



# Privacy Rights Clearinghouse

Empowering Consumers. Protecting Privacy.

Published on *Privacy Rights Clearinghouse* (<https://www.privacyrights.org>)

Today's Date: Dec 20, 2014

---

## Fact Sheet 14: Are You Being Stalked?

Copyright © 1994 - 2014  
Privacy Rights Clearinghouse  
Posted June 1994  
Revised July 2014

\*\*\*\*\*

**This is for informational purposes only.**

**We are not able to counsel stalking victims.**

**If you need counseling or assistance, please go to**

<http://ovc.ncjrs.gov/findvictimservices/search.asp>

[1]

or

<http://victimsofcrime.org/help-for-crime-victims/find-local-assistance---connect-directory> [2]

for victim assistance.

For additional resources please see:

[Resources](#)

\*\*\*\*\*

\*

1. [What Is Stalking?](#)
2. [Who Is Affected?](#)
3. [Cyberstalking](#)
4. [California Law](#)
5. [Federal Law](#)
6. [Tips for Stalking Victims](#)
7. [Resources](#)

## 1. What Is Stalking?

Stalking refers to harassing or threatening behavior that is engaged in repeatedly. Such harassment can be either physical stalking or cyberstalking.

- Physical stalking is following someone, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing one's property.
- Cyberstalking involves using the Internet or other electronic means to harass.

Either type of action may or may not be accompanied by a credible threat of serious harm. But both types can cause psychological damage, and each can potentially lead to an assault or even murder.

All states have anti-stalking laws, but the legal definitions vary. Some state laws require that the perpetrator, to qualify as a stalker, make a credible threat of violence against the victim. Others require only that the stalker's conduct constitute an implied threat.

**We regret that we are not able to provide telephone assistance or counseling to stalking victims. If you need counseling or any other type of assistance, please see the [Resources](#) [3] section below.**

## 2. Who Is Affected?

In September 2012, the Bureau of Justice Statistics (BJS) released a report on Stalking Victims in the United States.

<http://www.bjs.gov/index.cfm?ty=pbdetail&iid=1211> [4]. The BJS report found that:

- During a 12-month period, an estimated 1.5% of persons age 18 or older were victims of stalking.
- The percentage of stalking victims was highest for individuals who were divorced or separated (3.3%), compared to those married, never married, or widowed.
- A greater percentage of females were stalked than males; however, females and males were equally likely to experience harassment.

**Young adults are the primary targets of stalking; most victims are less than 35 years old. Women are more likely to be the victims of stalking, though stalking incidents are reported to the police by men as often as by women.**

Most victims know their stalker. Slightly more than 30% of stalking offenders are a known, intimate partner - a current or former spouse, a co-habiting partner, or a date. Approximately 45% of stalking offenders are acquaintances other than intimate partners. Just under 10% of all stalkers are strangers. In approximately 15% of stalking cases, the victim does not know the identity of the stalker and thus cannot report whether he or she might be an intimate partner, acquaintance or stranger.

**Individuals who are divorced or separated are at the greatest risk (3.4%) for stalking.**

**Financial toll.** A stalking victim may need to take time from work to change a phone number, move, replace damaged property, obtain a restraining order or testify in court. Of the 79% of stalking victims who were employed during the 12 months preceding the SVC interview, 1 in 8 lost time from work. 130,000 victims reported that they had been fired from or had been asked to leave their jobs because of stalking.

About 16% of victims reported property damage in conjunction with stalking.

Stalkers may also commit **identity theft** against victims – including opening or closing accounts, taking money from accounts, or charging purchases to a victim's credit card. Learn more about preventing identity theft by reading PRC [Fact Sheet 17: Coping with Identity Theft](#) [5].

### 3. Cyberstalking

In recent years stalkers have seized on the anonymity of the Internet to commit their crimes. This has added a new dimension because many victims of cyberstalking don't know the identity of the stalkers. That can make the fear more palpable and prosecution more unlikely.

It is difficult to define cyberstalking because it can appear in so many forms. As technology evolves, so does the practice of cyberstalking. A web-savvy stalker can wreak havoc on the online life of a victim. This can be incredibly damaging, particularly as more people use the Internet to pay bills, make friends, date, work, share ideas and find jobs.

Some examples of tactics a cyberstalker may use 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. In the anonymous world of the Internet, it is difficult to verify a stalker's identity, collect the necessary evidence for an arrest and then trace the cyberstalker to a physical location.

