

The Use of Technology to Stalk

OVW Funding

This project was supported by Grant No. 15JOVW-22-GK-03986-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.



- *Practitioner guides
 - *Training modules
 - *Victim resources
 - *Webinars



Sign Up for our Newsletter!

Technology-Facilitated Stalking



Technology does not cause stalking. Stalkers cause stalking.



Technology & In-Person Stalking









The majority of stalking victims experienced both in-person stalking and technology-facilitated stalking.

SURVEILLANCE

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



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

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



INTIMIDATION

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

COMMON TECHNOLOGY TACTICS EXPERIENCED BY STALKING VICTIMS

66%



UNWANTED PHONE CALLS, VOICEMAILS, TEXT MESSAGES

UNWANTED E-MAILS OR SOCIAL MEDIA MESSAGES



55%

32%



MONITORED ACTIVITIES USING SOCIAL MEDIA

POSTED/THREATENED TO POST INAPPROPRIATE/PERSONAL INFO



29%

22%

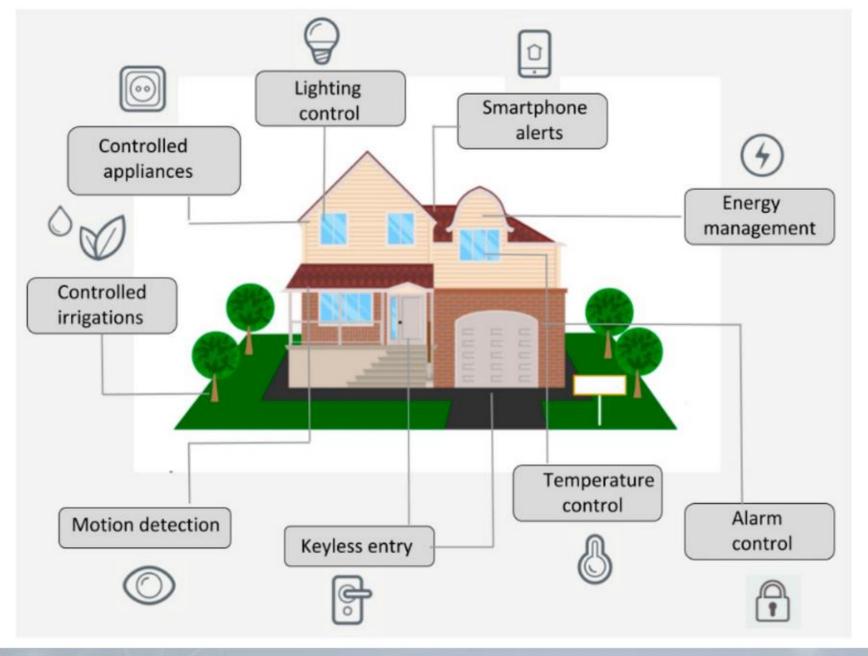


SPIED ON/MONITORED ACTIVITIES USING TECH

TRACKED LOCATION WITH ELECTRONIC DEVICE OR APP



14%





Tracking Location



How Do Stalkers Track Location?

Property Tags



Access to and/or Shared Victim Accounts









Installed Stalkerware





Family Trackers

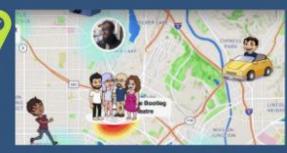






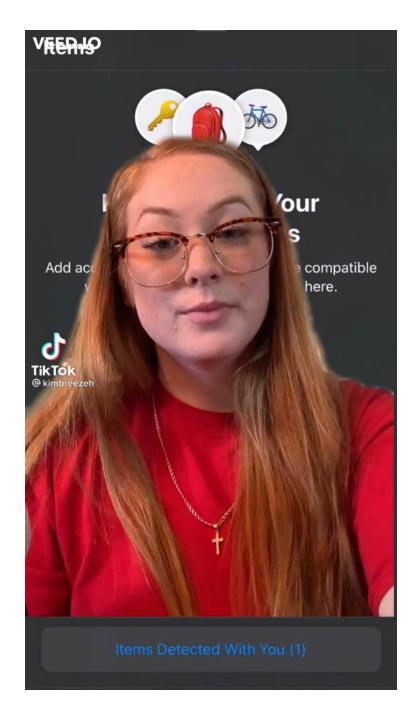
Social Media Maps/Check-ins





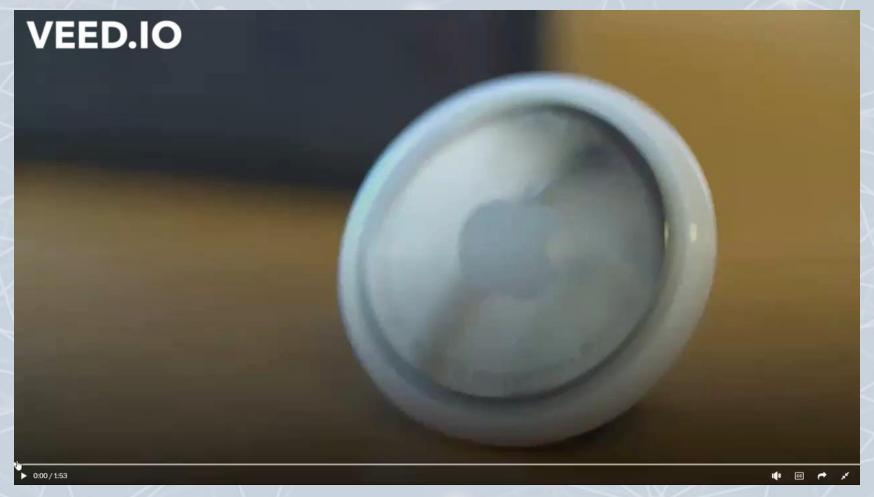
Proxy Stalking





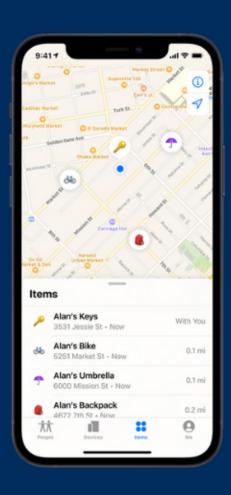


AirTags



Note: Notification time is now a few hours, NOT 3 days Android now has an automatic AirTag tracker

