Understanding and Addressing the Impact of Stalking on Young People

Presented by:
Lorien Castelle, Director of Prevention
Nasim Sarbandi, Project Coordinator
Statewide Membership Organization

- **Members:**
  Domestic violence service providers, allied agencies and community members

- **Mission:**
  Create and support the social change necessary to prevent and confront all forms of intimate partner violence

- **Work:**
  Training, technical assistance, public policy, systems advocacy, best practices, broad-based collaboration

- **Philosophy:**
  Anti-oppression, trauma informed, and survivor centered principles integrated into all of our work
• Identify the most common ways technology and online spaces are misused in the context of intimate partner stalking among student populations
• Identify strategies survivors can use to increase privacy and securely access technology and online spaces
• Stalking laws and remedies
• Learn strategies for helping survivors safety plan
DEFINITION OF STALKING

- A pattern of behavior directed at a specific person that would cause a reasonable person to feel fear.*
- A Pattern of Behavior… Not a single incident or “one off” event. Called a “course of conduct” in most stalking statutes
- Context is Critical in Stalking Cases

* Slide’s information from SPARC
STALKING FACTS


• Women are more likely than men to experience stalking. (The National Intimate Partner and Sexual Violence Survey (NISVS): 2010 Summary Report, Center for Disease Control (2011))

• 18-24 year olds experience the highest rates of stalking. (The National Intimate Partner and Sexual Violence Survey (NISVS): 2010 Summary Report, Center for Disease Control (2011))

• Most stalkers are male. (The National Intimate Partner and Sexual Violence Survey (NISVS): 2010 Summary Report, Center for Disease Control (2011))

• The majority of the time, the victim knows the perpetrator. (The National Intimate Partner and Sexual Violence Survey (NISVS): 2010 Summary Report, Center for Disease Control (2011))
Does leaving = Safety?
State Report, Centers for Disease Control and Prevention (2017)
IDENTIFYING A PATTERN OF BEHAVIOR

Identifying a Pattern of Behavior

<table>
<thead>
<tr>
<th>S</th>
<th>Surveillance</th>
</tr>
</thead>
<tbody>
<tr>
<td>L</td>
<td>Life Invasion</td>
</tr>
<tr>
<td>I</td>
<td>Interference</td>
</tr>
<tr>
<td>L</td>
<td>Intimidation</td>
</tr>
</tbody>
</table>


* Slide from SPARC*
IDENTIFYING A PATTERN OF BEHAVIOR

SLII Examples: Peggy Klinke Story

**Surveillance**
- Watched Patrick’s house
- Showed up at Peggy’s gym and house
- Followed Peggy
- Kept track of her schedule (like when she was gone for the wedding)

**Life Invasion**
- Phone calls
- Public humiliation – posted flyers of Peggy in her neighborhood
- Harassed/threatened friends and family

* Slide from SPARC
IDENTIFYING A PATTERN OF BEHAVIOR

SLII Examples: Peggy Klinke Story

**Interference**
- Ruined reputation (through flyers, spray paint, etc.)
- Stalked Peggy’s new boyfriend, Mark
- Physically attacked her and murdered her

**Intimidation**
- Property damage to Peggy’s home
- Committed arson on Mark’s home
- Threatened Peggy
- Threatened Peggy’s family

* Slide from SPARC
Section 2: Technology Abuse, Safety Planning, Evidence Gathering, And Using Technology To Increase Safety

• Tools Abusers Use To Stalk And Harass
• Safety Planning With Survivors
• Gathering Evidence Of Technology Abuse
TECHNOLOGY ABUSE

Simple

• Monitoring or changing functions or features
• Manipulating features
• Eavesdropping on calls
• Spying on activity
• Track location via phone app such as family location feature or find my phone

Complex
TECHNOLOGY ABUSE

Email & Messaging

• Abusers can gain access to email accounts, phones, etc.
  – Delete messages
  – Send fraudulent messages to coworkers, family and friends
  – Intercept and monitor messages
### Activity on this account

This feature provides information about the last activity on this mail account and any concurrent activity. Learn more.

