NATIONAL WOMEN'S LAW CENTER

Technology-Facilitated Abuse: Recent Developments in the Law and Guidance for Supporting Survivors

Legal Network for Gender Equity Webinar	**5 December 2024** **3:00–4:30 pm**

LEGAL NETWORK FOR GENDER EQUITY
NATIONAL WOMEN'S LAW CENTER FUND LLC

TIME'S UP
LEGAL DEFENSE FUND

Today's Presenters

Dr. Mary Anne Franks (she/her)
Eugene L. and Barbara A. Bernard Professor in Intellectual Property, Technology, and Civil Rights Law, George Washington Law School and *President and Legislative & Tech Policy Director*, Cyber Civil Rights Initiative

Annie Seifullah (she/her)
Founding Partner, Incendii Law PLLC and *Co-chair*, New York Cyber Abuse Task Force

Lindsey M. Song (she/her)
Associate Program Director of the Family Law Project, Queens Family Justice Center, Sanctuary for Families and *Co-chair*, New York Cyber Abuse Task Force

Dr. Mary Anne Franks (she/her) is the Eugene L. and Barbara A. Bernard Professor in Intellectual Property, Technology, and Civil Rights Law at George Washington Law School. Her areas of expertise include First Amendment law, Second Amendment law, law and technology, criminal law, and family law. Dr. Franks also serves as the President and Legislative & Tech Policy Director of the Cyber Civil Rights Initiative, the leading U.S.-based nonprofit organization focused on image-based sexual abuse.

Her model legislation on the non-consensual distribution of intimate images (NDII, sometimes referred to as “revenge porn”) has served as the template for multiple state and federal laws, and she is a frequent advisor to the federal government, state and federal lawmakers, and tech companies on privacy, free expression, and safety issues. Dr. Franks is the author of the award-winning book, *The Cult of the Constitution* (Stanford Press, 2019); her second book, *Fearless Speech* (Bold Type Books) was published in October 2024. She holds a JD from Harvard Law School and a DPhil from Oxford University, where she studied as a Rhodes Scholar. She is an Affiliate Fellow of the Yale Law School Information Society Project and a member of the District of Columbia bar.

Annie Seifullah, Esq. (she/her) is the Founder and Owner of Incendii Law, PLLC, a woman-owned, woman-led law firm in New York City that specializes in fighting powerful predators including serial abusers, banks and lenders, and prisons. Annie specializes in representing survivors looking to recover money damages from those harmed them -- or the organizations that aided or enabled the abuse that they suffered. Annie's proudest legal achievements include six- and seven- figure payouts to victims of child abuse and sexual assault, a 7-figure settlement against a police force for wrongful imprisonment, and countless final orders of protection for individuals escaping physically, emotionally, and technologically abusive relationships.

Annie's ability to deeply connect to her clients and fiercely advocate for them is an outcome of being a survivor of intimate partner violence and image based sexual abuse (formerly known as "revenge porn"). Relying upon her own experiences and advocacy work, Annie authored the book *Scarlet Hashtag: Transform Your Public Shame into Your Power* to help others who are working to overcome the same. Annie is also the co-chair of the New York Cyber Abuse Task Force, a coalition of agencies, attorneys, and advocates working to end technology-facilitated abuse.

Annie received her Bachelor of Arts from University of Utah in 2001, an M.A. in Secondary English Education from CUNY City College of New York in 2005, and a Juris Doctor from CUNY School of Law in 2018. She lives in Queens with her partner Sam and her son, Khalil, who is the center of her world.

Lindsey M. Song, Esq. (she/her) is the current Associate Program Director of the Family Law Project, Queens Family Justice Center (QFJC) at Sanctuary for Families. As Associate Program Director, Lindsey supervises the Sanctuary Family Law team at the QFJC in providing consultations, screenings, and representation to intimate partner violence survivors in Queens. Prior to joining Sanctuary in 2015, Lindsey received a Juris Doctor degree from Georgetown University Law Center in 2014.

Since 2016, Lindsey has lead the New York Cyber Abuse Task Force (NYCATF) as Co-Chair. The NYCATF is a collaboration of agencies, attorneys, and advocates working to end technology-facilitated intimate partner abuse in all its forms, which includes but is not limited to the non-consensual dissemination, or threat of dissemination, of sexual images, including deep fake images (cyber sexual abuse/nonconsensual pornography), hacking, stalking, spoofing, harassment, identity theft, impersonation, and more.

In her time as Co-Chair of the Task Force, Lindsey has become a nationally recognized expert in the area of technology-facilitated abuse and gender-based violence, presenting at White House Roundtables on the issue in 2023 and 2024, and featured in the Atlantic, New York Times, CBS, BuzzFeed News, The New York Post, and other publications for her knowledge and expertise. She has presented at over 150 trainings including technology-facilitated abuse, ethics, evidence, and other related topics to educational, governmental, and nonprofit agencies as well as corporations including the New York City Family Justice Centers, the NYS Unified Court System Family Violence Task Force, NYS Integrated Domestic Violence Courts, several District Attorney's Offices, Bar Associations, the Practicing Law Institute; state, local, and national nonprofits; medical schools; dozens of law firms and local area law schools, and others. Lindsey has also organized dozens of conferences and trainings addressing the intersection of tech abuse and intimate partner violence, including presentations with international representation and advocates from criminal, civil, and related areas of law and policy.

