1. What Is Online Harassment?

Online harassment may involve threatening or harassing emails, instant messages, or posting information online. It targets a specific person either by directly contacting them or by disseminating their personal information, causing them distress, fear, or anger.

Cyberstalking is a type of online harassment that involves using electronic means to stalk a victim, and generally refers to a pattern of threatening or malicious behaviors. All states have anti-stalking laws, but the legal definitions vary. Some state laws require that the perpetrator make a credible threat of violence against the victim. Others require only that the stalker’s conduct constitute an implied threat.

2. Who Is Affected?

In July 2017, the Pew Research Center’s American Trends Panel conducted a nationally representative survey of internet users’ experiences with online harassment. The survey found that 41% of Americans have been personally subjected to harassing behavior online, and 66% have witnessed harassing behaviors directed at others. Nearly one-in-five Americans (18%) have been subjected to particularly severe forms of harassment online, such as physical threats, harassment over a sustained period, sexual harassment or stalking.

3. Cyberstalking

Stalkers can use the anonymity of the Internet to commit their crimes. Many victims of cyberstalking don’t know the identity of the stalkers. That can make the fear more palpable and prosecution more unlikely.

Some examples of cyberstalking include:

- Sending manipulative, threatening, lewd or harassing emails from an assortment of email accounts.
- Hacking into a victim’s online accounts (such as banking or email) and changing the victim’s settings and passwords.
- Creating false online accounts on social networking and dating sites, impersonating the victim or attempting to establish contact with the victim by using a false persona.
- Posting messages to online bulletin boards and discussion groups with the victim’s personal information, such as home address, phone number or Social Security number. Posts may also be lewd or controversial – and result in the victim
receiving numerous emails, calls or visits from people who read the post online.
- Signing up for numerous online mailing lists and services using a victim's name and email address.

Cyberstalking is difficult to combat because the stalker could be in another state or sitting three cubicles away from the victim. Online anonymity can make it difficult to verify a stalker’s identity, collect the necessary evidence for an arrest and then trace the cyberstalker to a physical location.

Social networking presents security issues for victims of stalking. A profile on a social network might include information such as your email address, phone number, general (or even specific) address information, birthday, legal name, names of family members, and even minute-to-minute updates on your location. If a victim has a public profile, a stalker could easily access any information posted to the social networking account. Even with strong privacy settings or a private profile, a stalker might be able to access your account. A few of the ways this can be accomplished include:

- Hacking your account
- Creating a false profile and sending a "friend request" or "follow request." The request may even appear to be from a known friend or family member. Verify with your friends and family members that they own the account before accepting the request.
- Gaining access to the accounts of your already-established connections (such as Facebook friends or Twitter followers).

Often related to social media is another type of harassment called “revenge porn,” or the online posting of explicit photos or videos of people without their permission. There are laws providing for criminal and civil liability for revenge porn, but victims may want to first take action to get the material taken down as quickly as possible. Many social media sites have created policies for reporting and removing this kind of material from their websites.

If you are a victim of stalking, consider suspending your social networking accounts until the stalking has been resolved. If you decide to continue to use social networking sites, here are a few tips to help keep you safe:

- Take advantage of privacy settings. With some social networking sites, you may be able to make your profile completely private simply by checking a box. With others, such as Facebook, privacy settings can be complex to navigate.
- Take advantage of added security settings. One of the best examples is two-factor authentication. When you enable this, your account will require you to provide something you know (like a password) with something you have (like a specific device). Therefore, if someone gets your password he or she will not be able to log in to the account without the specific code that the service sends to your device. You can find a list of sites offering two-factor authentication at [https://twofactorauth.org/][4].
- Limit how much personal information you post to your account. For example, you may not want to include contact information, your birth date, the city you were born in or names of family members.
- Do not accept "friend requests" (or "follow requests") from strangers. If you recognize the individual sending the request, contact him or her off-line to verify he or she sent the request.
- Warn your friends and acquaintances not to post personal information about you, especially your contact information and location.
- Avoid posting photographs of your home that might indicate its location. For example, don't post photographs showing a house number or an identifying landmark in the background.
- Use caution when joining online organizations, groups or "fan pages." Never publicly RSVP to events shown online.
- Use caution when connecting your cell phone to your social networking account. If you do decide to connect your cell phone to your online account, use extreme caution in providing live updates on your location or activities.
- Avoid posting information about your current or future locations, or providing information a stalker may later use to hone in on your location, such as a review of a restaurant near your house.
- Always use a strong, unique [password][5] for every social networking site.

