LEGISLATION/LAWS/CONSOLIDATED\)](#) / [Civil Rights \(/LEGISLATION/LAWS/CVR\)](#) / [Article 5: Right Of Privacy \(/LEGISLATION/LAWS/CVR/A5\)](#) /

[PREV](#)

[SECTION 52-A](#)

[Private Right Of Action For Unwarranted Video Imaging Of Residential Premises \(/Legislation/laws/CVR/52-A\)](#)

[UP ONE LEVEL](#)

[ARTICLE 5](#)

[Right Of Privacy \(/Legislation/laws/CVR/A5\)](#)

Section 52-B

SHARE

Private right of action for unlawful dissemination or publication of an intimate image

Civil Rights (CVR)



Private right of action for unlawful dissemination or publication of an intimate image. 1. Any person depicted in a still or video image, regardless of whether or not the original still or video image was consensually obtained, shall have a cause of action against an individual who, for the purpose of harassing, annoying or alarming such person, disseminated or published, or threatened to disseminate or publish, such still or video image, where such image:

a. was taken when such person had a reasonable expectation that the image would remain private; and

b. depicts (i) an unclothed or exposed intimate part of such person; or (ii) such person engaging in sexual conduct, as defined in subdivision ten of section 130.00 of the penal law, with another person; and

c. was disseminated or published, or threatened to be disseminated or published, without the consent of such person.

2. In any action commenced pursuant to subdivision one of this section,

the finder of fact, in its discretion, may award injunctive relief, punitive damages, compensatory damages and reasonable court costs and attorney's fees.

3. This section shall not apply to the following:

a. the reporting of unlawful conduct;

b. dissemination or publication of an intimate still or video image made during lawful and common practices of law enforcement, legal proceedings or medical treatment;

c. images involving voluntary exposure in a public or commercial setting;
or

d. dissemination or publication of an intimate still or video image made for a legitimate public purpose.

4. Any person depicted in a still or video image that depicts an unclothed or exposed intimate part of such person, or such person engaging in sexual conduct as defined in subdivision ten of section 130.00 of the penal law with another person, which is disseminated or published without the consent of such person and where such person had a reasonable expectation that the image would remain private, may maintain an action or special proceeding for a court order to require any website that is subject to personal jurisdiction under subdivision five of this section to permanently remove such still or video image; any such court order granted pursuant to this subdivision may direct removal only as to images that are reasonably within such website's control.

5. a. Any website that hosts or transmits a still or video image, viewable in this state, taken under circumstances where the person depicted had a reasonable expectation that the image would remain private, which depicts:

(i) an unclothed or exposed intimate part, as defined in section 245.15 of the penal law, of a resident of this state; or

(ii) a resident of this state engaging in sexual conduct as defined in subdivision ten of section 130.00 of the penal law with another person; and

b. Such still or video image is hosted or transmitted without the consent of such resident of this state, shall be subject to personal jurisdiction in a civil action in this state to the maximum extent permitted under the United States constitution and federal law.

6. A cause of action or special proceeding under this section shall be commenced the later of either:

a. three years after the dissemination or publication of an image; or

b. one year from the date a person discovers, or reasonably should have discovered, the dissemination or publication of such image.

7. Nothing herein shall be read to require a prior criminal complaint, prosecution or conviction to establish the elements of the cause of action provided for by this section.

8. The provisions of this section are in addition to, but shall not supersede, any other rights or remedies available in law or equity.

9. If any provision of this section or its application to any person or circumstance is held invalid, the invalidity shall not affect other provisions or applications of this section which can be given effect without the invalid provision or application, and to this end the provisions of this section are severable.

10. Nothing in this section shall be construed to limit, or to enlarge, the protections that 47 U.S.C § 230 confers on an interactive computer service for content provided by another information content provider, as such terms are defined in 47 U.S.C. § 230.

[PREV](#)

[SECTION 52-A](#)

[Private Right Of Action For Unwarranted Video Imaging Of Residential Premises \(/Legislation/laws/CVR/52-A/\)](#)

[UP ONE LEVEL](#)

[ARTICLE 5](#)

[Right Of Privacy \(/Legislation/laws/CVR/A5\)](#)

Appendix K – New York Penal Law § 245.15

[The Laws Of New York \(/LEGISLATION/LAWS/ALL\)](#) / [Consolidated Laws \(/LEGISLATION/LAWS/CONSOLIDATED\)](#) / [Penal \(/LEGISLATION/LAWS/PEN\)](#) / [Part 3: Specific Offenses \(/LEGISLATION/LAWS/PEN/P3\)](#) / [Title N: Offenses Against Public Order, Public Sensibilities And The Right To Privacy \(/LEGISLATION/LAWS/PEN/P3TN\)](#) / [Article 245: Offenses Against Public Sensibilities \(/LEGISLATION/LAWS/PEN/P3TNA245\)](#) /

[PREV](#)[SECTION 245.11](#)[Public Display Of Offensive Sexual Material \(/Legislation/laws/PEN/245.11/\)](#)[UP ONE LEVEL](#)[ARTICLE 245](#)[Offenses Against Public Sensibilities \(/Legislation/laws/PEN/P3TNA245\)](#)

Section 245.15

Unlawful dissemination or publication of an intimate image

Penal (PEN)

SHARE



1. A person is guilty of unlawful dissemination or publication of an intimate image when:

(a) with intent to cause harm to the emotional, financial or physical welfare of another person, he or she intentionally disseminates or publishes a still or video image of such other person, who is identifiable from the still or video image itself or from information displayed in connection with the still or video image, without such other person's consent, which depicts:

(i) an unclothed or exposed intimate part of such other person; or

(ii) such other person engaging in sexual conduct as defined in subdivision ten of section 130.00 of this chapter with another person; and

(b) such still or video image was taken under circumstances when the person depicted had a reasonable expectation that the image would remain private and the actor knew or reasonably should have known the person depicted intended for the still or video image to remain private, regardless

of whether the actor was present when the still or video image was taken.