For a list of state cyberstalking laws, see the **National Conference of State Legislature's** [State Electronic Harassment or "Cyberstalking" Laws](#) [6] .

If you are a victim of cyberstalking, try to gather as much physical evidence as possible and document each contact. For more information and tips, visit the [National Center for Victims of Crimes webpage: If You Are a Victim of Cyberstalking](#) [7].

The fact that cyberstalking doesn't involve physical contact doesn't mean it is any less dangerous than "real life" stalking. It's not difficult for an experienced Internet user to find enough of the victim's personal information, such as phone number or place of business, to establish his or her physical location.

**Social networking**, through websites such as Facebook, Twitter, MySpace, Meetup and LinkedIn, present 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:

1. Hacking your account
2. 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.
3. Gaining access to the accounts of your already-established connections (such as Facebook friends or Twitter followers).

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. Lifehacker has an article titled "[Here's Everywhere You Should Enable Two-Factor Authentication Right Now](#) [8]" that lists specific sites offering two-factor authentication (note that the article is from August 2012 and that you should not consider the list complete).
- **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 online polls or quizzes, particularly those that ask for personal information.
- Don't post 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 for every social networking site. Read our [10 Rules for Creating a Hacker-Resistant Password](#) [9].
- Final tip: remember, you most likely will not know if your stalker has accessed your online social networking account. Only post information that would not expose you to harm if your stalker should read it.

The reality is that both cyberstalking and physical stalking can lead to a physical attack. Always get help quickly, document all stalking incidents and take precautions to protect yourself.

We regret that we are not able to provide telephone assistance or counseling to cyberstalking victims. If you need counseling or any other type of assistance, please see the [Resources](#) [3] section below.

#### **4. California Law**

California was the first state to pass an anti-stalking law in 1990 in response to the stalking and murder of actress Rebecca Schaeffer. Now, all states have an anti-stalking law.

In California, both criminal and civil laws address stalking. 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, [www.leginfo.ca.gov](http://www.leginfo.ca.gov) [10])

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.)

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)

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)

#### **5. Federal law**

Stalking first received widespread public focus in 1980 with the murder of John Lennon, and again in 1981 with John Hinckley Jr.'s assassination attempt on President Reagan. But it was not

until the 1989 death of Rebecca Schaeffer, a rising young actress killed by an obsessed fan who'd stalked her for two years, that laws were enacted.

Such high-profile cases raised the public's awareness of this crime. But the majority of stalking victims are ordinary people, mostly women, who are being pursued and threatened by someone with whom they have had a prior relationship.

Federal laws that deal with stalking:

- Full Faith and Credit (1994; 2000). This federal law mandates nationwide enforcement of orders of protection, including injunctions against harassment and stalking, in states, tribes, and U.S. territories. ([18 U.S.C. Section 2265](#) [11])
- Interstate Stalking (1996; 2000). 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](#) [12])
- Interstate Domestic Violence (1994; 2000). 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](#) [13])
- Interstate Violation of a Protection Order (1994; 2000). 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. Section 2262(a)(2) makes it a federal crime to compel another person to cross state, tribal, or international lines by force, coercion, duress, or fraud and to subsequently engage in conduct that violates a protection order. ([18 U.S.C. Section 2262](#) [14])

- Federal Domestic Violence Firearm Prohibitions (1994; 1996). Section (g) (8) makes it a federal crime to possess a firearm or ammunition if subject to a "qualifying" protection order issued on behalf of a spouse or intimate partner. Section (g)(9) makes it a federal crime, punishable by up to 10 years in prison, to possess a firearm or ammunition if convicted in any state or federal court of a "qualifying" misdemeanor crime of domestic violence. ([18 U.S.C. Section 922](#) [15])
- Interstate Communications. This statute makes it a federal crime to transmit in interstate or foreign communications any threat to kidnap or injure another person. ([18 U.S.C. Section 875\(c\)](#) [16])
- Harassing Telephone Calls in Interstate Communications. This statute makes it a federal crime to use a telephone or other telecommunications device to annoy, abuse, harass, or threaten another person at the called number. ([47 U.S.C. Section 223\(a\)\(1\)\(C\)](#) [17])
- For more information about federal and state laws on stalking and harassment, visit the [National Center for Victims of Crime website](#) [18].