This account does not seem to be open in any other location. However, there may be sessions that have not been signed out.

Sign out all other web sessions

<table>
<thead>
<tr>
<th>Access Type (Browser, mobile, POP3, etc.)</th>
<th>Location (IP address)</th>
<th>Date/Time (Displayed in your time zone)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser (Chrome) Show details</td>
<td>* United States (NY) 69.193.14.114</td>
<td>9:59 am (0 minutes ago)</td>
</tr>
<tr>
<td>IMAP () [ ] Hide details</td>
<td>United States (MA) (2607-fb90-5565b-7ef0:4df6:fb55:663e:1459) 12:04 am (9 hours ago)</td>
<td></td>
</tr>
<tr>
<td>IMAP () Show details</td>
<td>United States (MA) (2607-fb90-5565b-7ef0:4df6:fb55:663e:1459) Mar 25 (19 hours ago)</td>
<td></td>
</tr>
<tr>
<td>IMAP () Show details</td>
<td>United States (MA) (2607-fb90-5565b-7ef0:4df6:fb55:663e:1459) Mar 25 (1 day ago)</td>
<td></td>
</tr>
<tr>
<td>IMAP () Show details</td>
<td>United States (MA) (2607-fb90-5565b-7ef0:4df6:fb55:663e:1459) Mar 24 (2 days ago)</td>
<td></td>
</tr>
<tr>
<td>IMAP () Show details</td>
<td>United States (MA) (2607-fb90-5565b-7ef0:4df6:fb55:663e:1459) Mar 24 (2 days ago)</td>
<td></td>
</tr>
<tr>
<td>IMAP () Show details</td>
<td>United States (MA) (2607-fb90-5565b-7ef0:4df6:fb55:663e:1459) Mar 24 (2 days ago)</td>
<td></td>
</tr>
</tbody>
</table>

Alert preference: Show an alert for unusual activity, change.

* indicates activity from the current session.

This computer is using IP address 69.193.14.114 (United States (NY))
TECHNOLOGY ABUSE

Text Messaging & Instant Messaging

• Messages can be falsified, spoofed, or sent anonymously from the carrier’s website or other third party services

• Apps and services can make evidence collection more difficult, e.g. Tiger Text, Snap Chat, etc.
Active sessions on Facebook
**Active Sessions on Messaging Apps**

### CURRENT SESSION

<table>
<thead>
<tr>
<th>App</th>
<th>Version</th>
<th>Status</th>
<th>Device</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telegram</td>
<td>iOS 4.8.1</td>
<td>online</td>
<td>iPhone 6, iOS 10.2.1</td>
<td>172.58.217.240</td>
</tr>
</tbody>
</table>

### Terminate all other sessions

Logs out all devices except for this one.

### ACTIVE SESSIONS

<table>
<thead>
<tr>
<th>App</th>
<th>Version</th>
<th>Date</th>
<th>Device</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telegram</td>
<td>Desktop</td>
<td>1.2.6</td>
<td>PC, Windows</td>
<td>24.29.49.197</td>
</tr>
<tr>
<td>Telegram</td>
<td>Desktop</td>
<td>9049</td>
<td>Mac, OS X</td>
<td>108.183.4.178</td>
</tr>
</tbody>
</table>
TECHNOLOGY ABUSE

Messaging, Phones & Evidence Collection

• With a valid search warrant, a carrier *might* be able to retrieve deleted messages or document that messages were sent from one party to another.

• Using special software, law enforcement might be able to extract old backup files (e.g. iTunes / iPhone backups).

• SIM cards, internal memory and MicroSD cards may contain evidence.