Today's Agenda

Part I	Introductions
Part II	Updates to legislation, policy, and federal case law
Part III	Recent trends in how technology is being used
Part IV	Strategies and tips for litigating attorneys
Part V	Q&A and Announcements

Today's Agenda

Part I	Introductions
Part II	Updates to legislation, policy, and federal case law
Part III	Recent trends in how technology is being used
Part IV	Strategies and tips for litigating attorneys
Part V	Q&A and Announcements

Legislative Updates

- As of 2024, 49 states + DC, Guam, Puerto Rico, UCMJ criminalize some forms of nonconsensual intimate imagery (NCII)
- Roughly 30 states also prohibit "deepfake" NCII
- VAWA Reauthorization 2022: Federal Civil NCII Statute (15 USC § 6851)

Proposed or Pending Legislation

SHIELD ACT (passed Senate July 2024)

TAKE IT DOWN ACT (passed Senate Dec 2024)

DEFIANCE ACT (passed Senate July 2024)

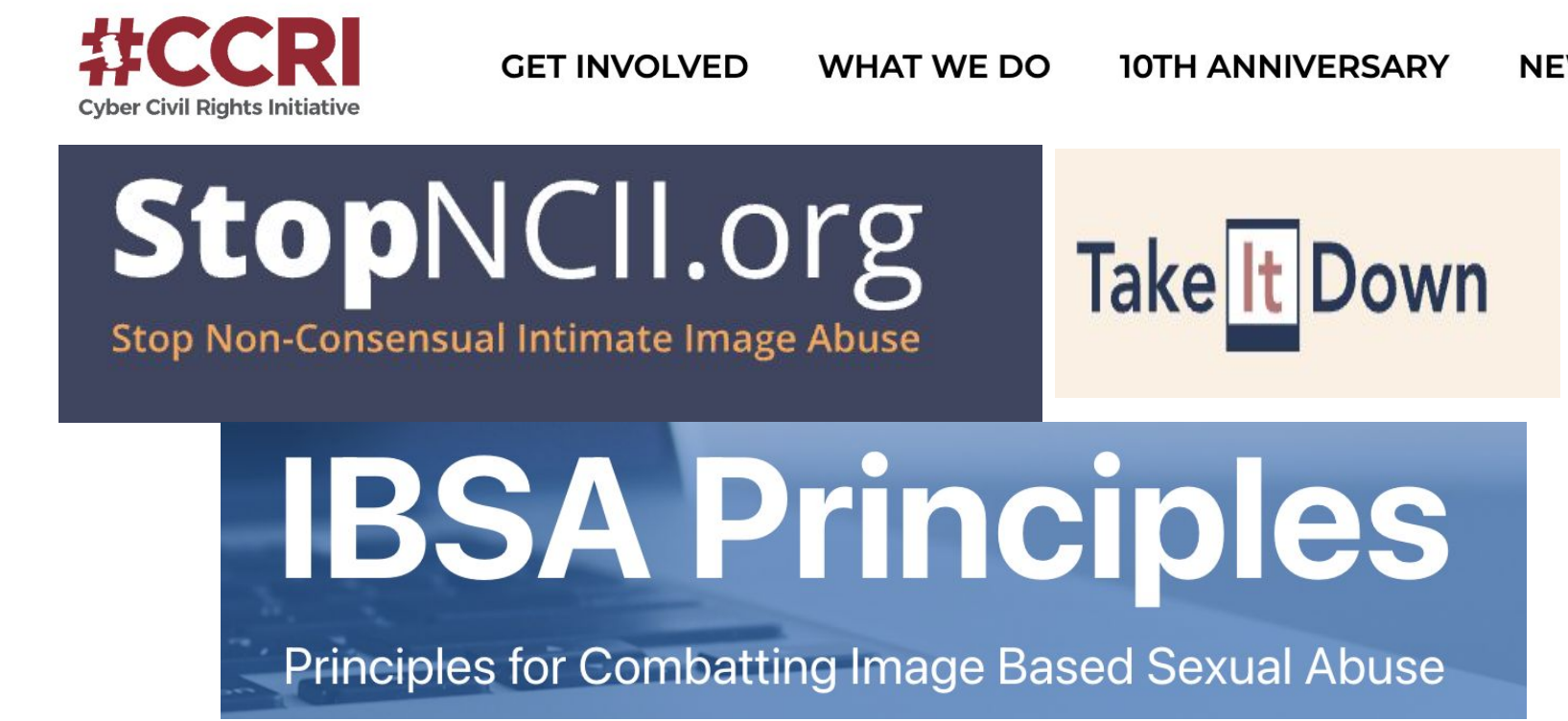
PREVENTING DEEPFAKES OF INTIMATE IMAGES ACT (introduced 2024)

INTIMATE PRIVACY PROTECTION ACT (introduced 2024)

NATIONAL WOMEN'S LAW CENTER

Policy and Resource Updates

If you need help, please visit the CCRI Safety Center or contact the CCRI Image Abuse Helpline at 844-878-CCRI (2274).