## 6. Tips for Stalking Victims

These tips will help you guard your personal information and lessen the chance that it will get into the hands of a stalker or harasser. However, some of these tips are extreme and should only be used if you are indeed being stalked. Harassment can take many forms, so this information may not be appropriate in every situation and may not resolve serious stalking problems.

See also the Supplement to this fact sheet, PRC [Fact Sheet 14a: Security Recommendations for Stalking Victims](#) [19], provided by the Los Angeles Police Department's Threat Management Unit.

**We regret that we are not able to provide telephone assistance or counseling to stalking victims. If you need counseling or any other type of assistance, please see the [Resources](#) [3] section below.**

1. **Use a private post office box.** Residential addresses of post office box holders are generally confidential. However, the U.S. Postal Service will release a residential address to any government agency, or to persons serving court papers. The Post Office only requires verification from an attorney that a case is pending. This information is easily counterfeited. Private companies are generally stricter and will require that the person making the request have an original copy of a subpoena.



Be sure to get a private mailbox that is at least two ZIP codes away from your residence. Use your private post office box address for all of your correspondence. Print it on your checks instead of your residential address. Instead of recording the address as "Box 123," use "Apartment 123." If you must use a traditional home mailbox, make sure it has a lock.

2. **Do not file a change of address with the U.S. Postal Service.** Send personal letters to friends, relatives and businesses giving them the new private mailbox address. Give true residential address only to the most trusted friends. Ask that they do not store this address in rolodexes or address books that could be stolen.
3. **Sign up for your state's address confidentiality program.** As of October 2007, 28 states had an address confidentiality program, though many of the other states and territories had some mechanism in place to protect victim confidentiality. Address confidentiality programs offer a no-cost mail-forwarding program that enables victims of domestic violence and stalking to protect their residential address. A few states limit the program to just the driver's license or voter records. For a list, visit the Stalking Resource Center's [Address Confidentiality Programs Chart](#) [20].
4. **Obtain an unpublished and unlisted phone number.** The phone company lists names and numbers in directory assistance (411) and publishes them in the phone book. Make sure you delete your information from both places. Do not print your phone number on your checks. Provide a work number or use an alternate number such as a voice mail number when asked – that is, a message-only number that is used solely for receiving recorded messages from callers. Consider replacing you landline with a cell phone if you haven't already done so. (see [below](#)) Always use caution when sharing your number.
5. **If your state has Caller ID, order Complete Blocking** (called "Per Line" Blocking in some states). This can help prevent your phone number from being disclosed when you make calls from your home. Be aware that blocking is not 100% effective. Programming "glitches" can sometimes inadvertently reveal blocked numbers. At least one company now offers a service that can "unblock" blocked numbers. It does this by forwarding your call to a toll-free number, which can then capture your phone number.

For the best protection, use a pre-paid calling card from a pay phone (but this may reveal the general location of the pay phone). As payphones are become less prevalent, you may also try a pre-paid cell-phone (see [below](#)). Consider using a Caller ID Spoofing service to mask your number. Also see PRC [Fact Sheet 19: Caller ID and My Privacy](#) [21].

6. **Buy a pre-paid cellular phone with cash.** You typically do not need to provide a billing address or sign a contract for these kinds of phones. Be sure to get a phone number with a different area code from your current location. The most secure phones are those that do not connect to the Internet. When activating your phone, provide little or no personal information. Immediately disable any location tracking services (talk to your carrier or refer to the manual to learn how to do this). Try to keep a charged cell phone readily accessible to call for help in the event of an attack.

Some websites advertise a service to pinpoint the physical location of any cell phones (including those with location tracking disabled) using triangulation of signals to cell towers. Regardless of what these websites promise, it is extremely unlikely that anyone other than law enforcement agents and telecommunications companies have the ability to track the location of cell phones in the U.S. unless the phones have location tracking enabled or special software installed. Most of the time, a stalker would need physical access to your phone to install software in order to use location tracking devices. At a minimum, a stalker (or even the police) would need to know a victim's phone number in order to track his or her location through the phone.

You can protect your phone number by using a Caller ID Spoofing service when you make phone calls. This will allow you to choose whatever number you want to appear on the recipient's Caller ID. Remember that when the phone is powered off completely, not even the police or a telecommunications carrier can track its location.

If your stalker somehow learns your phone number, change your number by contacting your carrier. For maximum security, replace the phone entirely (especially recommended if your stalker gets physical access to your phone). Some domestic violence shelters offer free cell phones to battered women.