Understanding AirTags



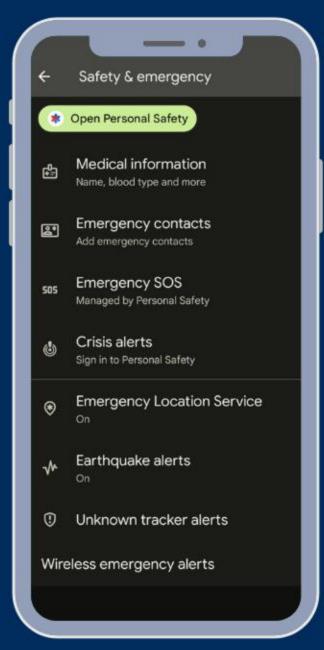
- Shows current location, not location history
- Frequency of the location update varies
 - Depends on other devices in range
- While Tile requires people to have downloaded the Tile app for the location tracking to "ping," AirTag "pings" off any Apple device within 800 feet

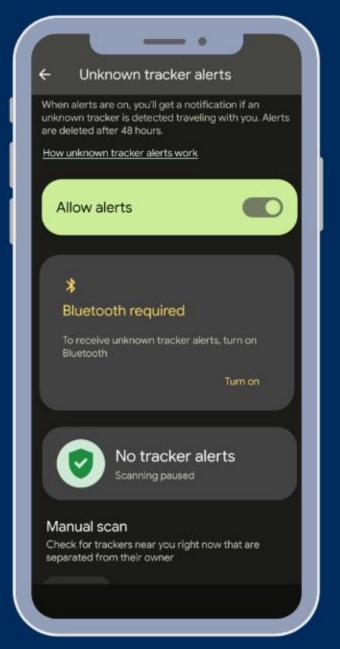
Notification Limitations

- 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



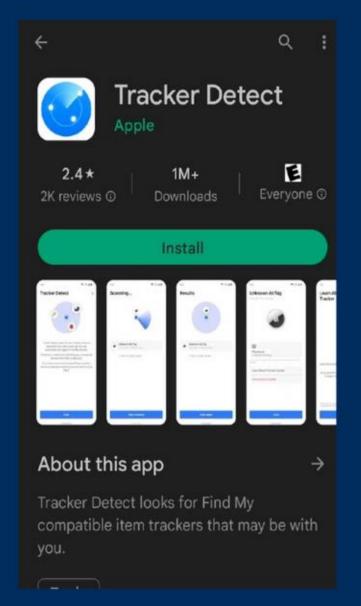




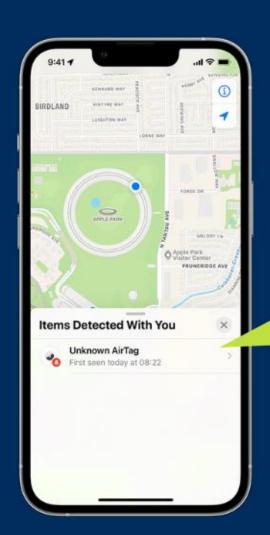


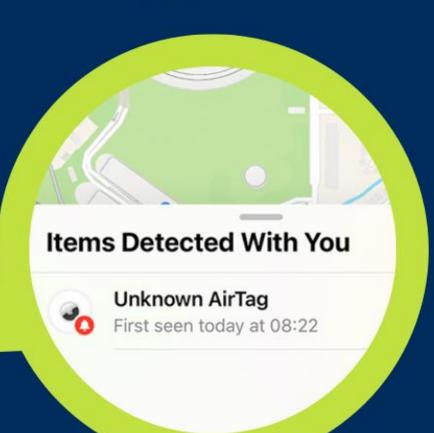
AirTag Alert: Android

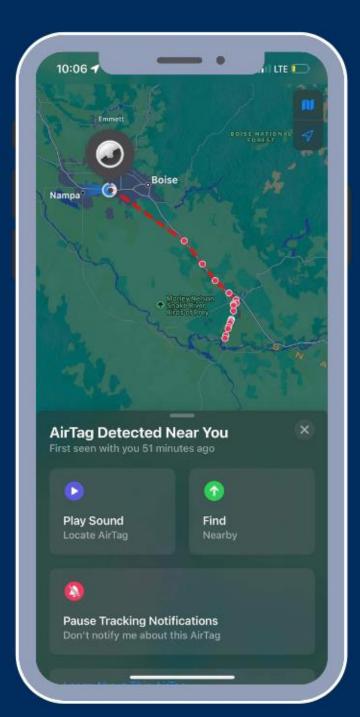


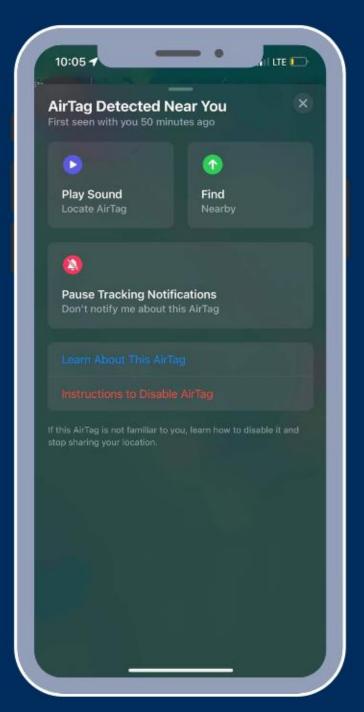


AirTag Alert: Apple