• Survivors can take screenshots, photographs or video of phone and message content, as well as the properties of a message (time & date stamp, contact info: name *and* number sent from).
Smartphones & Apps

- Many companies now offer connecting your smartphone to your home security system (Ex. – AT&T Digital Life)
TECHNOLOGY ABUSE

Smartphones & Apps

- Receive text and video alerts of events at home
- Arm or disarm the alarm, unlock, lock and open doors
- Monitor indoor activity with contact sensors and cameras
- Family Map / Family Locator Plans
- Teen driving monitors
- Apps can be renamed, or completely invisible
- Photo apps that allow users to hide pictures, sometimes behind other pictures that require a password to be viewed
Caller ID & Email Spoofing

- Caller ID spoofing gives the caller the ability to show a different number on the caller ID display, change their voice, and record calls.

- Email spoofing is the creation of email messages with a fake email address, misleading the recipient about the origin of the message.

- Can you identify situations that these tools might be helpful for survivors?
Spoofing, Safety Planning & Evidence

• If survivor suspects a call has been spoofed, they can call the number that came in to check if a call was actually placed.

• Spoofed numbers do show up on the survivors bill, but the owner of that number will not show a call on their bill.

• You can often identify the source of an email spoof by the IP address in the received line.
Truth In Caller ID Act of 2009

• Signed into law December 2010 and enacted in June 2011, this law prohibits caller ID spoofing for purpose of defrauding or otherwise causing harm.

• The FCC now:
  – Prohibits any person or entity from transmitting misleading or inaccurate caller ID information with the intent to defraud, cause harm, or wrongfully obtain anything of value.
  – Subjects violators to a penalty of up to $10,000 for each violation.
  – Exempts authorized activities by law enforcement agencies and situations where courts have authorized caller ID manipulation to occur.
Phishing

- Phishing is a method of trying to gather personal information using deceptive e-mails and websites.
- It uses social engineering methods to convince you to click or download something
Cell Phone Spyware

- Hardware example: SIM Card Spy – Transfer files on a cell phone SIM card to a computer for viewing, saving and editing

- Software can be difficult to install without physical access, but also can be very difficult to detect
Detecting Cell Phone Spyware

- Unusual battery drain, or battery is warm when not in use
- Unexplainable spikes in data usage
- May take longer to shut down
- Screen may light up when not using
- May hear clicks or sounds when on calls
- Additional incoming calls on the bill that user didn’t receive
- Perpetrator knows things that could only be known with access to the phone
- Perpetrator currently has or has had physical access
SAFETY PLANNING

Safety Planning For Phones

- Ensure phone use is a part of every safety plan
- Use passcodes – the more complex, the better
- Use pay-as-you-go phones
- Treat usual phone like a tracking device
- Be wary of “gifts”
- Always give location information to 911 in an emergency in case phone settings have been changed without your knowledge
- Unmask blocked calls ([TrapCall](#))
SAFETY PLANNING

Safety Planning For Phones

• Educate and strategize about safe phone use and increased privacy

• Document calls, text messages, photo & video messages (date, time, content, number / IP address)
  
  • Record if possible, particularly if it is threatening (apps are available)

  • Print out call logs and billing records that corroborate the documentation
Computer Spyware

- Can be used to record all:
  - Keystrokes
  - Websites visited
  - Emails and IMs
  - Windows and application details
- Can take screen shots
- Restart, shutdown & logoff computer
- Control desktop and mouse remotely
- Make computer talk
Computer Spyware and Safety Planning

• Clearing history is not enough

• Identify safer computers (libraries, friends' houses, internet cafes, etc.) that can be used for sensitive web surfing

• If a survivor’s computer (or phone) is being monitored, it may be important to continue using it, so as not to alert the abuser and risk escalation

• Create separate safe email/IM accounts and don’t use your name
TECHNOLOGY ABUSE

GPS Technology

• Track a person or object using satellite technology in real time

• Vehicle navigation systems

• Small and easily hidden

• Affordable and readily available (ex. Tile)
Safety Planning & GPS Technologies

• Trust instincts

• Do visual sweeps or ask law enforcement, mechanic or private investigator to do a sweep

• If a device is located, strategize about the removal – remember it might be better to leave it where it is
Social Media

