The Use of Technology to Stalk-- April 2025

Slide 1

SPARC
Stalking Prevention, Awareness, and Resource Center
The Use of Technology to Stalk

Slide 2

OVW Funding
This project was supported by Grant No. 15JOVW-24-GK-03011-MUMU awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this program are those of the author(s) and do not necessarily reflect the views of the Department of Justice, Office on Violence Against Women.

Slide 3

www.StalkingAwareness.org
*Practitioner guides
*Training modules
*Victim resources
*Webinars
Instagram, Facebook, and Twitter logos
@FollowUsLegally
Sign Up for our Newsletter!

Slide 4

Technology does not cause stalking. Stalkers cause stalking.
SPARC logo

Slide 5

Technology & In-Person Stalking
The majority of stalking victims experienced both in-person stalking and technology-facilitated stalking.

Messing, J., Bagwell-Gray, M., Brown, M.L., Kappas, A., & Durfee, A. (2020). Intersections of Stalking and Technology-Based Abuse: Emerging Definitions, Conceptualization, and Measurement. Journal of Family Violence 35(1): 693-704.

Slide 6

Stalking is:
Criminal
Traumatic
Dangerous

Slide 7

Stalking: (Title IX Definition)
A pattern of behavior directed at a specific person that would cause a reasonable person to feel FEAR for the person's safety or the safety of others; or suffer substantial emotional distress.

Slide 8

SLII Framework
Surveillance: watching, following, gathering information
Life Invasion: Showing up in the victim's life
Interference: Sabotaging, attacking, or otherwise changing the victim's life
Intimidation: Threatening and/or scaring the victim

Logan, TK. & Walker, R. (2017). Stalking: A Multidimensional Framework for Assessment and Safety Planning, Trauma, Violence and Abuse 18(2), 200-222.

Slide 9

Surveillance
- Smart home devices
- Tracking software
- Tracking devices
- Monitoring online activity
- Accessing online accounts
- Cameras or audio/video recording devices

Interference
- Spreading rumors online
- Doxing
- Swatting
- Posing as victim and creating harm
- Posting private photos, videos, information online, real or fake
- Using technology to encourage others to harm the victim

Life Invasion
- Unwanted contact online or through text messages, phone calls, or other platforms
- Impersonating victim
- Impersonating others to access the victim
- Hacking and/or controlling victim's accounts

Intimidation
- Online threats
- Blackmail

- Sextortion
- Threats to release private info, photos, or videos (real or fake)
- Threats to interfere with property, employment, finances, accounts

Slide 10

Tracking Location

Slide 11

How Do Stalkers Track Location?
Property Tags
Family Trackers
Access to and/or Shared Victim Accounts
Social Media Maps/Check-ins
Installed Stalkerware
Proxy Stalking

Slide 12

(An embedded TikTok video)

Slide 13

Understanding AirTags
- Shows current location, not location history
- Frequency of the location update varies
    - Depends on other devices in range
- While Tile requires people to have downloaded the Tile app for the location tracking to “ping,” AirTag “pings” off any Apple device within 800 feet

Slide 14

Notification Limitations
- Alerts are inconsistent and designed to catch when device is traveling with the victim
- Most users are notified when they return home, not while traveling
- If the offender is present and/or in close proximity to victim regularly, notification is unlikely

Slide 15

(this slide shows two screenshots of settings in a cellphone in the Safety & emergency section and the unknown tracker alerts section. There is a slide you can enable to “allow alerts”)

Slide 16
Apple: Search for “Find my” App

Slide 17
If you have items associated with your account
(screenshot of items in “Find my” App)

Slide 18

If you DO NOT have items associated with your account
(screenshot of what it looks like to NOT have items in account)
Swipe up to make “Identify Found Item” option appear

Slide 19

AirTag Alert: Apple
(Screenshot of an AirTag detected notification)

Slide 20

(screenshot of AirTag detection near you)

Slide 21

(screenshot of Apple phone finding “Steve’s Keys”)

Slide 22
(screenshot reading “Searching Items… You can learn more about lost items or see if the owner has left a message by connecting to it. If you found an AirTag, you can learn more by holding the top of your iPhone over it until a notification appears.”)