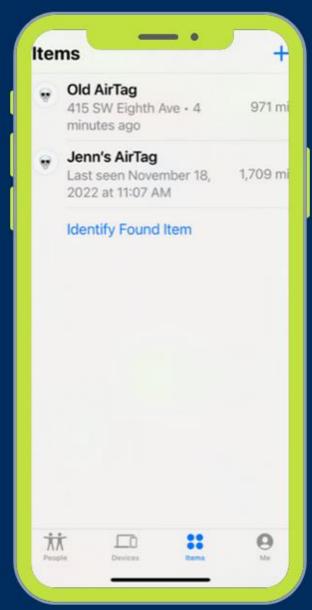


Apple: Search for "Find my" App

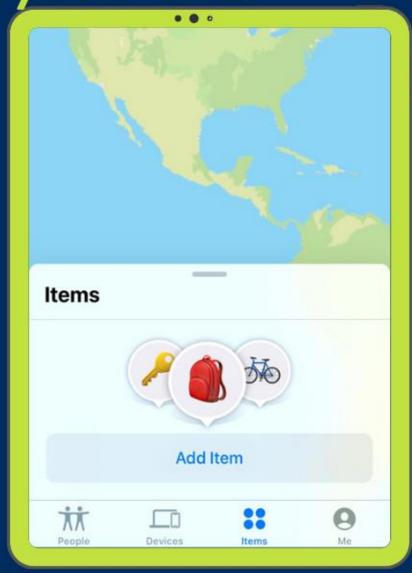


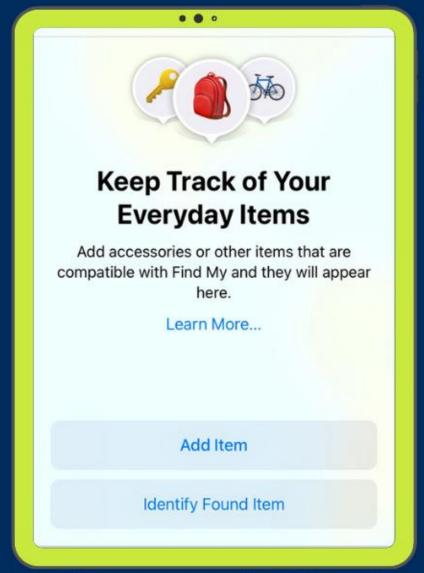
If you have items associated with your account





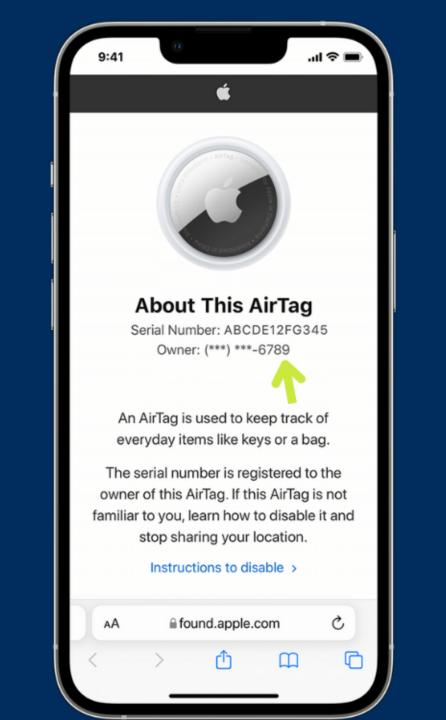
If you DO NOT have items associated with your account

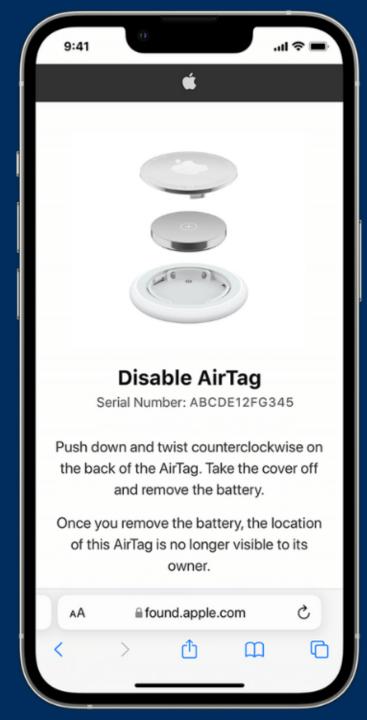




Swipe up to make "Identify Found Item" option appear







Disabling AirTag

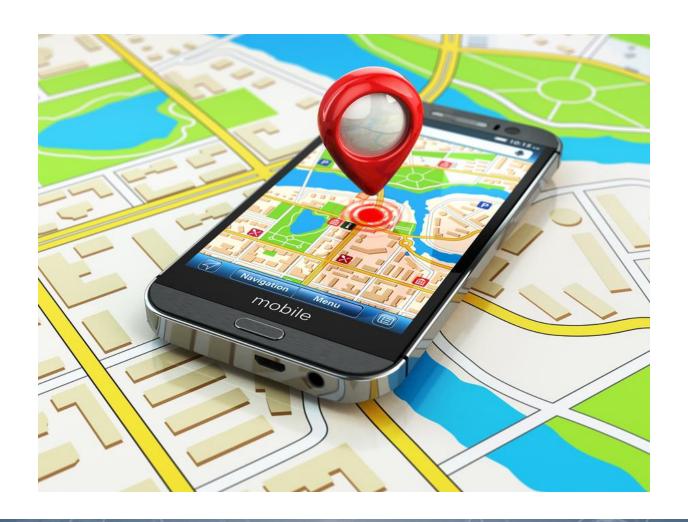
- Opening the AirTag to view the serial number disables the Tag -thereby alerting the offender that it's been found
 - Law enforcement should come to victim and consider faraday bag
- Turning off Bluetooth will NOT stop the device from emitting a signal to the offender
- Take screenshot for evidence