4. California Law

California was the first state to pass an anti-stalking law in 1990, but now all 50 states have an anti-stalking law.

In California, both criminal and civil laws address stalking and online harassment. According to the criminal laws, a stalker is someone who willfully, maliciously and repeatedly follows or harasses another (victim) and who makes a credible threat with the intent to place the victim or victim's immediate family in fear for their safety. The victim does not have to prove that the stalker had the intent to carry out the threat. ([California Penal Code 646.9][6])

California’s criminal laws addressing online harassment state that it is illegal to use an electronic communication device to make
repeated contact with another person with the intent to harass or annoy, or to make a single intentionally harressing contact if it includes any obscene or threatening language. (California Penal Code 653m.) Additionally, it is illegal to make credible threats by means of any electronic communication device, including but not limited to telephones, cell phones, smart phones, tablets and computers. (California Penal Code 442.)

Another law makes it a crime to use an electronic communication device to distribute personal information of another person without their consent, and with the intent to harass them or cause them fear. (California Penal Code 653.2)

The criminal penalty for stalking is imprisonment up to a year and/or a fine of up to $1,000. There are more severe penalties when the stalker pursues the same person in violation of a court restraining order, with a sentencing range of two to four years imprisonment. Persons convicted of felony stalking also face stricter penalties if they continue to stalk their victim(s). Courts may issue restraining orders to prohibit stalking. (California Family Code 6320)

A victim, family member or witness may request that the California Department of Corrections, county sheriff or the director of the local department of corrections notify them by phone or mail 15 days before a convicted stalker is released from jail or prison. The victim, family member or witness must keep these departments notified of their most current mailing address and telephone number. The information relating to persons who receive notice must be kept confidential and not released to the convicted stalker. (California Penal Code 646.92) The court may order a person convicted of felony stalking to register with local law enforcement officials within 14 days of moving to a city and/or county. (California Penal Code 646.9)

A victim of stalking may bring a civil lawsuit against the stalker and recover money damages. (See Civil Code 1708.7 for the elements and remedies of the tort of stalking.)

When stalking occurs in the workplace, an employer can request a temporary restraining order or an injunction on behalf of the employee who is a victim of stalking. (California Code of Civil Procedure 527.8)

Victims may also request that the California Department of Motor Vehicles (DMV) suppress their automobile registration and driver's license records from being released to persons other than court and law enforcement officials, other governmental agencies or specified financial institutions, insurers and attorneys. (California Vehicle Code 1808.21, 1808.22) Victims may also request that voter registration information, changes to their names and addresses, and other personally identifying information be kept confidential. It is prohibited for anyone to knowingly publicly post the personal information of a stalking or domestic violence victim with the intent to put them in danger or in fear of danger. (California Gov’t Code 6205-6210)

Many other states also have confidentiality programs that allow victims to suppress personal information.

California also has laws against “revenge porn,” or the online posting of explicit photos of people without their permission. It is a crime to take explicit photos or videos of another person and distribute them in a way that is intended to cause emotional distress. This applies to the distribution of both photos that the perpetrator took of the victim, as well as pictures the victim took of him/herself. If the victim is a minor, or if the perpetrator has previously been convicted, the punishment is more severe. (California Penal Code 647(j), 647(k)). For information on other states’ laws against revenge porn, see http://www.cagoldberglaw.com/states-with-revenge-porn-laws/[7].

5. Federal law

Federal laws that deal with stalking and harassment:

Unauthorized Information: The Computer Fraud and Abuse Act creates civil and criminal liability for a person who obtains any information from any internet-connected computer without authorization. An additional civil and criminal remedy exists for those who access a computer with the intent to defraud. This statute could be useful in situations where a victim has been secretly recorded through his/her own computer, or where the perpetrator gained access to sexual photos or videos through unauthorized access to the victim’s computer. (8 U.S.C. 1030)

Copyright Infringement: Victims of nonconsensual online publication of intimate photographs or videos (revenge porn) may bring a civil suit for copyright infringement if the victim is the person who originally took the picture, and is thus the copyright owner. (17 U.S.C. 50)