2. For purposes of this section "intimate part" means the naked genitals, pubic area, anus or female nipple of the person.

2-a. For purposes of this section "disseminate" and "publish" shall have the same meaning as defined in section 250.40 of this title.

3. This section shall not apply to the following:

(a) the reporting of unlawful conduct;

(b) dissemination or publication of an intimate image made during lawful and common practices of law enforcement, legal proceedings or medical treatment;

(c) images involving voluntary exposure in a public or commercial setting;
or

(d) dissemination or publication of an intimate image made for a legitimate public purpose.

4. Nothing in this section shall be construed to limit, or to enlarge, the protections that 47 U.S.C § 230 confers on an interactive computer service for content provided by another information content provider, as such terms are defined in 47 U.S.C. § 230.

Unlawful dissemination or publication of an intimate image is a class A misdemeanor.

[PREV](#)

[SECTION 245.11](#)

[Public Display Of Offensive Sexual Material \(/Legislation/laws/PEN/245.11/\)](#)

[UP ONE LEVEL](#)

ARTICLE 245

Offenses Against Public Sensibilities (/Legislation/laws/PEN/P3TNA245)



Device and Data Access when Personal Safety is At Risk

What's in this guide?

Apple makes it easy to connect and share your life with the people closest to you. What you share, and whom you share it with, is up to you — including the decision to make changes to better protect your information or personal safety.

If you'd like to revisit what you share with other people, or restore your device's original settings for any reason, this guide can help you understand what information you are sharing via your Apple devices, and how to make changes to protect your safety. It includes step-by-step instructions on how to remove someone's access to information you've previously granted: from location data on the Find My app, to meetings you've scheduled via Calendar.

If you're concerned that someone is accessing information you did not share from your Apple device, this guide will also help you identify risks, and walk you through the steps to help make the technology you rely on as private and secure as you want it to be.

Contents

Update your software	3
Restoring your device to factory settings	3
Protect your device	4
Protect your Apple ID	5
If you don't recognize a sign-in location	7
Check privacy settings	8
Using the Find My app	9
Sharing your location	10
Sharing with iCloud	11
Shared Albums in Photos	12
Shared Calendars	12
Sharing your Activity with Apple Watch	13
Delete unknown third-party apps	14
Delete unknown configuration profiles	15
If you use Family Sharing	16
Phishing and fraudulent requests to share info	17
Checklist: If you want to see if anyone else has access to your device or accounts	18
Checklist: If you want to stop sharing with someone whom you previously shared with	19
Checklist: If you want to make sure no one else can see your location	20

Update your software

Updating your software is one of the most important things you can do to protect your device and your information.

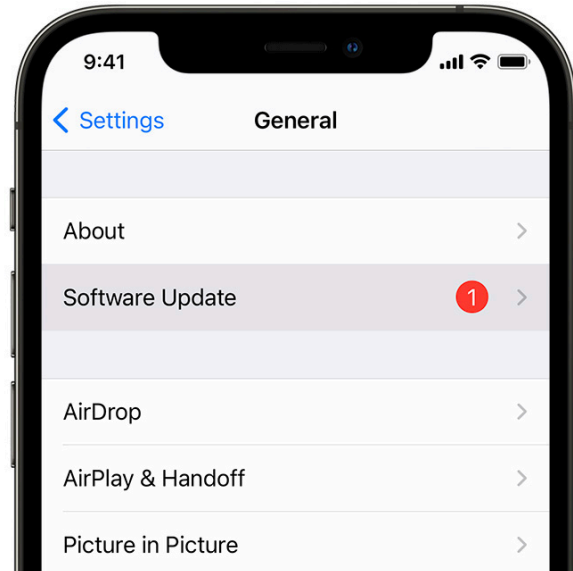
- On iPhone, iPad, or iPod touch, you can see the software version you are running by going to Settings > General > Software Update.
- On your Mac, go to System Preferences > Software Update.

If there is a software update [available for your device](#), download and install it.

If you have iOS 12 or later, you can also enable automatic updates from the Software Updates menu.

[Update your iPhone, iPad, or iPod touch](#)

[How to update the software on your Mac](#)



Restoring your device to factory settings

If you are not running the latest version of iOS and have concerns that someone else may have had physical access to your device, you should back up the information from your device and restore the device to factory settings. This process can take some time, but it will ensure that your device is accessible only by you, while preserving all of your information.

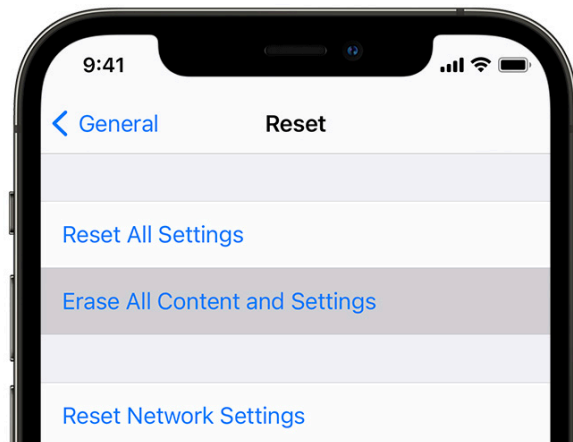
To erase your device and restore it to factory settings:

1. Go to Settings > General > Reset then tap Erase all Contents and Settings.
2. Enter your passcode or Apple ID password.
3. Wait for your device to erase.