Evidence with AirTags

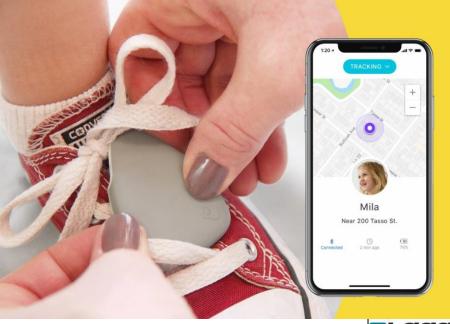
- * Serial number is unique to each AirTag
- * Serial number is on physical device, but will not show up on phone
- * Contact <u>lawenforcement@apple.com</u> to check device registration
- * Check financial records of suspect
- * Contextual evidence



Global Positioning System (GPS) Devices







9jiobił

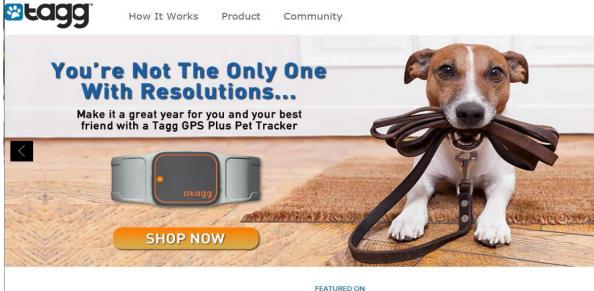
Jiobit tracks no matter how far they run.

* Child trackers

The

New Hork Times

* Pet trackers



OBENEWS





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

























Percentage of People Checking In or Sharing Their Location By Platform and Privacy Settings

	Private	Public		Private	Public
Facebook	57.1%	42.9%	Snapchat	60.9%	39.1%
Instagram	43.5%	56.5%	Twitter	26.5%	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.

Spoofing







What You May Hear:

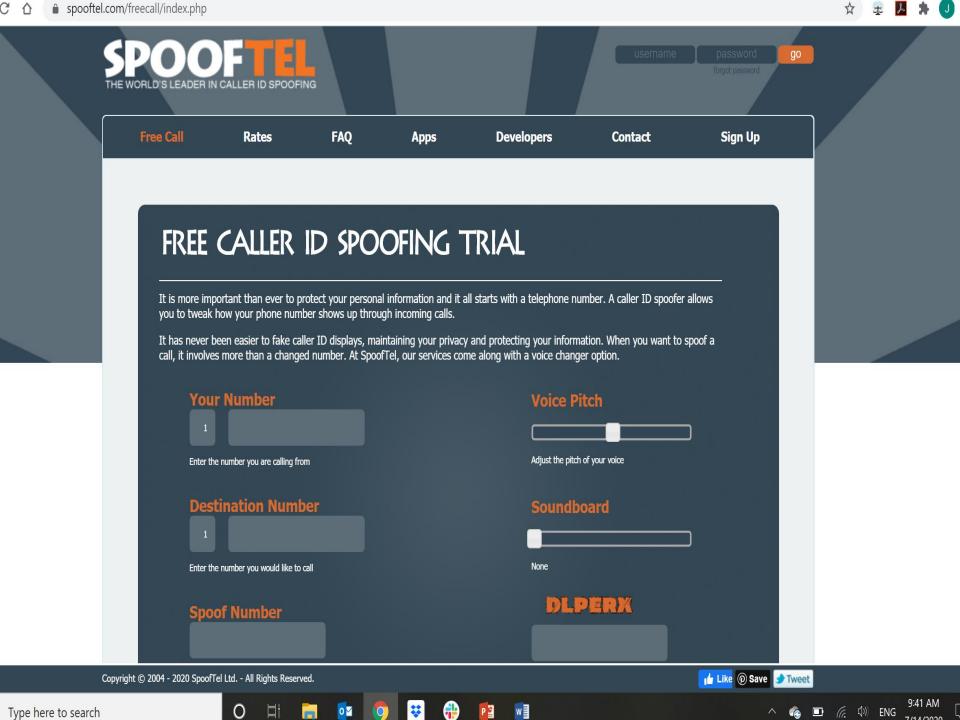






- "It shows up as my mom/friend/someone
 I know, but it is the offender calling."
- "I know it's the offender, but it doesn't sound like them."
- "I blocked the offender, but they just keep calling me from different numbers."
- "People are saying I called them, but I didn't."





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

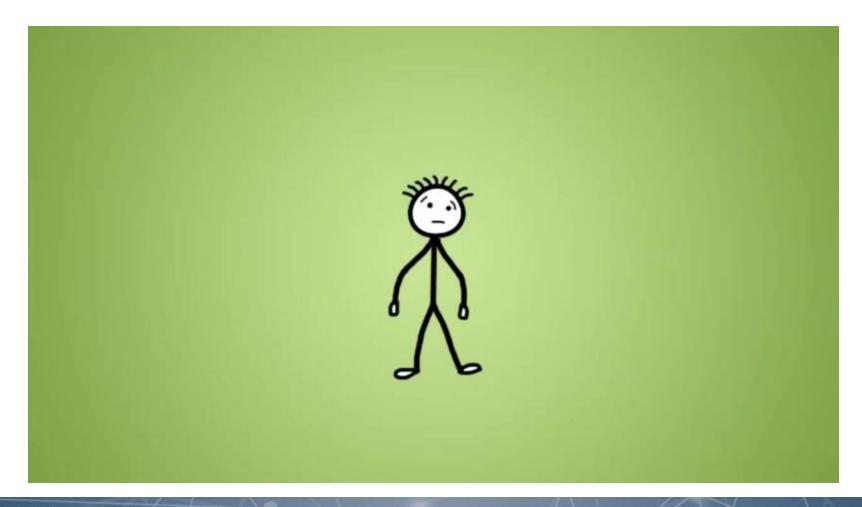
Documentation with a SpoofCard

- * 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

Stalkerware



Cell Phone Spyware





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."

What is Stalkerware?