SCOTUS Update

Colorado v. Counterman (2023)

Today's Agenda

Part I	Introductions
Part II	Updates to legislation, policy, and federal case law
Part III	Recent trends in how technology is being used
Part IV	Strategies and tips for litigating attorneys
Part V	Q&A and Announcements

Cyber Abuse = TECHNOLOGY-FACILITATED ABUSE

or “tech abuse” or “cyber abuse” for short

(Both terms can be used interchangeably)

What is tech abuse / cyber abuse?

The use of technology to frighten, control, bully, harm, monitor, intimidate or threaten another person.

- **Can be isolated incident or repeated/persistent pattern.**
- **One determined person can cause tremendous harm.**
- **For a victim, it can feel endless and inescapable.**

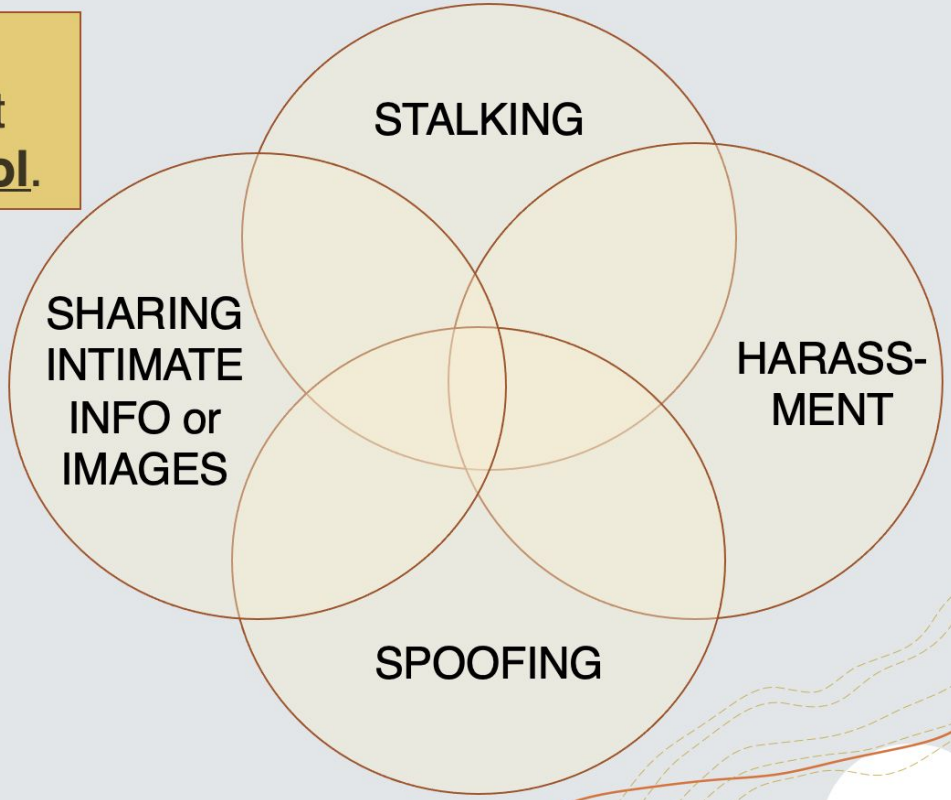
Harm is amplified when abuser has intimate and specific knowledge of the person they are targeting.

Cyber Abuse is Gender-Based Violence

- 90% of victims of forms of cyber abuse are female
- 93% suffered severe emotional distress due to the abuse
- 30% said they have been harassed or stalked outside of the Internet by users that have seen the material online
- 51% contemplated suicide – some completed suicides
- LGBTQIA folks are **4x more likely** to be victims