• Abusers can use social media to stalk and harass survivors

• Abusers can gain access to a survivor’s profile without consent

• Abusers can create false profiles
Social Media & Privacy

- Virtually every social media app has location based features that you opt into when you first set up the app.
- Posts and media are automatically time stamped and geo-tagged with the general or exact location.
- Privacy settings change regularly and can be very nuanced.
- Abusers can create false profiles on social media sites.
Social Media & Safety Planning

• More than Facebook!
• Keep profile settings as private as possible
• Only login on trusted devices
• **Always logout!!**
• Remember that even when set to private, abusers can still access
• Review: What are you sharing? Who do you want to see it?
• Avoid tying accounts to optional personal information
• Use print screen to track harassment, stalking, etc.
SAFETY PLANNING

Social Media, Online Privacy, & Safety Planning

• Data brokers
• Do a Google search of your name
• Profile pictures
• Post only what you want the public to see or know, even if you have your page set with privacy in mind – once it’s been shared online, it’s out of your control
• Request that people not post personal information about you on social media (including tags and check-ins)
• Blocking and un-friending
• Temporary deactivation of accounts is often available
You can report online abuse!

- Most sites have rules about what is allowed on their site
- Some content can be removed based on the site’s:
  - Terms of Service, Content Policies, Community Guidelines/Standards
- Most sites will remove images or videos content if the person who posted it doesn’t have copyright over the material*

* The language on this slide used from NNEDV
TECHNOLOGY ABUSE

Video & Audio Monitoring

• Hidden cameras cheap and easy to get

• Very small, can be hidden anywhere and difficult to detect

• Phones can be left in places and set to auto answer so that conversations can be monitored
Safety Planning & Recording Devices

- Trust instincts
- Where does the victim feel like they are being watched/overheard?
- Any new gifts or objects in the space they are being monitored?
- Meet in secure locations that aren’t being monitored
- If device is located, assess best next steps — will abuse escalate if device is found? Will it be tampering with evidence?
- Obtain equipment to sweep for wireless signals
TECHNOLOGY ABUSE

Wi-Fi Routers

• Unsecured routers can be used to hijack devices; email accounts can be taken over; can use the connection for malicious/illegal purposes

• Wireless routers can be set to record all sites visited by any device connected to it

• Access to websites can be blocked (firewall)
SAFETY PLANNING

Wi-Fi Routers

• Don’t connect to public WiFi
• Secure your wireless network (change the SSID and password protect)
• Use WPA2-PSK {AES} security
• Change default administrator passwords and usernames
• Turn off when not in use for extended periods of time
• Check for firmware updates
Tech Abuse Safety Planning & Evidence Gathering

• Always do emotional safety planning first

• Pay attention to the subtleties of a survivor’s story

• Ask clarifying questions to identify the what, the how, the when and the where

• Consider not just the survivor’s use of technology, but also those they are close with
SAFETY PLANNING & EVIDENCE GATHERING

Tech Abuse Safety Planning & Evidence Gathering

• Don’t overwhelm survivors
• Encourage them not to delete evidence
• Blocking someone means you won’t know what they are posting
• Educate about the use of the criminal justice system
• Does the abuser’s behavior violate an Order of Protection (OP)? Can it help the survivor get an OP?
• Consider using non-tech specific laws for prosecution
MORE ON EVIDENCE

• Advocates should NOT collect or store evidence

• Social media and email services have access logs that show where your account has been accessed from

• Email headers contain IP address

• “Download Your Information” tool on Facebook

• Be aware that you can access some websites digital trails such as Facebook, Snapchat, Google, etc. but some other digital trails are only available to law enforcement and courts with Warrant/Subpoena

• Warrant for account information from spoof company

• Record conversations (New York is a one party consent state)
EVIDENCE & OPTIONS

- Police engagement
- Police collaboration with prosecution for evidence gathering
- Demonstrate course of conduct
- Email documentation to law enforcement for safe keeping / course of conduct demonstration
- Defamation claims
- Make sure orders of protection include social media and electronic communication
PROSECUTION & SURVIVOR BEHAVIOR

• Survivor behavior can be confusing to some prosecutors.