Slide 23

(screenshot reading “About This AirTag. Serial Number: ABCED12FG345 Owner: (****) ***-6789
An AirTag is used to keep track of everyday items like keys or a bag. The serial number is registered to the owner of this AirTag. If this AirTag is not familiar to you, learn how to disable it and stop sharing your location. Instructions to disable”

Slide 24
Disabling AirTag

- Opening the AirTg to view the serial number disables the Tag – thereby alerting the offender that it’s been found
    - Law enforcement should come to victim and consider faraday bag
- Turning off Bluetooth will NOT stop the device from emitting a signal to the offender

- Take screenshot for evidence

Slide 25

*child trackers
Jiobit tracks no matter how far they run.
*pet trackers
(Screenshot of Tagg website)

Slide 26

(photo of Tagg pet tracker)

Slide 27

(photo of tracker)

Slide 28

Global Positioning System (GPS) Devices

Slide 29

Location Sharing
- May be coerced
- Victim may not realize they are sharing their location
- A stalker may utilize multiple methods/applications to track their victims

Slide 30

Percentage of People Checking In or Sharing Their Location By Platform and Privacy Settings
Facebook: Private 57.1% Public 42.9%
Instagram: Private 43.5% Public 56.5%
Snapchat Private 60.9% Public 39.1%
Twitter Private 26.5% Public 73.5%
Nearly 1 in 4 people felt it's extremely or moderately safe to share their location on social media.
30.7% of people with Snapchat shared their location on the Snapchat map.
2020 ADT LLC dba ADT Security Services. https://www.adt.com/resources/location-services-risks

Slide 31

Unidentified Caller

Slide 32

*67 Calls: TrapCall (trapcall.com)
(screenshot of webpage)

Slide 33

Here's how to unmask calls with TrapCall Video

Slide 34

Trap Call User Interface
(screenshot of webpage)

Slide 35

Spoofing

Slide 36

What You May Hear:

- "Numbers I don't recognize call and harass me."
- "I keep getting hang-up calls from random numbers."
- "It shows up as my mom/friend/someone I know, but it is the offender calling."
- "I know it's the offender, but it doesn't sound like them."
- "I blocked the offender, but they just keep calling me from different numbers."
- "People are saying I called them, but I didn't."

Slide 37

Video with QR and caption that reads "How can you remain anonymous when you call someone? The best way is by using SpoofCard. With SpoofCard you can change your CallerID"

Slide 38

Spoof Phone Calls
(screenshot of AppStore with 24 different IPhone Apps)

Slide 39

(screenshot of webpage called SpoofTel which offers a Free Caller ID Spoofing Trial)

Slide 40

Spoofing

- Offenders spoof number victim will answer

- Offenders spoof victim with court, police, or other numbers victim will answer
- Offenders believe we can't prove they spoofed the call

Slide 41

Documentation with a SpoofCard

- Phone records from: victim, "friend", and suspect
    - Victim's records show "friend" called but friend's records show no call
    - Suspect's records show a call to SpoofCard
        - Call the number and record
- Financial records of suspect

Slide 42

Stalkerware

Slide 43

Stalkerware: What You May Hear

- "They hacked my phone."
- "They hacked my account/s: e-mail, Facebook, Instagram, Snapchat…"
- "They're reading my texts."
- "They are listening to my calls."
- "They seem to know everything I've done on my phone."
- "They know my passwords and logins, even though I just changed them."
- "They have and/or are referencing pictures of me I took on my phone."
- "They keep showing up where I am."

Slide 44

What is Stalkerware?