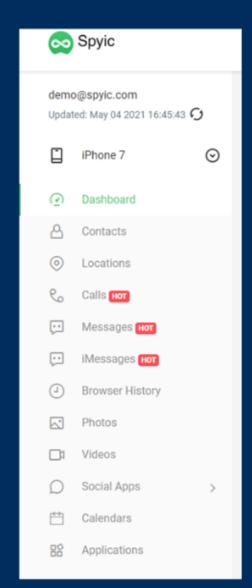


- Commercially available software used for spying
- Made for individual use
- Typically hides itself from the list of installed programs and does not display any activity notifications



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

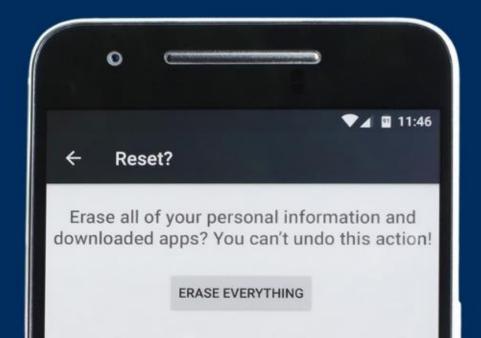




Removing Stalkerware

All actions may cause potential safety concerns!

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





Non-Stalkerware Possibilities



SHARING SETTINGS

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





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

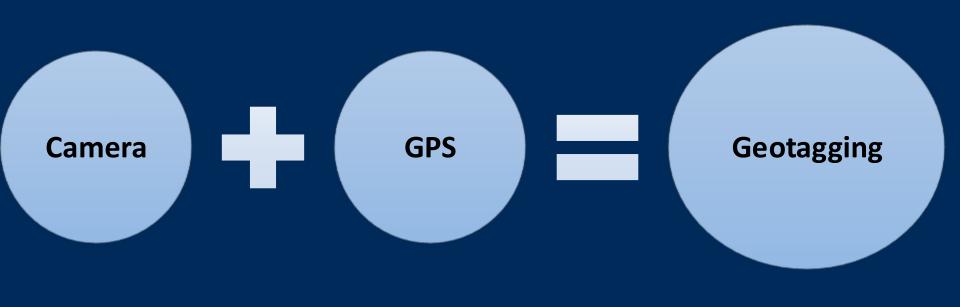


- Devices: GPS tracker, key logger, cameras, recording devices
- Friends, family, colleagues

Public Data



Geotagging





Exif Viewers Show Geo-Info

Exif: Exchangeable image file format: Descriptive data (meta-data) in an image file that include the date the photo was taken, resolution, shutter speed, focal length and geolocation

Exif Wizard By homedatasheet.com, Open iTunes to buy and down





EXIF Data









Jeffrey's Exif Viewer

From Web	Image URL:		View Image At
O FIOIII FIIE			

Basic Image Information

randomly.

information.

Dasie Image Information					
Target file:	IMG_7655[1].JPG				
Camera:	Apple iPhone 6				
Lens:	iPhone 6 back camera 4.15mm f/2.2 Shot at 4.2 mm Digital Zoom: 2.362934363×				
Exposure:	Auto exposure, Program AE, ¹ /30 sec, f/2.2, ISO 200				
Flash:	Off, Did not fire				
Date:	March 2, 2016 7:50:32PM (timezone not specified) (1 hour, 31 minutes, 8 seconds ago, assuming image timezone of US Pacific)				
Location:	Latitude/longitude: 38° 58' 1.9" North, 92° 22' 26.2" West (38.967208, -92.373947)				
	Location guessed from coordinates: 2200 Interstate 70 Dr SW, Columbia, MO 65203, USA				
	Map via embedded coordinates at: Google, Yahoo, WikiMapia, OpenStreetMap, Bing (also see the Google Maps pane below)				
	Altitude: 223 meters (731 feet) Camera Pointing: South				
File:	3,264 × 2,448 JPEG (8.0 megapixels) 1,193,426 bytes (1.1 megabytes)				
Color Encoding:	WARNING: Color space tagged as sRGB, without an embedded color profile. Windows and Mac browsers and apps treat the colors				

Images for the web are most widely viewable when in the sRGB color space and with an embedded color profile. See my Introduction to Digital-Image Color Spaces for more

Viewing EXIF data

- * Online exif data viewers
- * Apps
- * Right click on the photo on a desktop and go to properties-details

Safety Strategies

- * Turn location "off" on cell phone camera
- * Review social media site to determine if exif data can be viewed
- * Remove exif data using an online exif data removal tool