[How to back up your iPhone, iPad, and iPod touch](#)

[How to erase your iPhone, iPad, or iPod touch](#)

[How to erase a disk for Mac](#)



Protect your device

To prevent anyone except you from using your devices and accessing your information, make sure you use unique passcodes or passwords **that only you know**, and use Touch ID or Face ID on your iPhone or iPad.

Face ID allows you to set up an alternate appearance, so that Face ID still recognizes you if you have an appearance that can look vastly different. Touch ID allows you to add additional fingerprints.

If you believe someone else knows your device passcode or may have added an alternate appearance or fingerprint on your device, you can reset or remove these in Settings using the instructions at these pages:

[Use a passcode with your iPhone, iPad, or iPod touch](#)

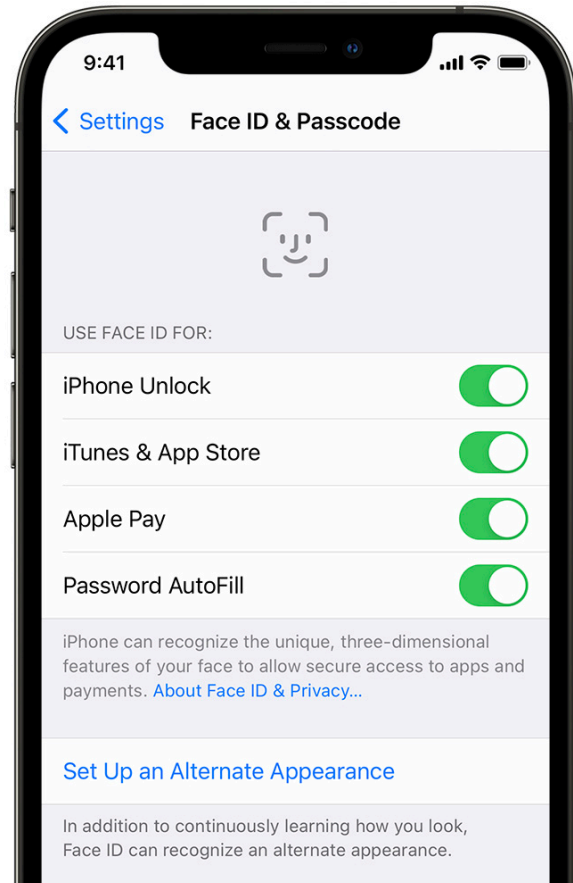
[Use Face ID on your iPhone or iPad Pro](#)

[If Face ID isn't working on your iPhone or iPad Pro](#)

[Use Touch ID on iPhone and iPad](#)

[Change or reset the password of a macOS user account](#)

[Use Touch ID on your Mac](#)



Protect your Apple ID

Your Apple ID is the personal account that you use to sign into your device and access Apple services. This includes services like the App Store, iCloud, iMessage, FaceTime, and Find My, and personal information that you store with Apple and share across devices, like contacts, payment info, photos, device backups, and much more.

Here are a few important things you can do to secure your Apple ID and protect your privacy:

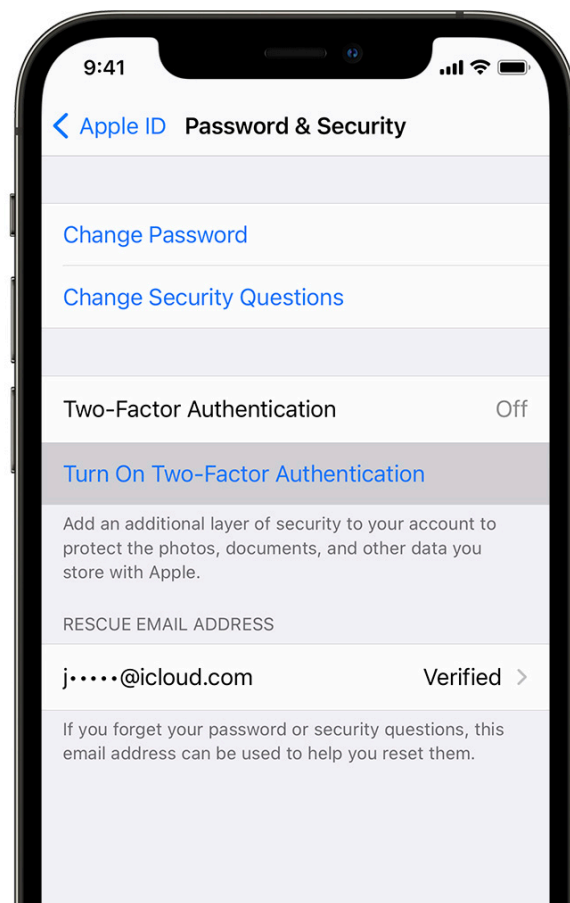
1. Don't share your Apple ID password with anyone, even family members. If you share an Apple ID, you're giving someone else access to all your personal data and your content. If someone else set up your Apple ID and password, you should change your password. You can use [Family Sharing](#) to share information and services without sharing accounts.
2. Use two-factor authentication for your Apple ID. Two-factor authentication is designed to ensure that you're the only person who can access your account, even if someone knows your password. With two-factor authentication, you'll need to provide your password and a six-digit verification code that automatically appears on your trusted device(s) when you want to sign in to a new device for the first time.

You must verify at least one trusted phone number—a number where you can receive verification codes by text message or automated phone call—to enroll in two-factor authentication.

3. Pay attention to notifications about your Apple ID. Apple notifies you by email, text, or push notification when changes are made to your account, such as when you sign in for the first time on a new device or when your password is changed, so it's important to keep your contact information up to date.

To check and update your Apple ID security information, go to Settings > [your name].