- Commercially available software used for spying
- Made for individual use
- Typically hides itself from the list of installed programs and does not display any activity notifications

Slide 45

Cell Phone Spyware video

Slide 46

About Stalkerware

- Physical access to the device is almost always required for installation
- Can be on both Apple and Android devices, but more common on Android
- Best to assume all activities on device are being monitored

Slide 47

Removing Stalkerware
All actions may cause potential safety concerns!

- Factory reset
    - Note: this also destroys the evidence
- Change passwords on all apps/accounts when reinstalled
- Antivirus can sometimes remove stalkerware

Slide 48

Non-Stalkerware Possibilities
Sharing Settings:

- Phone login and password security
- Cloud/Account Backup
- Family sharing, “find my device”

Account Access:

- Individual accounts: email, social media, dating websites
- Smart device accounts
- Previously shared accounts

Other Tools:

- Devices: GPS tracker, key logger, cameras, recording devices
- Friends, family, colleagues

Slide 49

Public Data

Slide 50

Geotagging
Camera + GPS = Geotagging

Slide 51

Exif Viewers Show Geo-Info
Exif: Exchangeable image file format: Descriptive data (meta-data) in an image file that includes the date the photo was taken, resolution, shutter speed, focal length and geolocation
Exif Wizard by homedatasheet.com (screenshot of ITunes Store with app)

Slide 52

EXIF Data
(Photo of a couple and a screenshot of the program)

Slide 53

(screenshot from Google My Activity reading “Web & App Activity: Your Web & App Activity includes the things you do on Google services, like Maps, Search, and Play. It can also include things you do on sites, apps, and devices that use Google services or your voice and audio recordings. The activity you keep is used to give you more personalized experiences, like faster searches and more helpful app and content recommendations. You can see your activity, delete it manually, or choose to delete it automatically using the controls on this page. Learn more.”)

Slide 54

(screenshot from iCloud account webpage)

Slide 55

Find Yourself…
*FastPeopleSearch.com
*TruePeopleSearch.com
*PeopleSearchNow.com

Slide 56

Technology-Facilitated Stalking and Sexual Assault

Slide 57

Sexual Assault, Stalking, & Technology

- Offenders use technology to facilitate and cover up sexual violence
    - Using platforms to find and groom victims (messages, online communities)
    - Gifts that monitor or allow access
- Misusing access to publicly available data to gain information
- Threats to disseminate intimate images
    - Including those acquired through surveillance cameras
    - Sexual exploitation/trafficking via tech

Slide 58

(screenshots of news articles)
“Jebidiah Stipe, Wyoming Marine, Solicited Ex-Girlfriend’s Rape and Assault on Craigslist”
“Details emerge in Web rape case”
“Judge gives man 60 years in Craigslist rape case”

Slide 59

Dating App Facilitated Sexual Assault (DAppSAs)

- 14% of the 1,968 rapes committed by acquaintances occurred during and initial meetup arranged through a dating app
- High percentage of victims with self-reported mental illness (59.6%)
- More violent Sas than acquaintance Sas
    - Increased strangulation (32.4%); assaultive/penetrative acts; and victim injuries, especially anogenital and breast injuries

“Due to the increased violent nature of DAppSAs, the researchers propose that sexual predators use dating apps as hunting grounds for vulnerable victims.”

Slide 60

Dating App Concerns

- Use proximity-based location
- No screening out of sexual offenders
- DAppSA more likely to be currently enrolled college students (compared to non DAppSA victims)
- Male victims – percentage of DAppSA male victims was 2x more than rate of nonDAppSA male victims
- DAppSA victims were significantly more likely to self-report mental health and chronic medical issues

Slide 61

Non-Consensual Distribution of Intimate Images

Slide 62

16% of victims 18-24 years old report that the stalker shared nude, semi-nude, and/or sexually explicit photos or videos of them

Slide 63

New AI deepfake app creates nude images of women in seconds / The resulting fakes could be used to shame, harass, and intimidate their targets

Slide 64

Nonconsensual Image Resources
#CCRI Cyber Civil Rights Initiative
Image Abuse Helpline: 1-844-878-2274 CyberCivilRights.org
StopNCII.org Stop Non-Consensual Intimate Image Abuse
C.A. Goldberg Victims’ Rights Law Firm www.cagoldberglaw.com
DMCA Defender DMCADefender.com

Slide 65

Use of Technology to Stalk
Responding to Victims

Slide 66

Should Victims just log off?