NATIONAL WOMEN'S LAW CENTER

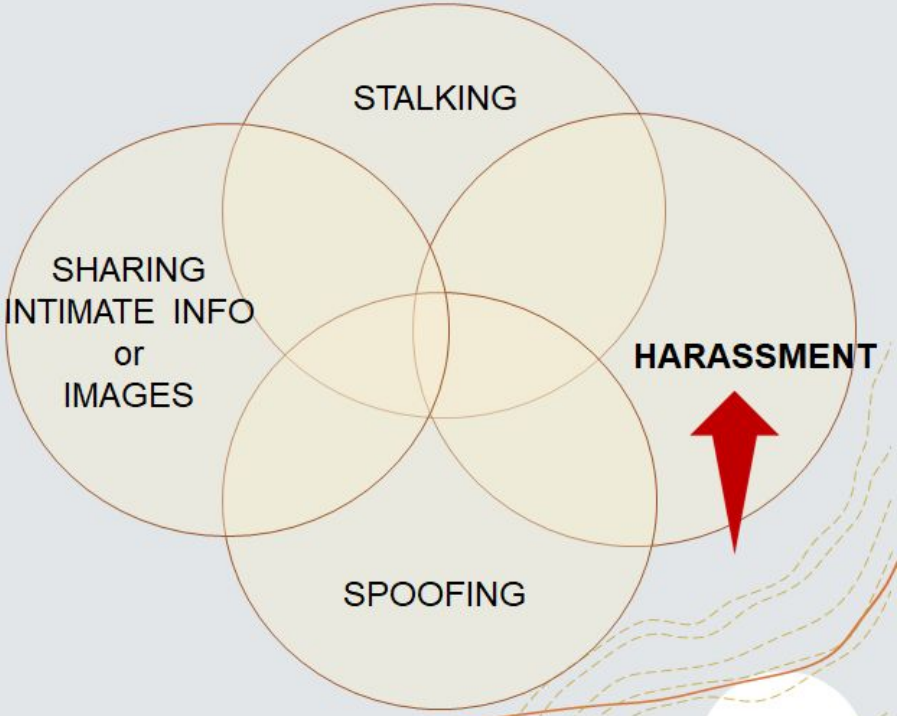
Gender based violence is about **power and control**.



NATIONAL WOMEN'S LAW CENTER

A tech abuser will:

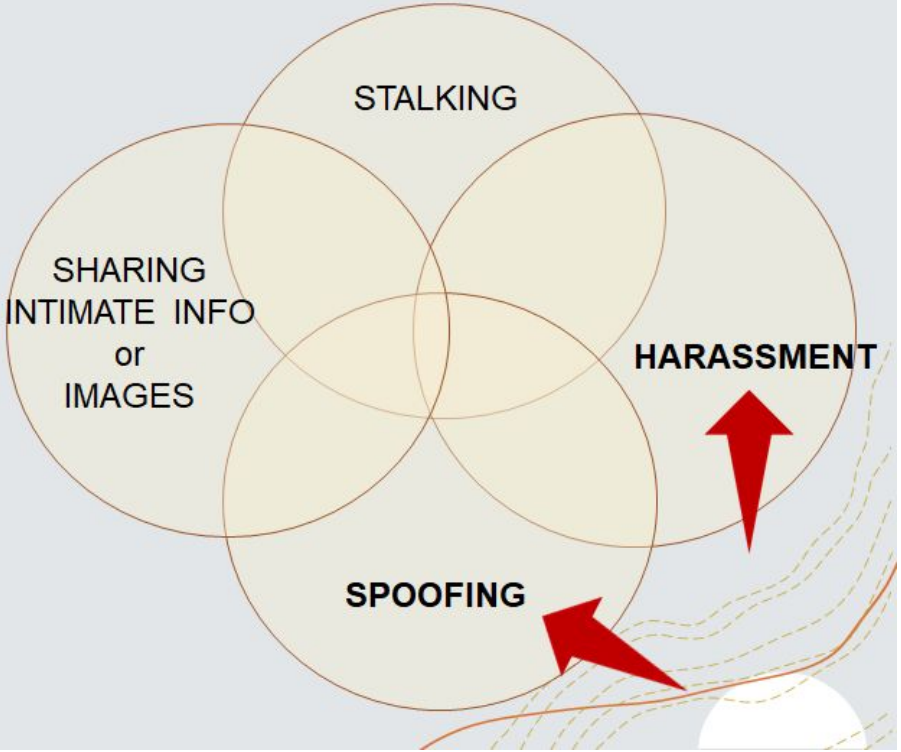
Use technology platforms to contact the **victim's friends, family, or work colleagues** when the abuser can no longer get access to the victim directly.



NATIONAL WOMEN'S LAW CENTER

A tech abuser will:

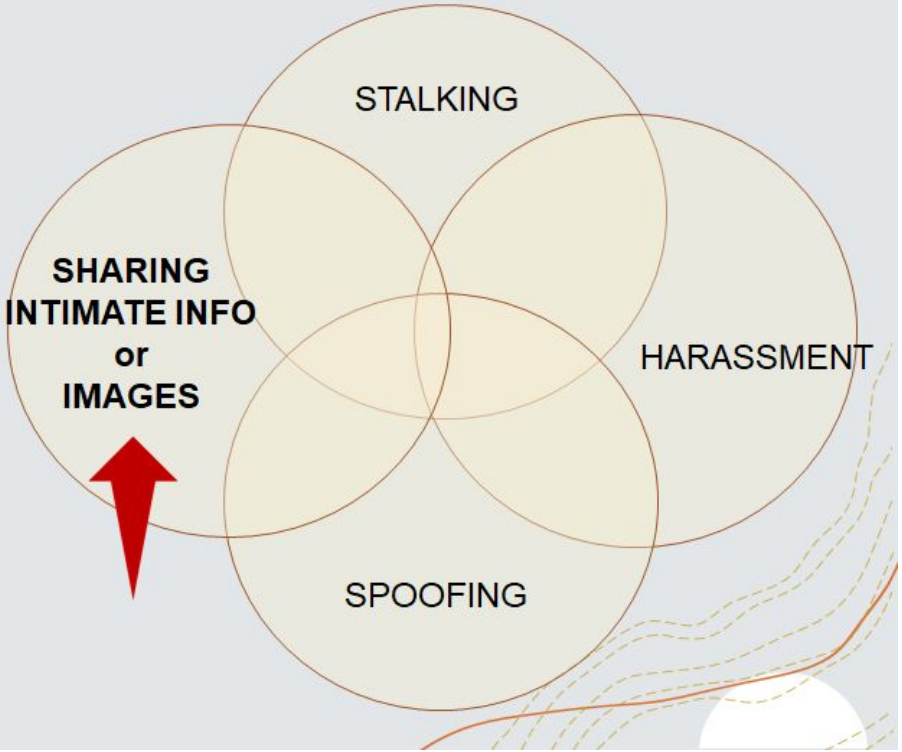
Create "spoofed" or impersonating phone numbers and email addresses to continue to communicate with victim **even after victim has blocked the** abuser.