7. Guard the cell phones of your children. If your child has a cell phone, remember that it too can be an avenue for tracking you. A stalker who intercepts your child's phone, such as a former partner who has partial custody of a child, can load tracking or recording software onto a cell phone. Be just as cautious with a child's phone as you are with your own.
8. **Avoid calling toll-free 800, 866, 888, 877 and 900 number services.** Your phone number could be "captured" by a service called Automatic Number Identification. It will also appear on the called party's bill at the end of the month. If you do call toll-free 800 numbers, use a pay phone or a prepaid cellular phone (see [above](#)) that can be quickly disposed of, should the number become compromised.

9. **Have your name removed from any "reverse directories."** The entries in these directories are in numerical order by phone number or by address. These services allow anyone who has just one piece of information, such as a phone number, to find where you live. Reverse directories are published by phone companies and direct marketers. Contact the major directories and request that you be removed from their listings:

- Haines Criss+Cross Directory, Attn: Director of Data Processing, 8050 Freedom Ave. N.W. , North Canton, OH 44720.  
By phone: Call (800) 843-8452 and ask for extension 312.
- Equifax Direct Marketing Solutions (formerly Polk):  
By mail: Equifax Direct Marketing Solutions, Attn: List Suppression File, PO Box 740256 Atlanta GA 30374  
Include your name, address, ZIP code, phone number and a description of what information you would like suppressed.  
By phone: (888) 567-8688.

Review our list of [Online Information Brokers](#) [22] to find out what companies may be publishing your information online. Some of these, such as Switchboard.com, are online reverse directories. Opt-out when possible if you believe they have accurate contact information for you.

10. **Let people know that information about you should be held in confidence.** Tell your employer, co-workers, friends, family and neighbors of your situation. Alert them to be suspicious of people inquiring about your whereabouts or schedule. If you have a photograph or description of the stalker and vehicle, show a photo or describe the person to your neighbors, co-workers, friends, family and neighbors.
11. **Do not use your home address when you subscribe to magazines.** In general, don't use your residential address for anything that is mailed or shipped to you.
- 10a. Do not accept packages** at work or home unless they were personally ordered by you.
12. **Avoid using your middle initial.** Middle initials are often used to differentiate people with common names. For example, someone searching public records or credit report files might find several people with the name Jane Doe. If you have a common name and want to blend in with the crowd, do not add a middle initial. In fact, consider using your first initial and last name only in as many situations as you can.

13. **When conducting business with a government agency**, only fill in the required pieces of information. Certain government agency records are public. Anyone can access the information you disclose to the agency within that record. Public records such as those held by a county assessor, county recorder, registrar of voters, or state motor vehicles department (DMV) are especially valuable to a stalker, as are business licenses.

**Ask the agency if it allows address information to be confidential in certain situations.** If possible, use a commercial post office box and do not provide your middle initial, phone number or your Social Security number. If you own property or a car, you may want to consider alternative forms of ownership, such as a trust. This would shield your personal address from the public record. (For more information on government records and privacy, see PRC [Fact Sheet 11: From Cradle to Grave - Government Records and Your Privacy](#) [23])

14. **Put your post office box on your driver's license.** Don't show your license to just anyone. Your license has a lot of valuable information to a stalker, including your date of birth.

15. **Don't put your name on the list of tenants** on the front of your apartment building. Use a variation of your name that only your friends and family would recognize.

16. **Be very protective of your Social Security number.** It is the key to much of your personal information. Don't pre-print the SSN on anything such as your checks. Only give it out if required to do so, and ask why the requester needs it. The Social Security Administration may be willing to change your SSN. Contact the SSA for details. (See PRC [Fact Sheet 10: My Social Security Number - How Secure Is It?](#) [24])

17. **Alert the three credit bureaus**--Experian, Equifax and Trans Union. Put a fraud alert on your credit reports to avoid fraudulent access. Better yet, freeze your credit reports. (See PRC [Fact Sheet 17a: Identity Theft - What to Do if It Happens to You](#) [25] for information on establishing fraud alerts and security freezes.

18. **If you are having a problem with harassing phone calls**, put a beep tone on your line so callers think you are taping your calls. Use an answering machine or voicemail service to screen your calls, and put a "bluff message" on your machine to warn callers of possible taping or monitoring. Be aware of the legal restrictions on taping of

conversations.

Use an answering machine even if you already have Caller ID. It is possible for a tech-savvy stalker to circumvent Caller ID by having a trusted number appear when he or she calls. This practice is known as Caller ID Spoofing. Consider screening your calls by allowing all incoming calls to go to the answering machine before you pick up.