Slide 67

Safety Planning and Technology
Victims may consider:

- Secure passwords
- Hard-to-guess security questions
- Enable 2-factor authentication
- Use a second, safer device with/if possible
- Learn about settings and location-sharing defaults, set these intentionally
- Be mindful of smart device and social media usage

Slide 68

Android and Gmail users should use Google's Security Checkup
Apple users should update their phones and use Apple's Safety Check

Slide 69

Gmail Safety Check

- Gmail account is connected to and controls key safety elements of Android phones
- Gmail account is also key to many important accounts for password reset
- Go to Security Checkup and review all tabs
    - Check access, sign-in, recovery, and sharing – including email forwarding or linked accounts

MyAccount/Google.com/security-checkup

Slide 70

Apple Safety Check

- Where?
    - Settings > Privacy and
    - Settings > Safety Check
- Why?
    - Location tracking, text messages, phone call history, emails, credit cards
    - Highest risk!

Slide 71

Documentation

- Screenshot or take photos of call log/ text conversation
- Overlap screenshots/photos
- Capture time and date
- Take screenshot/photo of the contact info
- Consider apps like Tailor or StitchIt

Slide 72

Facebook Documentation

- Capture and save screenshots (PrntScrn)
- Some sites offer a “download your information” service in account settings

Slide 73

Technology & Stalking: Big Picture

- Believe victims. Offenders can misuse technology a variety of creative ways to access, contact, and monitor their victims.
- This technology is out there – and it’s easy to use. Offenders don’t have to be particularly “tech savvy” to terrorize victims through technology
- Build knowledge on privacy/sharing settings across applications and devices. Sharing settings/defaults are often not intuitive
- Ask specific questions about offender contact and knowledge. This can better help you collect evidence and safety plan.
- Consider both evidence preservation and victim safety. See if the victim has access to a safer device.
- Charge relevant technology-related crimes (when appropriate and applicable).

Slide 74

Wrap Up & Resources

Slide 75

Just Tech Investigation & Prosecution of Online Abuse
Targeting prosecutors and law enforcement officers, Just Tech aims to increase the likelihood of positive case outcomes and victim experiences, as well as address the disproportionate impact of online abuse experienced by underserved communities.

Slide 76

Tech Safety
Welcome to the Tech Safety App. This app contains information that can help someone identify technology-facilitated harassment, stalking, or abuse and includes tips on what can be done.

Slide 77

For Victims
Victim Connect resource center
Confidential referrals for crime victims 855-4-VICTIM

Slide 78

(screenshot of a blank Stalking Incident Log document)

Slide 79

Stalking & Harassment Assessment & Risk Profile (SHARP) coercivecontrol.org
Narrative Report & Risk Profile
Safety Planning Suggestions

Slide 80

Stalking Response Checklists for Organizations & Campuses
(Screenshot of documents)

Slide 81

Campus Investigations & Hearings
Stalking & Title IX
(screenshots of documents)

Slide 82

Know it, name it, stop it.
Public Awareness Campus Workshop
(screenshots of documents and videos)

Slide 83

Order Stalking Awareness Brochures & Posters for your Community Today!

Slide 84

www.StalkingAwareness.org

- Practitioner guides
- Training modules
- Victim resources
- Webinars

@FollowUsLegally & SPARC

Sign up for our Newsletter!

Slide 85

Kendra Eggleston M.A.
Training & Campus Specialist SPARC
202.642.0295
KEggleston@stalkingawareness.org
StalkingAwareness.org
@FollowUsLegally