NATIONAL WOMEN'S LAW CENTER

A tech abuser will:

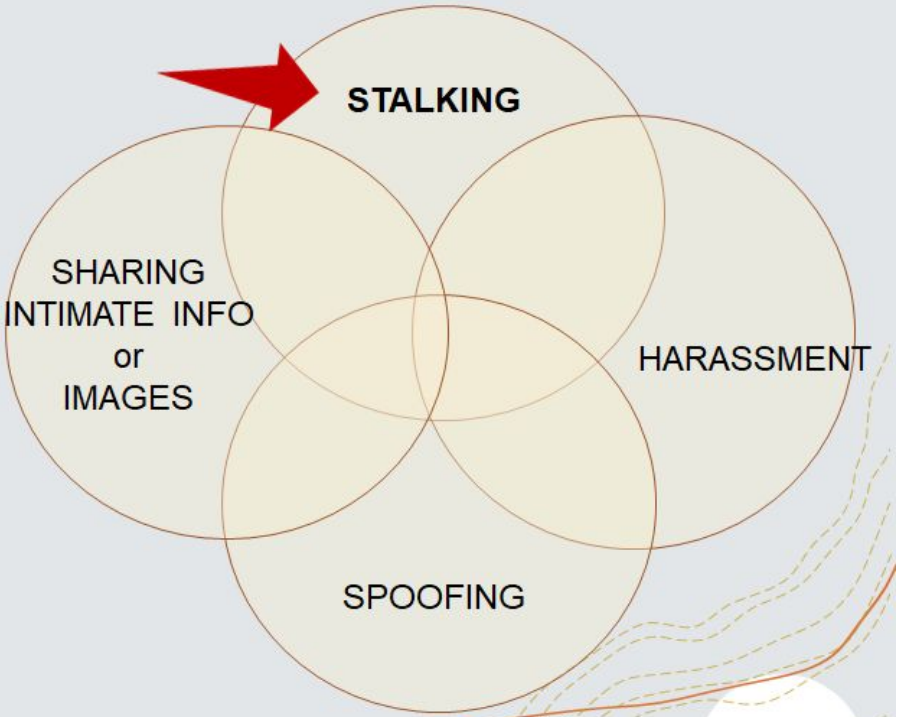
Threaten to **reveal private and/or embarrassing information** about the victim to public forums if the victim doesn't meet the abuser's demands.



NATIONAL WOMEN'S LAW CENTER

A tech abuser will:

Use **spyware** to stalk or spy on the victim or **gain access to victim's accounts** to obtain private information, eavesdrop on conversations, or location.