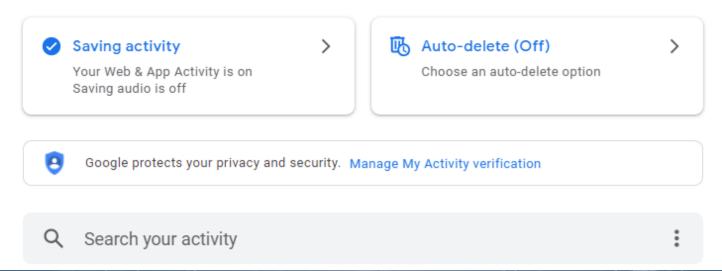




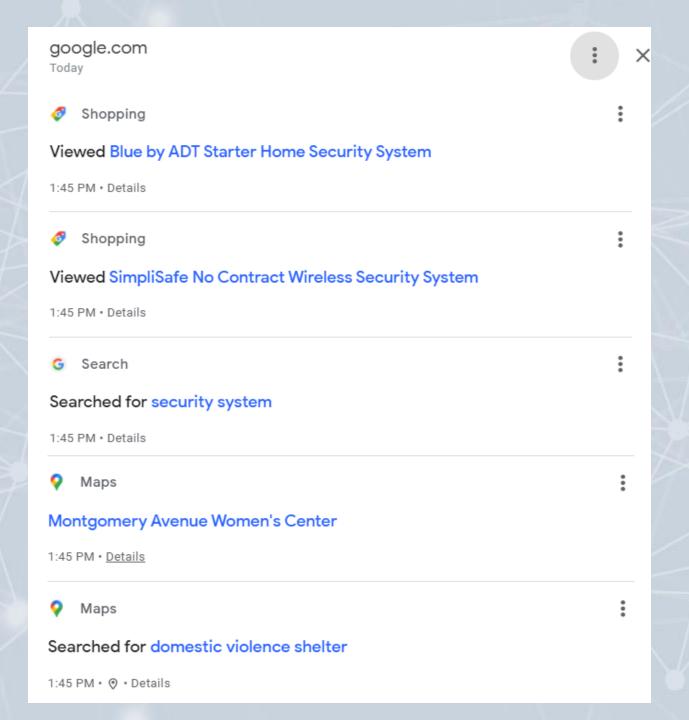
Web & App Activity

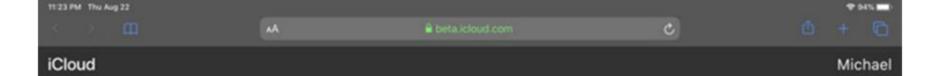
Your Web & App Activity includes the things you do on Google services, like Maps, Search, and Play. It can also include things you do on sites, apps, and devices that use Google services or your voice and audio recordings. The activity you keep is used to give you more personalized experiences, like 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











Good evening, Michael.

Account Settings >





Find iPhone

Find Yourself...

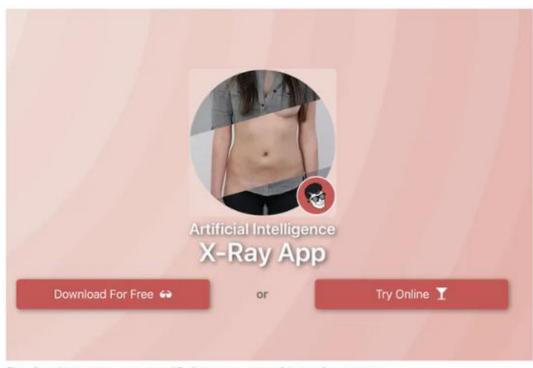
- * FastPeopleSearch.com
- * TruePeopleSearch.com
- * PeopleSearchNow.com

Non-Consensual Distribution of Intimate Images





New AI deepfake app creates nude images of women in seconds



/ The resulting fakes could be used to shame, harass, and intimidate their targets

By JAMES VINCENT

Jun 27, 2019, 6:23 AM EDT | O Comments / O New







The DeepNude app creates AI fakes at the click of a button.



Nonconsensual Image Resources



Image Abuse Helpline: 1-844-878-2274

CyberCivilRights.org



C.A.GOLDBERG

VICTIMS' RIGHTS LAW FIRM

www.cagoldberglaw.com





Technology-Facilitated Stalking and Sexual Assault



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

Jebidiah Stipe, Wyoming Marine, Solicited Ex-Girlfriend's Rape And Assault On Craigslist

Details emerge in Web rape case

California Marine also tried to solicit rape of ex-wife, authorities say

By WILLIAM BROWNING - Star-Tribune staff writer Feb 5, 2010 💂 0

Judge gives man 60 years in Craigslist rape case



Dating App Facilitated Sexual Assault (DAppSAs)









- 14% of the 1,968 rapes committed by acquaintances occurred during an 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.

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















Use of Technology to Stalk

Responding to Victims



Should victims just log off?

DELETE ACCOUNT?

Delete account and all data? This cannot be undone.

Cancel

DELETE

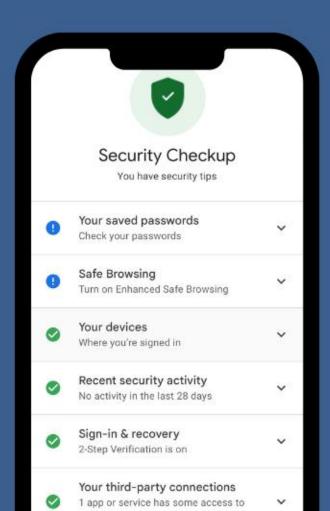
Safety Planning and Technology

Victims may consider:

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

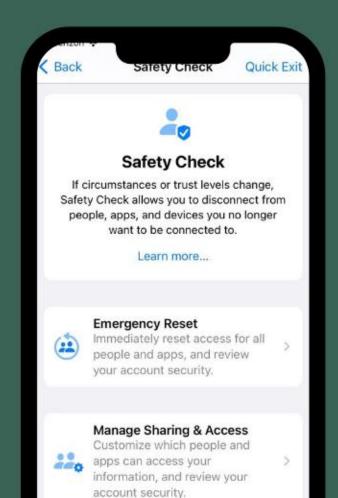


Android and Gmail users should use Google's Security Checkup

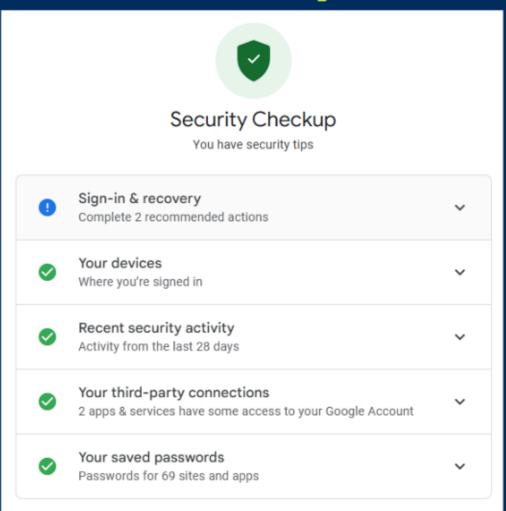




Apple users should update their phones and use Apple's Safety Check



Gmail Safety Check

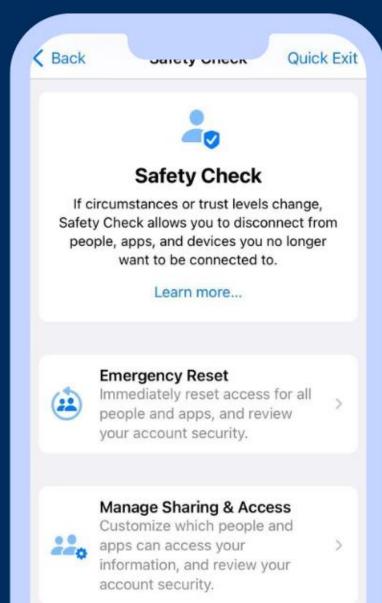


- Gmail account is connected to and controls key safety elements of Android phones
- Gmail account is also key to many important accounts for password reset
- Go to Security Checkup and review all tabs
 - Check access, sign-in, recovery, and sharing including e-mail forwarding or linked accounts