Tap Name, Phone Numbers, Email to see and update personal information. Tap Password & Security to see your trusted phone numbers, whether two-factor authentication is on, and trusted devices. You can also view and update this info at your Apple ID account page: appleid.apple.com.



If you think your Apple ID has been compromised, follow these steps to review your account information and protect your account:

1. Change your Apple ID password and choose a strong password—eight or more characters, including upper and lowercase letters, and at least one number.
2. Review all the personal and security information in your account. Update any information that isn't correct or that you don't recognize, including your name, your primary Apple ID email address, and phone number(s).
3. If you have two-factor authentication enabled, review your trusted devices on iOS, by going to Settings > [your name] and review the devices listed. If you see a device that you don't recognize or haven't authorized to use your account, you can select it and tap Remove from Account.
4. If you haven't yet, set up two-factor authentication by going to Settings > [your name] > Password & Security. You may be asked to enter your Apple ID password to access these features. Tap Turn On Two-Factor Authentication.

[Sign in with your Apple ID](#)

[Change your Apple ID password](#)

[If you forgot your Apple ID password](#)

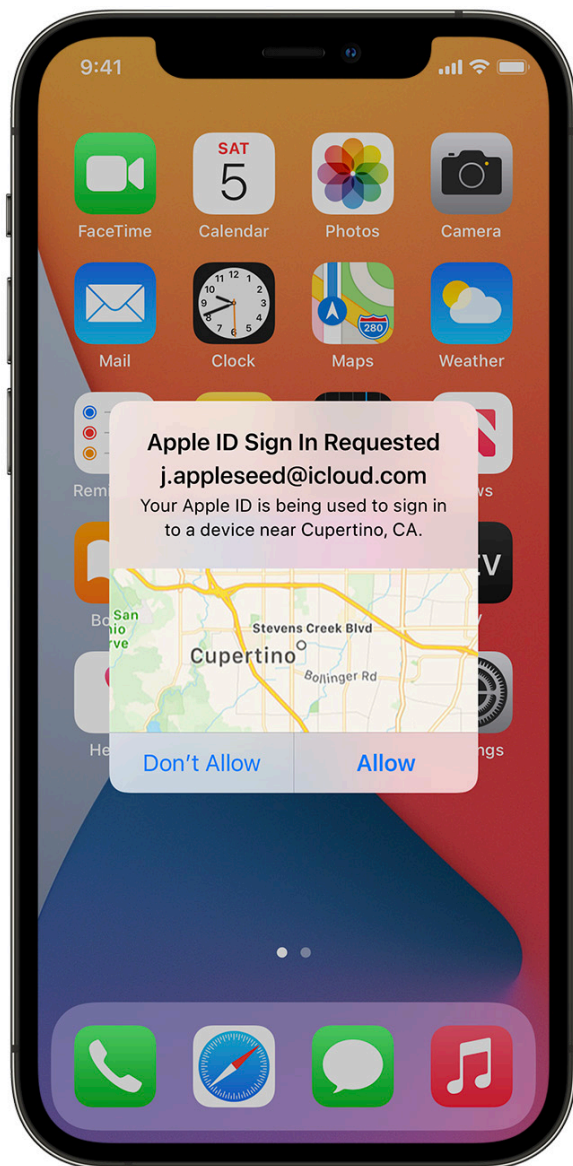
[Two-factor authentication for Apple ID](#)

[If you think your Apple ID has been compromised](#)

If you don't recognize a sign-in location

When you sign in on a new device, you get a notification on your other trusted devices. The notification includes a map of the location of the new device. This is an approximate location based on the IP address or network that the device is currently using, rather than the exact location of the device.

If you see a notification that your Apple ID is being used to sign in on a new device, and you're not signing in, tap **Don't Allow** to block the sign-in attempt.

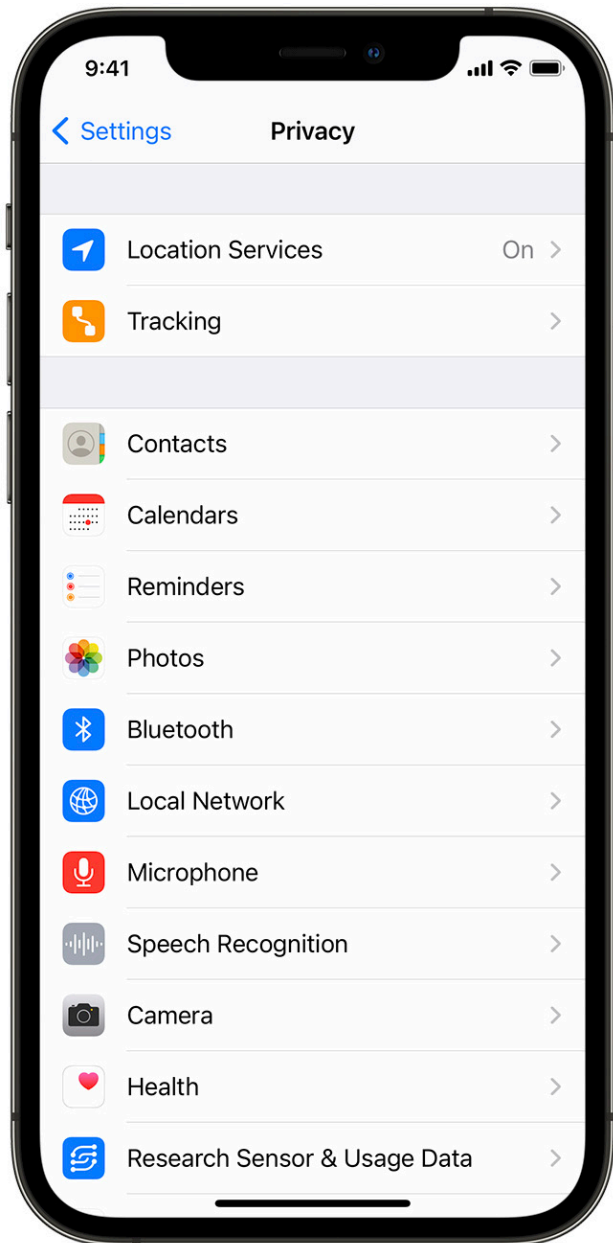


Check privacy settings

Privacy settings on your device have been carefully designed to put you in control of your data. For example, you can allow a social-networking app to use your camera so you can take and upload pictures to that app. You can also grant access to Contacts so a messaging app can find any friends that are already using the same app.