• Sometimes seemingly benign behavior from an abuser can be terrifying to a victim.

• Bailiffs need to be trained to identify and respond to courtroom intimidation.

• Remember - only unsuccessful intimidation ever comes to the attention of police or prosecutors.

• Asking “what was going through your mind when…” can be a powerful question offering vital information – sometimes factual, sometimes contextual.
STALKING LAW

• All 50 states
• District of Columbia
• US Territories
• Federal
• UCMJ
• Some tribal codes*

* Slide from NNEDV
STALKING LAWS

• New York State Laws and Provisions
• Federal provisions

• PL § 120.45. Stalking in the fourth degree
• PL § 120.50. Stalking in the third degree
• PL § 120.55. Stalking in the second degree
• PL § 120.60. Stalking in the first degree

* Slide from NNEDV
SAFETY PLANNING

Group Exercise
Passwords

- At least eight characters long
- Does not contain a complete word
- Contains characters from each of these categories:
  - UPPERCASE LETTERS; lowercase letters; numbers (123);
    special characters (!@#$%^&*)
- Does not contain your user name, real name, or company name
- Is significantly different from previous passwords and other passwords currently in use
- Two-step verification pass for emails, websites and apps
Computers

• Maintain current antivirus/anti-malware/anti-spyware software and keep it updated
• Update operating system
• Be extremely cautious about connecting to unsecure public Wi-Fi
• Use a virtual private network (VPN) for remote connection to office
• Use complex passwords and change them every few months
• Don’t use the same password across different sites
• Don’t click on any links in emails, even if you know who sent it to you, without first:
  – hovering over the link to see what the actual URL is (example: http://www.google.com/), or
  – typing the text of the link into a browser
Smart Phones

• Bluetooth: only turn on when you need it, then be sure to turn it off
• Using public Wi-Fi puts you at risk of hacking, malware and monitoring
• Cellular data connections are much more secure than Wi-Fi – be sure to use it if doing work on the phone
• Use complex passcodes
Databases

- Many programs are transitioning to new databases
- Cloud vs. local
- Remember that data entered can exist forever
- Data can be used for secondary purposes
- Risk of accidental deletion or alteration
- Privacy & safety
- Informed consent
- Backups – use same security
- SafetyNet & Confidentiality Institute Toolkit:
  http://techsafety.org/selecting-a-database
CONSIDERATIONS IN USING TECHNOLOGY

Social Media

• Social media spaces do not have the privacy or safety mechanisms in place to be used as service provision forums
• Have clear content guidelines (ex. NYSCADV Facebook Page)
• Be thoughtful about what you post
• Best use of social media: education
• Plan how your agency will respond to negative or opposing views
• Plan how your agency will handle survivor posts that reveal personal stories
SURVIVOR-CENTERED TECH SAFETY

Remember

• Safety + Privacy + Technology = Possible!

• Getting rid of technology is not the answer

• Safety planning around technology should be individual and specific
Key Concepts

• Respect and maintain confidentiality
• Offer support, information, safety options and advocacy unique to each survivor
• Identify and reinforce strengths and current methods of survival
• Do not offer personal opinions about what the survivor should do
• Accept and reinforce the survivor’s right to make their own decisions
IN CLOSING

• While it’s easy to get overwhelmed with all of the bad that can be done with technology, work hard to keep in mind how much these same technologies have helped survivors seek and find connection and safety.

• SAFETY PLAN, SAFETY PLAN, SAFETY PLAN!
RESOURCES

• NYSCADV: Nasim Sarabandi—nsarabandi@nyscadv.org 518-482-5465
• NNEDV SafetyNet Project: https://nnedv.org/content/safety-net/
• NNEDV Tech Safety Blog: http://techsafety.org/
• TechSafety APP: https://techsafetyapp.org/
• Stalking and Harassment Assessment and Risk Profile: http://www.cdar.uky.edu/CoerciveControl/sharp.html
• The Stalking Prevention, Awareness, and Resource Center: https://www.stalkingawareness.org