

# Digital Boundaries: Addressing the Growing Crisis of Cyber Sexual Assault

Lana Ramjit  
Clinic to End Tech Abuse  
Cornell Tech

# About the facilitator



**Lana**

lana.ramjit@gmail.com

- (ex-) Director of Clinic to End Tech Abuse and researcher at Cornell Tech from 2022-2024
- PhD (2021, UCLA) and B.A. (2015, Columbia) in Computer Science
- Survivor Advocacy
  - Columbia Rape Crisis Center, RAINN, etc

60+% of survivors report being subjected to technology abuse.

-Journal of Family Violence 2020



harassment



stalking



financial harm



surveillance

# Most common forms of tech abuse

## Harassment

creating new accounts or phone numbers to harass the survivor or their social circle

## Cyberstalking

non-consensual location sharing, spying on emails, spyware, hidden cameras

## Image-based abuse

(threatening to) share intimate or sexual images without consent, including fake images

# Abusers can cause harm if:

## they OWN something

- Abuser owns device/account
- Shared account/device
- Buying or gifting devices to survivor or children

## they can ACCESS something

- can unlock device and read information
- Remotely "hack" via security questions / passwords
- Install spyware / "dual-use" app

## they can CONTACT the survivor:

- Call/text/message victim or friend's/family
- Post harmful content on social media
- Proxy harassment
- "spoofing"

## they can PUBLICLY SHARE information

- Blackmail by threat of exposure
- "Doxxing" victim
- Non-consensual intimate images
- Fake profiles/advertisements of sexual services

# Simple Methods, Big Harm

- abusers often overstate their abilities with technology as a form of manipulation
- most technology abuse makes use of simple tools, like third-party apps or social media
- these simple methods *can* be very powerful, especially when they circumvent normal protections
- but simple methods can also stop abuse

# Who can help with tech abuse?

Everyone has a role to play, whether you consider yourself a tech expert or not!

- ❖ technologists
- ❖ caseworkers
- ❖ lawyers
- ❖ family attorneys
- ❖ law enforcement

# NYCs Clinic to End Tech Abuse



**CORNELL  
TECH**



Technologists at CETA provide services to hundreds of survivors in NYC since 2018, in a partnership between Cornell Tech, the Mayor's Office, the Anti-Violence Project, and Sanctuary for Families.



# When to refer to CETA

- The harming party is known to the survivor and a former intimate partner or family member.
- The survivor is concerned about *their own device* being unsafe or someone tracking their location.
- The survivor is willing to talk on the phone with a *volunteer* assistant.

# How to refer to CETA

Referrals can only be made through partners at the Family Justice Center (one located in each borough), the Anti-Violence Project for LGBTQ+ survivors, or survivors who are in Sanctuary for Families' residential programs.

Referrals are at the partner's discretion.



# Who can help with tech abuse?

Everyone has a role to play, whether you consider yourself a tech expert or not!

~~❖ technologists~~

can refer to



- ❖ caseworkers
- ❖ lawyers
- ❖ family attorneys
- ❖ law enforcement

## Rest of This Session

Big steps that non-technologists advocates can take *without* and before referring to CETA!

- Immediate mitigation strategies
- Relevant laws and statutes for NYC
- Help survivors gather evidence and make reports

**Mitigation**

Harming parties can use technology to evade orders of protection, in which case we need advocates, family law attorneys, and law enforcement to work together.

Not one simple solution, but there ARE options.

# Harassment and stalking

Survivors often benefit from knowing if a harming party is *attempting* to contact them.

This can help:

- identify if the harming party is escalating
- prove attempted violations of a restraining order
- give insight into their plans

# Screening, not blocking

Blocking may just force a PCH to other platforms.

Consider deleting the saved contact card and turning on "screen unknown callers".



better screening apps! built-in app is called CallScreen. another option is TrueCaller






not as good screening. delete the contact card and use unknown caller filtering





## Security Check

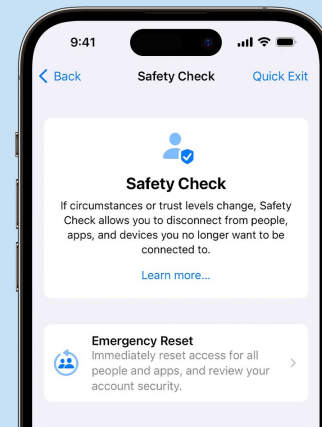
You have security tips

	<b>Your devices</b> Remove your account from Mac OS	▼
	<b>Recent security activity</b> No activity in the last 28 days	▼
	<b>Sign-in &amp; recovery</b> 2-Step Verification is on	▼

Android and Gmail users should use Google's **Security Checkup**



## How to Use Safety Check on your iPhone



**Apple** users should update their phones and use Apple's **Safety Check**

# Social Media

Most social media platforms have robust settings and options to review privacy and account safety.

For major platforms (WhatsApp, Instagram, Facebook, Tiktok), CETA has a spreadsheet linking to important privacy settings for social media--review these with survivors.

# Databrokers and online profile

 DeleteMe®

 **kanary**



Search for your client's name on Google--phone number, address, workplace--what's out there?

Services can take these down.

# Non-consensual intimate images (NCII)

A broad term for sharing private photos of someone without their consent:

- by posting them publicly or privately
- sending them to the survivor's community
- or threatening someone with such images

aka: image-based sexual abuse, "revenge porn"



**StopNCII.org**

Stop Non-Consensual Intimate Image Abuse

If the survivor has the photo in question and the photo meets certain criteria, then [www.stopncii.org](http://www.stopncii.org) can preemptively prevent the photo from being posted on several major platforms or have it taken down.