In Settings > Privacy, you can see the apps you have allowed to access certain information—such as Location Services, Contacts, Camera, Files & Folders, and more—as well as grant or revoke any future access to this info.

Select a type of data from the list to see which apps have asked for permission to use that data. An app won't appear on the list until it asks for permission, and you can grant or remove permission from any app that has asked for access. An app can use the data type in the setting only if you have given the app permission.



Using the Find My app

The Find My app for iPhone, iPad, and Mac helps keep you connected to your device even if it's lost or stolen and allows you to share your location with friends and family members.

You can use Find My to locate your friends and family and to share your location—your location is not shared by default. Share My Location, in the Me tab, must be on to share your location with friends, family, and contacts.

To see people with whom you are sharing your location, go to the People tab. When someone shares their location with you, you can choose to share your location back, or not.

You can stop sharing your location with a particular person in the People tab. Just choose the person, scroll down and select Stop Sharing My Location. Or you can stop sharing with everyone by turning off Share My Location in the Me tab.

If you stop sharing your location in Find My, the person will not receive a notification, but they will not be able to see you on their list of friends. If you re-enable sharing, they get a notification that you have started sharing your location with them.

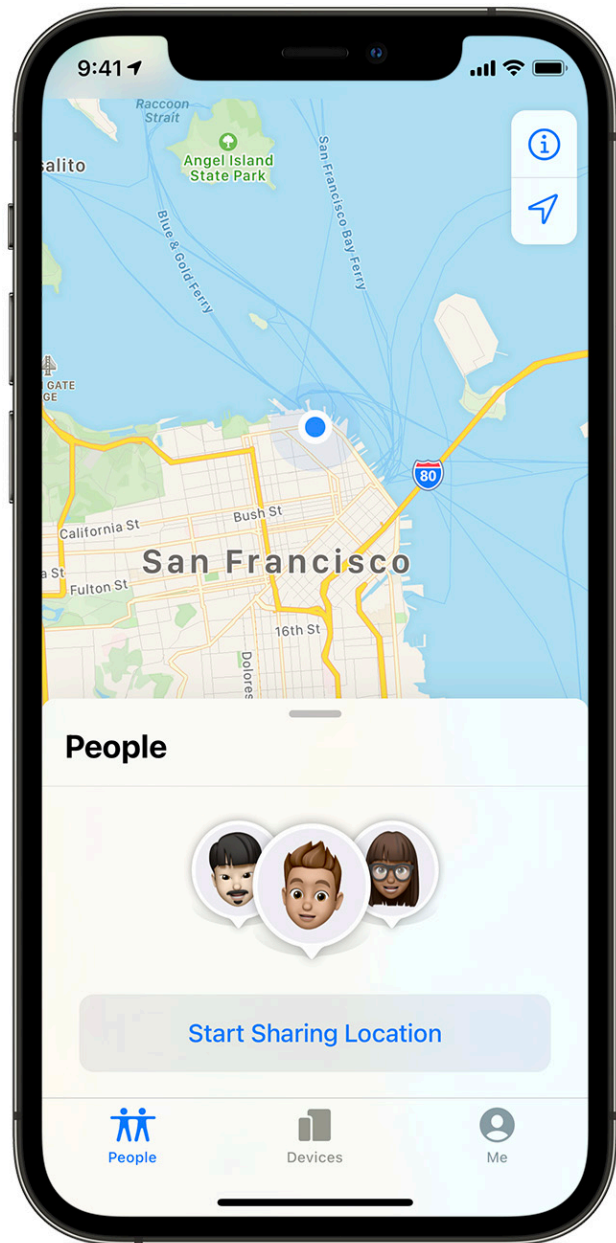
If you shared your location from iMessage rather than the Find My app, and you stop sharing, the person you stop sharing with sees a notification that you have stopped sharing your location.

If you set up [Family Sharing](#) and use Location Sharing, your family members automatically appear in the People tab, although they still have to share their location with you.

[Set up Find My on your iPhone, Mac, and other devices](#)

[Locate a lost or stolen device](#)

[Find friends and share your location with Find My](#)



Sharing your location

With your permission, Location Services allows apps and websites (including Maps, Camera, Weather, and other apps) to use location information, such as from cellular, Wi-Fi, Global Positioning System (GPS) networks, and Bluetooth to determine your approximate location. The first time an app tries to access your location, it must ask for your permission. You see a prompt explaining which app is asking for permission to use your location as well as the app developer's reason for requesting it.



To stop sharing your location with apps and services, for even a short period of time, go to Settings > Privacy > Location Services and turn off location sharing. This stops all apps on your device, such as Maps, from using your location. No one is notified if you turn off location services, but features may not work as expected without access to your location.

In Settings > Privacy > Location Services, you can also grant access to your location for individual apps and indicate how often the app may use your location.

To stop sharing your location with friends through the Find My app, turn off the Location Sharing option in the Me tab in Find My.

Note: Your device's location information may be used for emergency calls to aid response efforts, regardless of whether Location Services is on.