MyAccount/Google.com/security-checkup

Apple Safety Check

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



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



3:47 PM

1 0 ∦ 80% **■**







Today 3:40 PM

Answer your phone

I keep calling u

Over and over

But you aren't answering

Where are you?

Who are you with?

I need to tell you something important

Why aren't you answering me?

Please stop contacting me

All of these text messages and calls are starting to scare me. I will not respond after this text

What scares me is how you can treat me this way.

ANSWER YOUR PJONE!!!





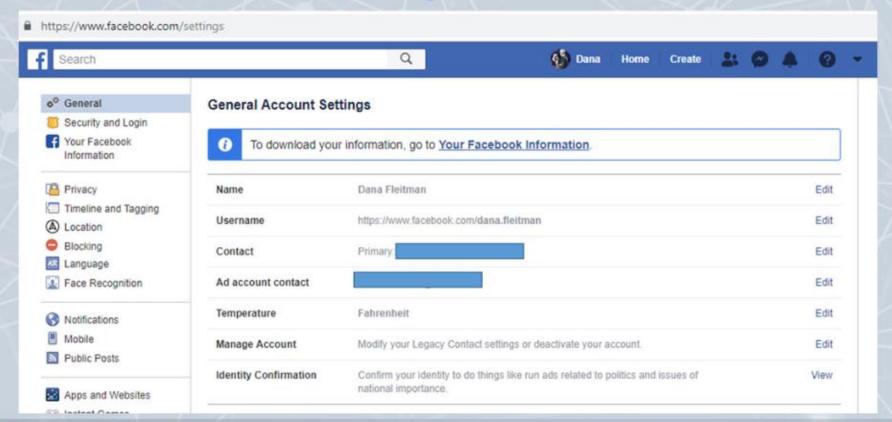






Facebook Documentation

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





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).



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.



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.









For Victims



Confidential referrals for crime victims 855-4-VICTIM



STALKING INCIDENT LOG

Date	Time	Description of Incident	Location of Incident	Witness Name(s) (Attach Address and Phone #)	Police Called (Report #)	Officer Name (Badge #)
-						
·-						
*						
i.e						
	*					



Wrap Up & Resources





STALKING RESPONSE CHECKLISTS FOR ORGANIZATIONS & CAMPUSES



Addressing Stalking: A Checklist for Domestic and **Sexual Violence Organizations**

Because there are very few stalking-specific service providers, stalking victims rely on d sexual violence programs to assist them with safety planning and resources. In reviews response to stalking, consider the following questions:

- Does your organization provide services to victims of stalking?
- If so, how easy is it for a stalking victim to know they can seek services from your For instance, is stalking specifically mentioned in your outreach materials?
- Do your organization's services address the needs of all victims of stalking ind stalked by someone who is not an intimate partner?

please use the checklist below assess your agency's efforts to respond to stalking Of course, different agencies vary in mission, scope, and capacity, so not all categ will be relevant to or feasible for every service provider.

Serving victims of stalking is included as part of your organization's state Organization Mission and Values values.

Website

- "Stalking" is mentioned on your website as a form of violence your age Your website links to <u>Victim Connect</u> (the referral hotline for victims of
- Your website provides definitional information/fact sheets on stalking
- ☐ Your website provides a link to a <u>stalking log</u> that victims can use to
- Your website features stories that focus on or include stalking.
- Your website notes that January is National Stalking Awareness M

- ☐ Your organization participates in National Stalking Awareness M Social Media relevant posts on your social media platforms.
 - describe platforms feature stories that focus on or inc

Yes	1	700	Consult.	_
	SF	N A		CONTRACT
N		J Ala		PRESVENTION
FAS			N 46	AWARENESS
				CHATTER

Addressing Stalking: A Checklist for Campus Professionals

Stalking is a violation of student conduct codes and Title IX, and a crime under the laws of the SO states, District of Columbia, U.S. Territories, and Federal government. Adults 18-24 years old experience the highest rates of stalking, making it vital for universities to appropriately address stalking on campus and ensure services are accessible to all

In reviewing your university's response to stalking, consider the following questions:

- Does your university provide stalking-specific services to victims? For example, counseling services for victims of stalking, access to an advocate for safety planning or information on campus no contact/protection orders
- How easy is it for a stalking victim to know they can seek services and from whom? For instance, is stalking mentioned specifically in outreach materials from your Title IX office, crisis center, gender resource center, office of residential life, and/or campus security/police?
- Do University policies and services address the needs of all victims of stalking, including those who do not primarily present as sexual assault victims and regardless of the victim-offender relationship, i.e. whether the
- stalker is/was an intimate partner, acquaintance, friend, stranger, family member, person of authority, etc.? Do University policies and services address stalkers and victims who are students, faculty, volunteers, alumni,

Use the checklist below to assess your campus efforts to respond to stalking.

Different offices and/or services vary in mission, scope and capacity, so not all categories or suggestions will be relevant or feasible. University programs that should consider this assessment include:

- Advocacy services □ Campus security/police/public safety
- Crisis center and/or hotline
- ☐ Gender resource center
- ☐ Greek life
- Health services

- Housing and residential life
- Mental health and counseling services
- ☐ Student affairs
- Student conduct and discipline
- ☐ Title IX office

1. Website Information

Stalking is listed as a form of violence the university addresses.