Eavesdropping: If non-consensually published material was originally obtained by the perpetrator’s intercepting an electronic communication, he may be criminally and civilly liable. (18 U.S.C. 2511)

Interstate Threats and Extortion: A person who publishes or threatens to publish private photos or videos of another with the
The intention of forcing the victim to do something he/she would not have done otherwise may be charged with extortion, if the perpetrator communicated with the victim via interstate commerce channels (phones, computers, internet, etc.) (18 U.S.C. 875)

- Interstate Stalking: Section 2261A(1) makes it a federal crime to travel across state, tribal or international lines to stalk another person with "the intent to kill, injure, harass, or place under surveillance with intent to kill, injure, harass, or intimidate another person." Furthermore, the travel must result in reasonable fear of death, serious bodily injury or substantial emotional distress either to a victim or a victim's family member, spouse or intimate partner. Section 2261A(2) makes it a federal crime to stalk another person across state, tribal or international lines, using regular mail, email, or the Internet. The stalker must have the intent to kill, injure, harass, intimidate or cause substantial emotional distress, or to place a victim or a victim's family member, spouse or intimate partner in fear of death or serious bodily injury. (18 U.S.C. Section 2261A [8])

- Interstate Domestic Violence: Section 2261(a)(1) makes it a federal crime to travel across state, tribal, or international lines with the intent to kill, injure, harass, or intimidate a spouse or intimate partner and to commit, or attempt to commit, a crime of violence against that spouse or intimate partner. 2261(a)(2) makes it a federal crime to cause a spouse or intimate partner to cross state, tribal, international lines, by force, coercion, duress, or fraud, and to commit, or attempt to commit, a crime of violence against that spouse or intimate partner. (18 U.S.C. Section 2261)

- Interstate Violation of a Protection Order: Section 2262(a)(1) makes it a federal crime to travel across state, tribal, or international lines with the intent to violate a protection order and to subsequently engage in conduct that violates that order.

- Harassing Telephone Calls in Interstate Communications: This statute makes it a federal crime to use a telephone, the internet, or any other telecommunications device to annoy, abuse, harass, or threaten another person at the called number. (47 U.S.C. Section 223(a)(1)(C))

- Falsifying Caller ID: It is possible for callers to disguise their identity by falsifying the telephone number that appears on the recipient’s caller ID. This is called “caller ID spoofing” and was made illegal by the Truth in Caller ID Act, which prohibits the transmitting of misleading or inaccurate caller ID information with the intent to defraud, cause harm, or wrongfully obtain anything of value. Violators are subject to a penalty of up to $10,000 per violation. If you suspect that caller ID information has been falsified, you can file a complaint with the FCC.

- Caller ID Blocking: Federal law protects the privacy of the person calling by requiring telephone companies to provide the option to block one’s phone number. Callers must have the choice to reveal or block their numbers for any interstate calls. To block your phone number for any call, dial *67 before making a call. To unblock your number, dial *82.

6. Resources

National Center for Victims of Crime

- 2000 M St. NW, Ste. 480
  Washington, D.C. 20036
  Phone: (202) 467-8700
  Web: http://www.victimsofcrime.org/ [9]


Office for Victims of Crime (U.S. Department of Justice)

- The OVC has an online Directory of Crime Victim Services [2]. The directory allows you to search by state or country for services that match specific types of victimization.

National Domestic Violence Hotline

- The NDVH helps victims find safe houses. (800) 799-SAFE

National Network to End Domestic Violence
• Specializes in technology-based stalking
• Web: www.nnedv.org [12]

Cyberstalking Resources:

• 12 Tips to Protect Yourself from Cyberstalking, http://womensissues.about.com/od/violenceagainstwomen/a/CyberPrevention.htm [14]

Other Websites:

• Association of Threat Assessment Professionals, www.atapworldwide.org [16] (no endorsement implied)

Source URL (modified on October 25, 2018): https://www.privacyrights.org/consumer-guides/online-harassment-cyberstalking

Links
[5] https://www.privacyrights.org/blog/your-password-%E2%80%9C%EF%BB%80%EF%BB%80%E2%80%9D-all-wrong
[8] http://www.law.cornell.edu/uscode/18/usc_sec_18_00002261---A000-.html