[About privacy and Location Services in iOS and iPadOS](#)

[Manage which apps can detect your Mac location](#)

Sharing with iCloud

iCloud securely stores your photos, videos, documents, music, apps, and more and keeps them updated across all your devices. iCloud also allows you to share photos, calendars, your location, and more with friends and family.

You sign in to iCloud—on your device or the web— with your Apple ID. See detailed information about [what is stored in iCloud](#).

You can view and change your iCloud settings on each device, including which Apple apps and third-party apps use iCloud, iCloud backups and more.

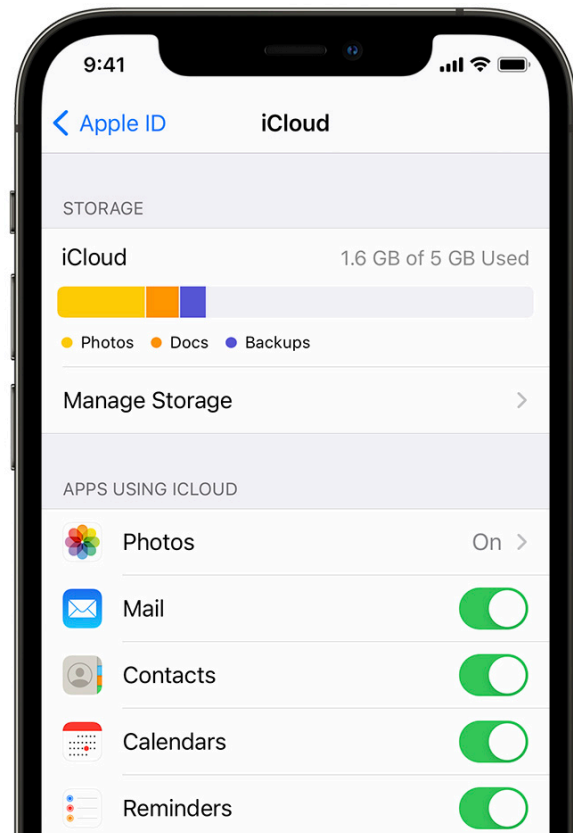
- On your iPhone, iPad, or iPod touch, go to Settings > [your name] > iCloud.
- On your Mac, go to System Preferences > Apple ID > iCloud.

You can also sign out of iCloud completely on a device. If you sign out of iCloud, it no longer backs up the information on that device.

- On your iPhone, go to Settings > [your name], scroll down and tap Sign Out.
- On your Mac, choose Apple menu > System Preferences. Click Apple ID, then click Overview, then click Sign Out.

[Change your iCloud feature settings](#)

[Sign out of iCloud on your iPhone, iPad, iPod touch, Apple TV, or Mac](#)



Shared Albums in Photos

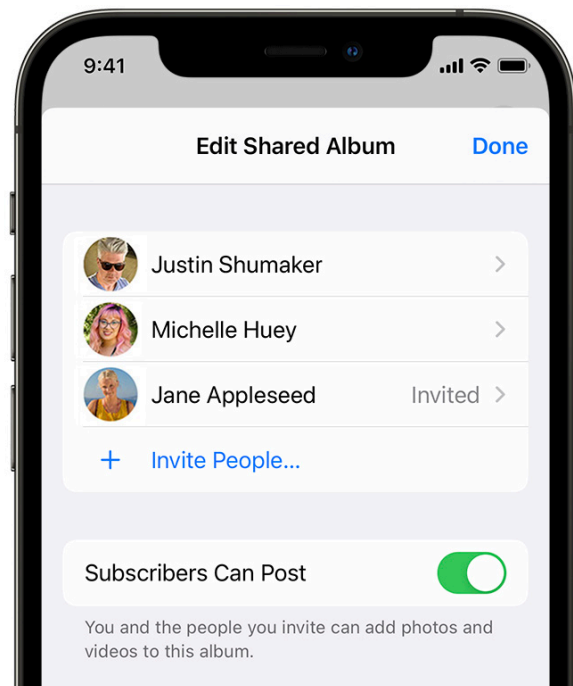
With Shared Albums in Photos, you choose the photos and videos you want to share, and the people you want to share them with. You can change your sharing settings anytime.

To see who you have shared albums with, go to Photos > Albums > Shared Albums. Select a shared album and tap the People tab to see the owner of the shared album and who the album is shared with.

If you are the album owner and would like to stop sharing, tap the name of the subscriber for options.

If you are a subscriber to a shared album, you can delete any photos that you shared. You can also select Unsubscribe from the bottom of the screen. If you stop sharing a photo or an album with someone, they will not receive a notification.

[How to share albums in Photos](#)



Shared Calendars

If you have previously invited a person to share your calendar, you can manage their ability to edit the calendar, or stop sharing the calendar with that person.

To see who you have shared a Calendar with, go to Calendar > Calendars. Select a shared calendar and tap the Info icon to see who the album is shared with.

If you're the Calendar owner and would like to stop sharing, tap the name of the subscriber for options. If you're a subscriber, you can select Delete Calendar from the bottom of the screen.