CAMPUS INVESTIGATIONS & HEARINGS

STALKING & TITLE IX

ASK THE ACCUSED / RESPONDENT

often the first to minimize what is happening to them and friends, family, peers, and responders also often e variousness. Any time a victim resorts are type of the rooms behavior, consider the possibility of a stalking case

TIPS FOR CAMPUS STALKING INVESTIGATIONS AND HEARINGS

Stalking is a serious, prevalent, and dangerous crime that impacts every campus in the United States; that is a violation of student conduct codes and Title IX; and that is a crime under the laws of the 50 states, District of Columbia, U.S. Territories, Uniform Code of Military Justice, and Federal government, as well as many tribal jurisdictions.

When a school investigates a report of stalking and holds disciplinary or Title IX hearings, there are a lot of things to consider.

This document provides guidance on what is important to consider and what is important to ask the victim/complainant and accused stalking/respondent. To refresh your understanding of stalking, watch webinars and read resources at Stalking/wareness.org. To review how stalking is covered under Title IX, see our resource on The Basics of Stalking and Title IX.

Schools that receive federal funding are required by Title IX to remedy any situation of sex discrimination, address its effects, and prevent it from happening again. Violating these requirements could cause a school to lose its federal funding or be liable for monetary damages to the student whose rights were violated.

IMPORTANT CONSIDERATIONS

Victims' perceptions of their own risk and what their stalker is capable of are one of the most accurate predictors of risk. The Stalking and Harassment Assessment and Risk Profile (SHARP) is a tool designed specifically to examine and assess stalking. It is a free web-based assessment available at www.CoerchesControl.org that assesses the "big picture" of the stalking situation and a victim's risk in the moment.

Remember that victims are sometimes unsure if what they are

Title IX defines stalking as a pattern of behavior directed at a specific person that would cause a reasonable person to fear for the person's safety or the safety of others; or suffer substantial emotional distress.

The individual incidents that establish a pattern of behavior may not be a violation

Fear is censual to the definition of scalking. Common stalking behaviors include—but are not limited to—responsed unwanted phone calls and messages, showing up when uninvited, following, surveillance, spreading,

What else can schools do to support stalking survivors?

Stalking is a crime under the laws of the 50 states, District of Columbia, U.S. Territories, Federal government, as well as many tribal codes. ¹⁴ Schools should ensure students know

People react to stalkers in a variety of ways. Some may seem irritated or angry rather than scared, while others may and dismiss their stalking as "no big deal." Irritation, anger, and/or minimization may be masking fear. It is helpful to c

STALKING AND TITLE IX: THE BASICS

What is Title IX?

From elementary schools to higher education, Title IX prohibits any school that receives federal funding from discrimination on the basis of sex and requires schools to respond so and remedy hostile educational environments. Violating these mean a school could lose its federal funding or be sued by the student whose rights under Title IX were violated.

Title IX of the Education Amendments of 1972:

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.

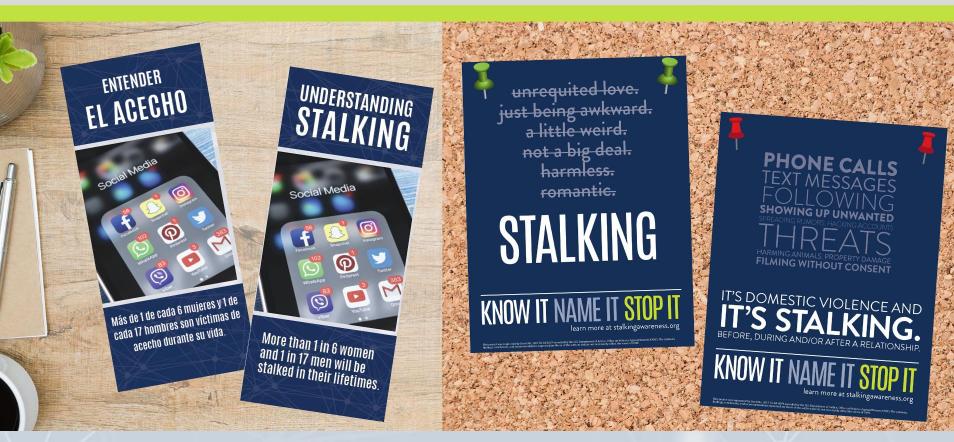
Supreme Court decisions and guidance from the U.S. Department of Education have further explained what Title IX means and what it covers. A school's Title IX responsibilities represent the floor, not the ceiling, of actions that schools can take to support victims.

Do schools have an obligation to protect their students from stalking under Title IX?

Title IX calls discrimination on the basis of sex "sexual harassment," with a slightly different meaning than you might think. It defines "sexual harassment" as unwelcome sexual or other conduct on the basis of sex, including a single instance of sexual assault, dating violence, domestic violence, or stalking.

New regulations announced by the Department of Education (DOE) in August 2020 specifically added stalking to the definition of sexual harassment. Prior to these new rules, Title IX did not explicitly recognize stalking as a form of sexual harassment. Unlike the informal guidance they replaced, the new Title IX regulations underwent a formal rulemaking process. This means that schools—at a minimum—are obligated to employene policies and procedures that adhere to the new regulations. The DOE will consult and apply the new regulations when determining whether a school violated Title IX or if a student's rights under Title IX were contacted by their school.

Order Stalking Awareness Brochures & Posters for your Community Today!





- *Practitioner guides
 - *Training modules
 - *Victim resources
 - *Webinars











@FollowUsLegally & SPARC

Sign Up for our Newsletter!

Kendra Eggleston M.A. Training & Campus Specialist

SPARC



202.642.0295



KEggleston@StalkingAwareness.org



StalkingAwareness.org