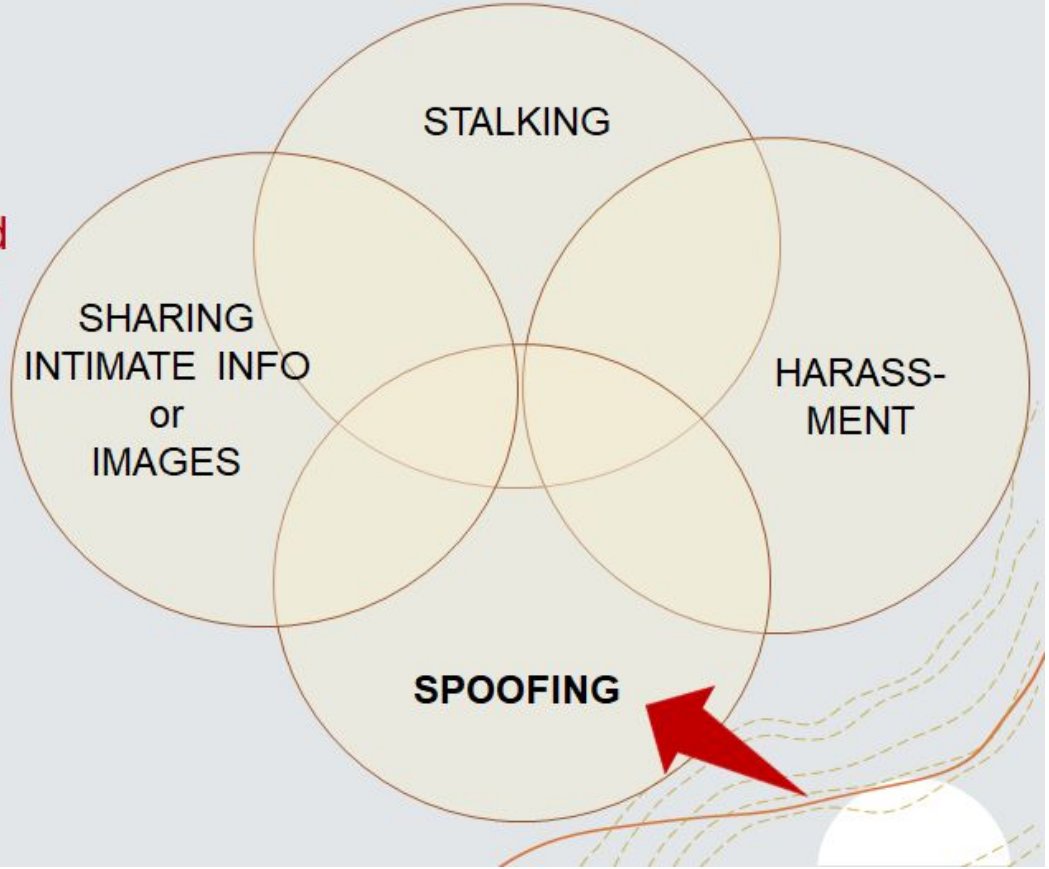


NATIONAL WOMEN'S LAW CENTER

A tech abuser will:

Create **impersonating accounts of victim** and make outrageous posts that cause the victim to look "crazy" or even criminal.

This is done to undermine the victim's credibility or isolate the victim from support communities.



NATIONAL WOMEN'S LAW CENTER

Technology Platforms:

Too many to count.

Main categories:

- Social media accounts
- Messaging apps
- Discussion boards
- Cloud-based storage
- "Spoofing" tools

NATIONAL WOMEN'S LAW CENTER

TECH YOU SHOULD KNOW:

SPYWARE.

- Malicious software that surveils a person through their devices.
- Difficult to detect and remove.
- Spyware is easy to install.

See it to believe it!

https://www.youtube.com/watch?v=FzLcWNiAvgo

NATIONAL WOMEN'S LAW CENTER

TECH YOU SHOULD KNOW:

"CONNECTED" APPS.

- Usually used for conveniently ordering or accessing products.
- Often accounts are shared with multiple members of the same household.

+ Amazon
+ Netflix
+ Seamless
+ GrubHub
+ Uber
+ Lyft
+ Instacart (grocery delivery)

Think about how many "connected" apps we use on a daily basis:

amazon

UBER

lyft

NETFLIX

instacart

seamless
Powered by GRUBHUB

These apps show:

What you are doing.

When you are doing it.

WHERE YOU ARE.

NATIONAL WOMEN'S LAW CENTER

OTHER APPS:

- Dating apps (Tinder, Hinge, Bumble, etc.)
- Financial & Payment apps (Venmo, CashApp, Zelle, etc.)
- User generated porn sites (Pornhub, Xhamster, etc.)
- Too many others to list here!

NATIONAL WOMEN'S LAW CENTER

Internet of Things

- Internet connected devices including but not limited to:
  - **Smart home devices:** Smart lights, smart thermostats, smart doorbells, smart speakers
  - **Wearables:** Fitness trackers, smartwatches, health monitoring devices
  - **Automotive:** Connected cars with features like GPS tracking, remote diagnostics
  - **Healthcare devices:** Remote patient monitoring devices like blood pressure monitors, insulin pumps

Today's Agenda

Part I	Introductions
Part II	Updates to legislation, policy, and federal case law
Part III	Recent trends in how technology is being used
Part IV	Strategies and tips for litigating attorneys
Part V	Q&A and Announcements

Collecting evidence – but of what?

NATIONAL WOMEN'S LAW CENTER

Criminal Law Example– NY Penal Law § 245.15

Unlawful Dissemination or Publication of an Intimate Image

- Class A misdemeanor
- Makes it a crime to share someone else's naked or sexual images without consent
- Elements
  - Intent to cause harm to the emotional, financial, or physical welfare of another person
  - Video or still image depicts (i) unclothed or exposed intimate part of victim or (ii) victim engaging in sexual conduct
  - **NOW INCLUDES** images created by digitization ("deep fakes")
  - Victim must be identifiable
  - Disseminated/published without victim's consent
  - Victim had a reasonable expectation that the image would remain private
  - Perpetrator knew or reasonably should have known the person depicted intended for the image to remain private

Criminal Laws– Check Your Jurisdiction!