[Share iCloud calendars on iPhone](#)

[Share iCloud calendars on Mac](#)

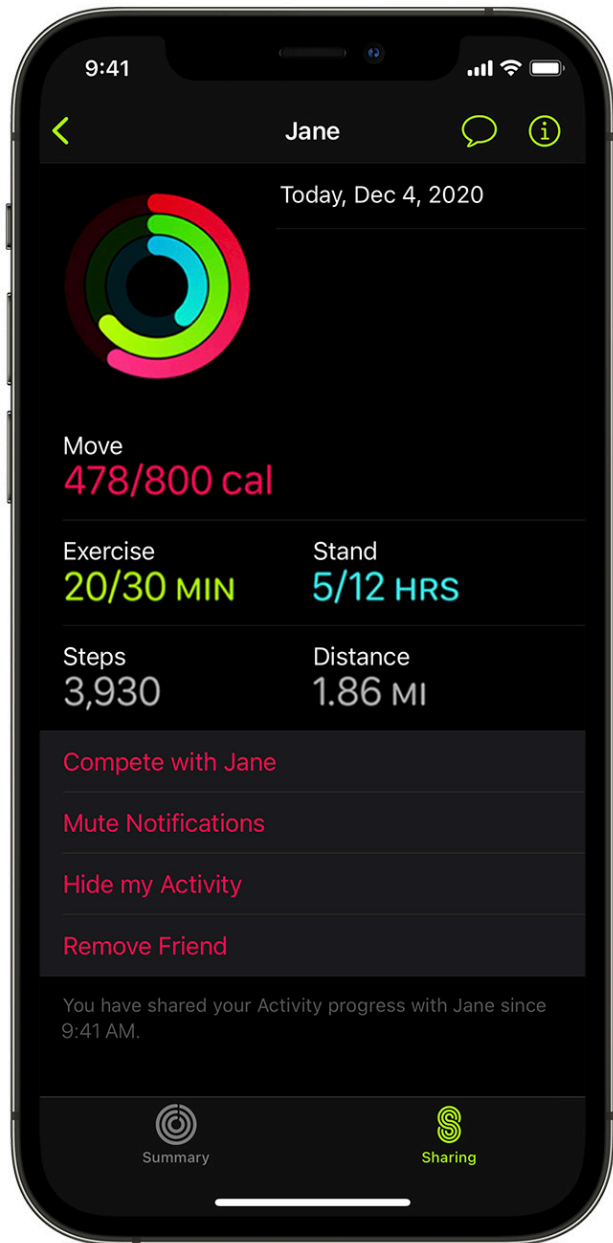


Sharing your Activity with Apple Watch

If you have an Apple Watch and previously shared your Activity rings with someone, they can see information about your activity level and workouts. It doesn't give them any information about your location.

You can hide your progress, or stop sharing your activity with a particular person entirely, from the Sharing tab in the Activity app. There are no notifications if you stop sharing your activity.

[Share your Activity and compete with friends with your Apple Watch](#)



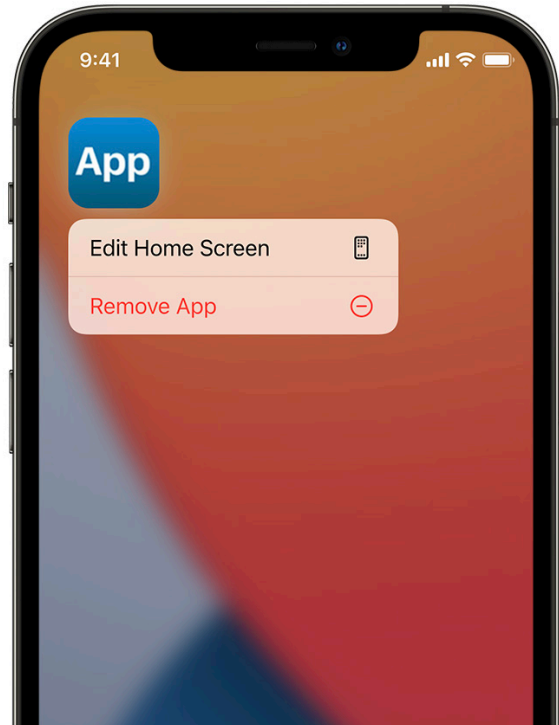
Delete unknown third-party apps

If you notice an app has permission to access your data, and you don't remember installing it or giving it permission to access your data, you may want to delete the app.

To delete an app on your iPhone, iPad, or iPod touch, touch and hold the app. Tap Remove App. Tap Delete App, then tap Delete to confirm.

[How to delete apps on your iPhone, iPad, and iPod touch](#)

[How to delete apps on your Mac](#)



Delete unknown configuration profiles

Device profiles, Mobile Device Management (MDM) tools, and custom apps may be used by companies or educational institutions to manage devices, and these tools may allow access to data or location information on the device.

If you see a profile installed on your device, and don't know of any reason for it, you can remove it and delete any associated apps. If your device belongs to your school or organization, check with your system administrator before deleting a necessary app or profile.

To remove a profile or MDM configuration from your iPhone, iPad, or iPod touch, go to Settings > General > Profiles & Device Management.* Select the profile, tap Delete Profile, and follow the onscreen instructions. Restart your device.

On your Mac, go to System Preferences, then click Profiles. Click the suspicious profile to select it, then click the Remove button (-) below the list of profiles. Click Remove to confirm. Restart your Mac.

*If you don't see this option in Settings, then no device management profiles are installed on your device.

[How to delete an app that has a configuration profile on your iPhone, iPad, or iPod touch](#)

[Use configuration profiles to standardize settings on Mac computers](#)



If you use Family Sharing

If you want to share purchases, photos, a calendar, and more with someone else, you can use Family Sharing, Shared Albums in Photos, or other easy-to-use sharing features.

Family Sharing makes it easy to share—App Store, music, movie, TV, and book purchases, subscriptions to [Apple Music](#), [Apple Arcade](#), [Apple News+](#), or [Apple TV+](#), [iCloud storage](#), and much more—without sharing each other's Apple accounts.

One adult in your household, the organizer, chooses the features the family will share and can invite up to five additional members to join. After the family members join, Family Sharing is set up on everyone's devices automatically—including a shared calendar and shared photo album. The family organizer can add anyone who has an Apple ID to their family and remove anyone over the age of 13 from the family group.