If you have harassing or threatening messages left on your answering machine or voicemail, tape record them in case you need them as evidence for a restraining order or in filing a police report. (See PRC [Fact Sheet 3: How to Put an End to Unwanted or Harassing Phone Calls](#) [26]. See also PRC [Fact Sheet 9: Wiretapping and Eavesdropping on Telephone Calls](#) [27]. The [Reporters Committee for Freedom of the Press](#) [28] offers a 50-state guide to laws regarding taping phone calls.)

**19. If you are a victim of cyberstalking, act promptly and firmly to defuse the situation.**

Take potential threats seriously. Very clearly tell that person to stop, saying something like, “Do not contact me in any way in the future.” Sometimes it is helpful to copy your “stop” message to the abuse department of the harasser’s Internet service provider. (If you have trouble determining that ISP, contact [www.Cyberangels.org](http://www.Cyberangels.org) [29] or [www.Haltabuse.org](http://www.Haltabuse.org) [30].)

Do not respond to any further messages from the harasser or have anyone else contact the harasser on your behalf. Change your email address if necessary. Do not enter any personal information into online directories. See [Cyberstalking Resources](#) at the end of this guide and the PRC's [Fact Sheet 18: Privacy and the Internet](#) [31]. For a list of state cyberstalking laws, see [National Conference of State Legislatures](#) [6].

**20. Keep a log of every stalking incident.** Building such a paper trail can make a successful prosecution more likely. Examples of evidence that may help build a case include: Caller ID records, logs of phone calls, copies of threatening letters and email messages, items sent to you in the mail, pictures of injuries, or even photos of the stalker outside your home. Plus, maintain a list of names, dates and times of your contacts with law enforcement.

**21. Consider getting professional counseling** and/or seeking help from a victims support group. They can help you deal with fear, anxiety and depression associated with being stalked.

22. **Make a police report. Consider getting a restraining order** if you have been physically threatened or feel that you are in danger. Study your state's stalking law to gain a clear understanding of what conduct constitutes an offense under the statute. You should contact an attorney or legal aid office if a restraining order becomes necessary.

When filed with the court, a restraining order legally compels the harasser to stay away from you, or he/she can be arrested. Be aware that papers filed for a restraining order or police report may become public record. Put minimal amounts of information on such documents and provide only a post office box address.

**Note:** Some security experts warn that restraining orders sometimes lead to violence. Before obtaining a restraining order, consider your options carefully.

23. **Be cautious about applying for a domain name.** If you use your name as a Web site domain name (for example, [www.janedoe.com](http://www.janedoe.com) [32]), it will be relatively simple for potential stalkers to locate your physical address because that information is available in the domain-name databases. Check your current listing by visiting [www.domainwhitepages.com](http://www.domainwhitepages.com) [33]. When registering a domain, look into private web registration services.

24. **Develop a safety plan.** Remember, even restraining orders do not always prevent stalking from escalating into violence. Make sure friends, neighbors, and co-workers know about your situation. Show them photos of the stalker. Keep handy the phone numbers of assisting agencies. Set up easy access to a reserve of money, credit cards, medication, important papers, keys, and other valuables in case you need to leave quickly. Have a safe place in mind that you can go in an emergency. Try not to travel alone. Always vary your routes. Carry a cell phone with you.

25. Password-protect all accounts, even your utilities. A stalker may try to transfer funds out of your bank account, cancel your credit cards or even cancel phone, electric or water service. Protect yourself by having hard-to-crack passwords on all of your accounts. See PRC [Alert: 10 Tips for Creating a Hacker-Resistant Password](#) [9].

26. **Be aware of your cellular phone's geolocation technology.** Geolocation technology built into your cell phone may enable a stalker to ascertain your location. You are at greater risk if the stalker has had access to your phone or your cellular account, and thereby may have had the ability to turn on geolocation tracking. If you suspect that your phone's geolocation tracking has been activated, call your carrier to find out. Request

that it be turned off. In fact, many domestic violence shelters will remove the battery from a victim's cell phone and/or turn it off to insure that the phone's geolocation feature cannot be used to locate the victim.

27. **And these final tips** from someone who was stalked for over three years: For your own protection, carry pepper spray. Get a mobile phone. Carry a digital or video camera. Never verify anything like your home address over the phone.