49 States + DC + Two Territories Now have Laws Against Nonconsensual Distribution of Intimate Images

The Cyber Civil Rights Initiative has a very helpful tool with information on state by state laws on image-based abuse.

https://cybercivilrights.org/nonconsensual-distribution-of-intimate-images/

Check your state or jurisdiction!

Civil Law Example– NY Civil Rights Law 52-b

Unlawful Dissemination or Publication of an Intimate Image

- Private right of action for Unlawful Dissemination (NY Civil Rights Law Section 52-b)
  - Mostly same elements as criminal penalty except that the private right of action includes dissemination/publication AND threats to publish
  - Injunctive relief, punitive damages, compensatory damages and reasonable court costs and attorney's fees.
- Amends the Civil Rights Law to allow victims to bring an action or special proceeding to obtain an order requiring a website to permanently remove an image/video (NY Civil Rights Law Section 52-b)
  - Image/video must be reasonably within website's control
  - Only allows for injunctive relief. Cannot bring an action for damages.

NATIONAL WOMEN'S LAW CENTER

Civil Laws– Check Your Jurisdiction!

- The global collective of nonprofit organizations, lawyers and advocates, End Cyber Abuse, has information on civil remedies for image-based abuse and examples from different jurisdiction.
  - https://endcyberabuse.org/core-elements/
- Check your state or jurisdiction!

Potential Other Criminal Offenses Available to Tech Abuse Victims

- Offenses again the right to privacy
  - Unlawful surveillance
  - Dissemination of an unlawful surveillance image
  - Tampering with private communications
- Harassment
- Coercion
- Stalking
- Witness tampering

NATIONAL WOMEN'S LAW CENTER

Best Practice for Litigating **Tech Abuse** Cases in Criminal and Family Courts

NATIONAL WOMEN'S LAW CENTER

BIG PICTURE CONCEPTS

Don't get discouraged by the technical details.

Start with the big picture, select key events to highlight, and remember that **good advocacy is about good story telling.**

Use testimony and evidence that tells the Family Court judge a story that:

- makes sense,
- shows the abusive power and control dynamic, and
- illuminates what might be unseen harms of tech abuse.

NATIONAL WOMEN'S LAW CENTER

BEST PRACTICES: **EVIDENCE**

Step 1: **Find it**

Step 2: Preserve it

Step 3: Admit it

NATIONAL WOMEN'S LAW CENTER

SOURCES OF TECH ABUSE EVIDENCE

- Client's Devices (phone, laptop, tablet, etc.)
  - Text Messages, voicemails, missed call logs, other apps
  - Photographs and videos
  - Recorded phone calls
- Client's accounts and social media
  - WhatsApp, Facebook, Instagram, other social media
  - Third –party websites where abuse occurred (client business websites, bank or financial institutions, and more)
  - Client's Email or messaging accounts
- Forensic evidence of spyware/stalkerware

INTERVIEWING THE SURVIVOR

- Be sensitive in your questioning - no victim blaming!
- Engage in anti-racist, trauma-informed, and culturally competent interviewing and advocacy.
- Be mindful of low-income and/or undocumented clients' needs.

.

NATIONAL WOMEN'S LAW CENTER

INTERVIEWING THE SURVIVOR

- **Survivor is usually the main source of evidence!**
  - Spend time (hours), ask specific questions, and make a thorough timeline.
  - Advise client and family/friends not to destroy evidence (spoliation)
- In some cases, it makes sense to not block the abuser. Allow victim to decide, talk it through from a safety perspective.
  - **Attorney may need to gather evidence directly**

NATIONAL WOMEN'S LAW CENTER

GATHERING EVIDENCE FROM CLIENT

- Set up meeting to gather all client's evidence
  - Capture whatever you can immediately!
  - Have client bring old phones, photos, recordings and store/sort them in chronological order
  - Review client's entire communication history with abuser (texts, direct messages on social media/apps, emails exchanged)

GATHERING EVIDENCE FROM CLIENT

- Speak with client's trusted friends and family (with permission)
- Conduct your own searches ("OSINT"):
  - Google the abuser, review any available social media sites
  - Discussion boards or "revenge porn" exchange boards
  - Public records search (i.e. PeopleMap in WestLaw)
  - **We'll talk a little later about ETHICAL implications of this…**

NATIONAL WOMEN'S LAW CENTER

BEST PRACTICES: **EVIDENCE**

Step 1: Find it

Step 2: Preserve it

Step 3: Admit it

NATIONAL WOMEN'S LAW CENTER

WHAT TO CAPTURE

Screenshots/Videos Should Include:

- Website URL
- Actual date and time of capture
- Name or phone number of sender or profile
- Perpetrator idiosyncrasies
- Also… captured evidence should not appear incomplete.

Voicemail Recordings Should Include:

- Date, time and sender information

Note: Remember What **Not** to Include.