You can check if you're already part of a family in Settings > [your name]:

- If you see Set Up Family Sharing, you are not using Family Sharing with this Apple ID.
- If you see an icon with Family Sharing, you can tap the icon to see your family members and roles.

If the family organizer turns off Family Sharing, it removes all family members from the family group at once. If there are children under 13 (age varies by country/region) in the family group, you must transfer them to another family before you can disband yours.

Also, any family member over the age of 13 can remove themselves from a family group at any time. Just tap your name and then tap Leave Family. You can also sign in to appleid.apple.com and choose Remove Account in the Family Sharing section.

For security reasons, a child (under 13) account cannot remove themselves from a family and cannot stop sharing details such as Screen Time without the Screen Time passcode. If you use a child account, the family organizer has access to shared family content on your device, such as shared photo albums and shared calendars, and can view Screen Time activity.

[Family Sharing](#)

[Leave Family Sharing](#)

Phishing and fraudulent requests to share info

Phishing refers to fraudulent attempts to get personal information from you.

Use caution if you receive unsolicited messages prompting you to accept gifts, download documents, install software or follow suspicious links. People who want to access your personal information use any means they can—spoofed emails and texts, misleading pop-up ads, fake downloads, calendar spam, even phony phone calls—to trick you into sharing information, such as your Apple ID or password, or to get you to provide a verification code for two-factor authentication.

You can use the tips at the page below to avoid being tricked into compromising your accounts or personal information.

[Recognize and avoid phishing messages, phony support calls, and other scams](#)

Checklist: If you want to see if anyone else has access to your device or accounts

- 1** Check which devices are signed in with your Apple ID by going to Settings > [your name]. If you see a device you don't recognize, tap the device name and select Remove from Account.
- 2** Check to see if there is an unexpected alternate appearance or additional fingerprint set up on your device by following the instructions to [use Face ID on your iPhone or iPad Pro](#) or [use Touch ID on iPhone and iPad](#).
- 3** Sign in to appleid.apple.com with your Apple ID and review all the personal and security information in your account to see if there is any information that someone else has added. Make sure all your information is up to date. If you have two-factor authentication turned on, review trusted devices for any devices that you do not recognize. If your account doesn't use two-factor authentication, [turn it on](#) now.
- 4** Review the installed apps on your device and look for apps you don't recognize or don't remember installing. You can look up any apps you find in the App Store to see what their purpose is.
- 5** Mobile Device Management (MDM) profiles are typically installed by employers, schools, or other official organizations, and allow additional privilege and access to a device. Look for an unknown MDM profile on your iPhone, iPad, or iPod touch in Settings > General > Profiles & Device Management. If you don't see this option in Settings, your device doesn't have any profiles installed.

Checklist: If you want to stop sharing with someone whom you previously shared with

- 1** Check Family Sharing settings by going to Settings > [your name]. If you're in a family, the names of the family members are visible. If you're part of a family, you can remove yourself from the family group as long as the account lists your age as over 13. If you're the family organizer, you can remove anyone over the age of 13 from the family.
- 2** In the Find My app, select the People tab to see with whom you share your location. Tap a person and tap Stop Sharing My Location, or to stop sharing with everyone, turn off Share My Location in the Me tab.
- 3** In the Photos app, go to Albums and then go to Shared Albums. Select a shared album and tap People to see the owner of the shared album and with whom the album is shared. If you're the album owner, tap the name of a subscriber for the option to remove them. If you're a subscriber, select Unsubscribe from the bottom of the screen. You can also delete any photos that you shared.
- 4** In the Calendar app, select Calendars. Select a shared calendar and tap Info to see with whom the album is shared. If you're the calendar owner, tap the name of the subscriber for the option to remove them. If you're a subscriber, you can tap Delete Calendar from the bottom of the screen.
- 5** If you have an Apple Watch and shared your Activity rings with someone, you can choose to stop sharing. In the Fitness app on your iPhone, tap the Sharing tab. Tap the person icon to see who you share with, click on the person's name and select either Remove Friend or Hide my Activity.
- 6** You can choose to share information with others through third-party apps as well. Review the apps that you installed on your device to see if any of them are sharing information, and follow their instructions to stop sharing. You can also delete the app.
- 7** If you're not running the latest version of iOS and have concerns that someone else may have had physical access to your device, or if someone else set your device up for you, you can backup the information from your device and restore it to factory settings. Learn [how to back up your iPhone, iPad, and iPod touch](#) and [how to erase your iPhone, iPad, or iPod touch](#).

Checklist: If you want to make sure no one else can see your location

- 1** To stop sharing your location with apps and services, for even a short period of time, go to Settings > Privacy > Location Services and turn off Location Services. This stops apps on your device, such as Maps, from using your location. No one is notified when you turn off location services, but some features may not work as expected without access to your location.
- 2** If you need to use certain apps that require location permissions, such as Maps or ride sharing apps, you can give app permission individually by going to Settings > Privacy > Location Services and allowing only certain apps to use location services.
- 3** To Stop sharing location in the Find My app, go to Settings > Privacy > Share My Location and turn off Share My Location. If you're concerned someone may have access to your Apple ID, you can also temporarily turn off Find My iPhone in this tab.
- 4** You can stop sharing your location with a particular person by going to the Find My app, going to the People tab, select the individual and tap Stop Sharing My Location. If you stop sharing your location in Find My, the person will not receive a notification, but they will not be able to see you on their list of friends. If you re-enable sharing, they get a notification that you have started sharing your location with them.
- 5** You can also choose to share your location with others using third-party apps. If you haven't turned off Location Services in Privacy Settings, conduct a review of apps you have installed on your device to see if any of them are sharing your location, and follow the relevant instructions to stop sharing.