## **Cyber Civil Rights Initiative Safety Center**

A central resource for steps to take if you or a client are targeted by image-based abuse, including a roster of local attorneys and local laws.

# Local laws and Statutes

*tech-specific provisions in NYC*

# Non-consensual intimate images

Under New York Penal Law 245.15, a misdemeanor if:

- Image is sexual in nature or shows certain body parts
- Intent is to cause physical, emotional, or financial harm
- Sharing happens without consent
- Image was shared with reasonable expectation of privacy

Survivor also retain right to pursue redress in civil court.

Consult an experienced attorney, not NYPD!



**Stalking is the highest predictor of homicide in IPV and includes:**

- Online contact, including anonymous online
- *Encouraging* others to contact the survivor online
- Jackie's Law: non-consensual use of a GPS or electronic tracking device

# Stalking and harassment

cyberstalking is punishable under the same statutes of non-cyber stalking *in addition* to a charge of aggravated harassment.

third and fourth degree stalking are misdemeanors, but *repeated acts of stalking* after prior convictions are felonies -- even if it's 'only' cyberstalking.

# Investigation and Orders of Protection

- Anonymous online contact is a violation of an OP!
  - automatically criminal
- a Domestic Incidence Report (DIR) is a mandated report that allows NYPD or the DA to investigate a potential violation even if harassment is anonymous.
- ✓ Check the box! NY orders of protection include an option where accessing the survivor's online accounts is covered in an order of protection.

## More resources



Technical assistance, training, and resources on stalking and harassment laws



Network/ mailing list of attorneys and advocates to consult on local cyberabuse issues

**Evidence**

# collecting evidence of cyberharassment

whether a survivor is ready to file a report or not, collecting evidence keeps that option open by establishing:


- *course of conduct* crimes like stalking and harassment
- the *intention* to cause emotional, financial harm
- nature of relationship ('reasonable expectation of privacy')
- which platforms might have *additional* evidence

# tips for documenting harassment


1. capture the whole screen, and don't crop, edit, or otherwise alter screenshots or images.
2. try to include a timestamp for messages
3. if a phone number is involved, delete the contact card to show the phone number, not a nickname
4. look up the phone carrier and any other related information you can get for free
5. keep a well-organized and annotated log of screenshots

# example of an incident log

Date and Time	Incident	Phone number/ username	Description	Platform	Screenshot?	Subscriber information
11/4/2024 1:38PM	Private message	555-123-4567	Private photos only shared with person causing harm sent to client's sister	Text message	Yes	TextNow
11/5/2024 9:10AM	Online post	@coolguy34	Threat of physical harm aimed at client	Facebook	Yes	coolguy100@yahoo.com



Any important context that helps identify the person.  
BRIEF summary



can use free tools to find this in just a few minutes!



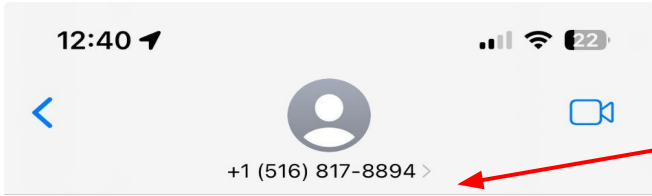
# documenting anonymous calls



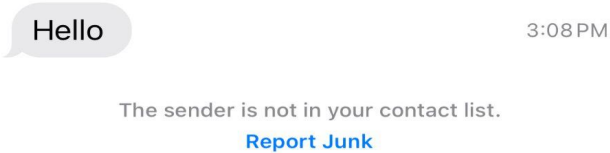
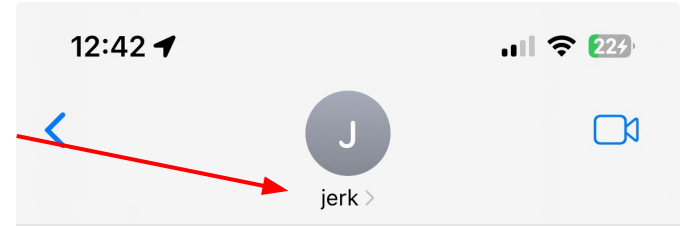
**TrapCall** - a subscription app that reveals the caller ID for callers using restricted, blocked, or \*67 to hide their number

**NumLookup** - a free service at [www.numlookup.com](http://www.numlookup.com) that will pull callerID as well as subscriber platform (e.g. AT&T, TextNow, Google Voice)





caller name



pull to side to  
get  
timestamp



cropped!



# Basic Subscriber Information (BSI)

**BSI is information that someone enters to sign up for an online service, like their name, phone number, and email address.**

If we know the platform, NYPD and civil subpoenas can unmask the harasser by obtaining BSI.

That's why you need to look up the phone number!

# VoIP services



**these services can give  
harming individuals cheap  
"anonymous" numbers...**



**but they are not really  
anonymous! document, look  
up the platform, get the BSI!**

# evidence collection for social media



**Spokeo** - can look up associated email addresses and phone numbers for a social media account

**NYPD** or a **civil attorney** can file subpoenas to social media platforms for BSI to obtain the subscriber information for harassment.

# Takeaway

- slow, frustrating, but there ARE tools available to us!
- harming individuals use these methods because they get away with it.
- we can all help the process with good records and simple, free tools.