NATIONAL WOMEN'S LAW CENTER

OPTIONS FOR HOW TO CAPTURE

- Screenshots of phone or computer
- Download voicemails, videos (may still need screenshot)
- Use another device to take a photo or video
- Install a screen recording software to capture computer activity
- Images printed, videos + audio saved to CDs or USB drives
- Forensic investigation
- Subpoena (more on this in a moment…)
- SMS Backup and Restore or export to PDF

NATIONAL WOMEN'S LAW CENTER

ADDITIONAL TIPS

- Consider removing abuser from "contacts" before preserving
- Have someone do the gathering who is not covered by the attorney-client privilege
- Sometimes possible to recover deleted texts, web content, or deactivated profiles – must act quickly
- Be careful not to connect client's device to your computer, especially with a hacking/spyware case

NATIONAL WOMEN'S LAW CENTER

Want to subpoena a tech platform?

1. **Send a preservation (litigation hold) letter**
2. **Send subpoena that conforms with New York rules and follow steps outlined in UIDDA**

The dirty truth about subpoenas to tech platforms is:
They are cumbersome, time-consuming, expensive (especially if tech platform is out-of-state), and more times than not… they are ***ignored***.

Be ***creative and strategic*** in using rules to your advantage.

BEST PRACTICES: **EVIDENCE**

Step 1: Find it

Step 2: Preserve it

Step 3: Admit it

GETTING EVIDENCE ADMITTED

Submit Evidence in the Right Format*

- Screenshots should be printed
  - Read and understand every correspondence – beware of submitting segments that could be misleading or harmful
- Voicemails and videos –bring laptop/way to show at trial
- Texts should be printed as screenshots
- No need to admit survivor's computer or cell phone, despite best evidence rule (discussed later)

Consider filing a notice to admit (CPLR 3123)

*This will be different if proceeding is virtual as opposed to in-person

AUTHENTICATION: METHODS

Evidence can be authenticated by:

Testimony of a witness with personal knowledge of its identity and authorship

Circumstantial evidence

Stipulation

Chain of custody

Expert testimony

Once evidence is authenticated, burden shifts, and challenges to its authenticity go to weight, not admissibility

AUTHENTICATION: WEBSITES

- **→Witness can authenticate←**
  - By testimony: competent witness can testify!
    - logged onto the site and viewed what was there
    - the exhibit (printout) fairly and accurately reflects what the witness saw.
- Webmaster can authenticate, but this is very uncommon

NATIONAL WOMEN'S LAW CENTER

AUTHENTICATION: TEXT MESSAGES

- "Fair and accurate representation" of messages received on ___ date
- Establish how client knew the abuser was texting
  - Is it a phone number commonly used by abuser? How many times had client communicated with them?
- If the number is unfamiliar to client – use other circumstantial evidence!
  - Use of nicknames or other insider knowledge
  - Testimony that recipient regularly communicated via text
  - Sequential consistency with prior/later text messages sent by that author
- If possible, establish that the message came from a device under the person's control

AUTHENTICATION: EMAILS

- Testimony of conversation participant that the emails are personal correspondence of the witness – fair and accurate representation of the e-mails they received on __ date
  - Usually sufficient in a family court proceeding.
  - Authenticate as if you would authenticate a text message or social media exchange.
- If issues with authenticating in above manner –
  - Can attempt to trace IP address in native .eml file
  - Pursue use of expert witnesses to explain if e-mail has been spoofed or misused

NATIONAL WOMEN'S LAW CENTER

1. Prepare ahead of time.

+Find out how your judge handles the presentation of tech/digital evidence.

+Some JXs treat tech evidence with more scrutiny.

2. Choose your battles.

+ Don’t get weighed down in confusing technicalities.

+ You don’t have to present everything. In fact, doing so can hinder your case.

3. Preserve Objections.

Questions?

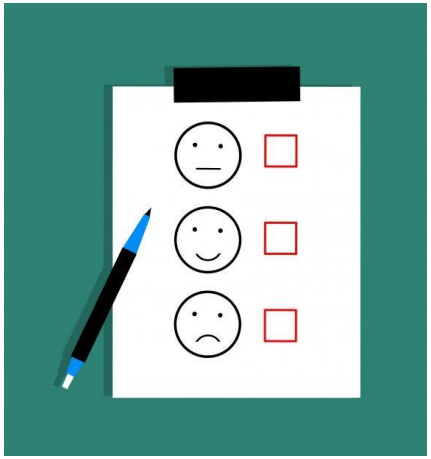
Dr. Mary Anne Franks (she/her)
Eugene L. and Barbara A. Bernard Professor in Intellectual Property, Technology, and Civil Rights Law, George Washington Law School and *President and Legislative & Tech Policy Director*, Cyber Civil Rights Initiative

Annie Seifullah (she/her)
Founding Partner, Incendii Law PLLC and *Co-chair*, New York Cyber Abuse Task Force

Lindsey M. Song (she/her)
Associate Program Director of the Family Law Project, Queens Family Justice Center, Sanctuary for Families and *Co-chair*, New York Cyber Abuse Task Force

NATIONAL WOMEN'S LAW CENTER

Take our survey!



Join the Legal Network for Gender Equity!

nwlc.org/legalnetwork

Follow us on social media!

@nwlc

facebook.com/nwlc

@nationalwomenslawcenter