## 7. 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/> [34]
- Read its guide for stalking victims on the Stalking Resource Center page, <http://www.victimsofcrime.org/our-programs/stalking-resource-center> [35]
- [Listen to an audio presentation](#) [36] by the Stalking Resource Center and other experts on the topic of "Stalking and Orders of Protection," (June 6, 2011).

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

- The OVC has an online [Directory of Crime Victim Services](#) [1]. 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  
Web: [www.ndvh.org](http://www.ndvh.org) [37]  
E-mail: [ndvh@ndvh.org](mailto:ndvh@ndvh.org) [38]

### National Network to End Domestic Violence

- Specializes in technology-based stalking
- Web: [www.nnedv.org](http://www.nnedv.org) [39]
- E-mail: [safetynet@nnedv.org](mailto:safetynet@nnedv.org) [40]
- [Privacy & Safety on Facebook-A Guide for Survivors of Abuse](#) [41]

## American Overseas Domestic Violence Crisis Center (AODVCC)

- Skilled at helping victims navigate out-of-country issues
- Have a 24-hour help line and also work with email and IM chat
- Web: <http://www.866uswomen.org/Get-Help-Now.aspx> [42]
- E-mail: [crisis@866uswomen.org](mailto:crisis@866uswomen.org) [43]
- Phone: 866-USWOMEN (879-6636)

## Cyberstalking Resources:

- Working to Halt Online Abuse, [www.haltabuse.org](http://www.haltabuse.org) [44]
- Wired Safety, [http://wiredsafety.org/index.php?option=com\\_content&view=category&id=96&layout=log&Itemid=41](http://wiredsafety.org/index.php?option=com_content&view=category&id=96&layout=log&Itemid=41) [45]
- Cyberangels, [www.cyberangels.org](http://www.cyberangels.org) [46]
- Women's Issues, 12 Tips to Protect Yourself from Cyberstalking, <http://womensissues.about.com/od/violenceagainstwomen/a/CyberPrevention.htm> [47]

## Other Websites:

- National Coalition Against Domestic Violence, list of state-by-state resources for victims, [www.ncadv.org/resources/StateCoalitionList.php](http://www.ncadv.org/resources/StateCoalitionList.php) [48]
- End Stalking in America, [www.esia.net](http://www.esia.net) [49]
- Feel Safe Again (Sandy's Law, Massachusetts) [www.feelsafeagain.org](http://www.feelsafeagain.org) [50]
- Association of Threat Assessment Professionals, [www.atapworldwide.org](http://www.atapworldwide.org) [51] (no endorsement implied)

\*\*\*\*\*

**This is for informational purposes only.**

**We are not able to counsel stalking victims.**

**If you need counseling or assistance, please go to**

<http://ovc.ncjrs.gov/findvictimservices/search.asp> [1]

or

<http://victimsofcrime.org/help-for-crime-victims/find-local-assistance---connect-directory> [2]

for victim assistance.

Tags:



- [Harassment & Stalking](#) [52]
- [Fact Sheet](#) [53]
- [cyberstalking](#) [54]
- [harassing phone calls](#) [55]
- [stalking](#) [56]

[Copyright © Privacy Rights Clearinghouse](#). This copyrighted document may be copied and distributed for nonprofit, educational purposes only. For distribution, see our [copyright and reprint guidelines](#). The text of this document may not be altered without express authorization of the Privacy Rights Clearinghouse.

### **Links:**

- [1] <http://ovc.ncjrs.gov/findvictimservices/search.asp>
- [2] <http://victimsofcrime.org/help-for-crime-victims/find-local-assistance---connect-directory>
- [3] <https://www.privacyrights.org/content/are-you-being-stalked#7>
- [4] <http://www.bjs.gov/index.cfm?ty=pbdetail&iid=1211>
- [5] <https://www.privacyrights.org/fs/fs17-it.htm>
- [6] <http://www.ncsl.org/issues-research/telecom/cyberstalking-and-cyberharassment-laws.aspx>
- [7] <http://www.victimsofcrime.org/our-programs/stalking-resource-center/stalking-information/the-use-of-technology-to-stalk>
- [8] <http://lifehacker.com/5938565/heres-everywhere-you-should-enable-two+factor-authentication-right-now>
- [9] <https://www.privacyrights.org/ar/alertstrongpasswords.htm>
- [10] <http://www.leginfo.ca.gov>
- [11] [http://www.law.cornell.edu/uscode/html/uscode18/usc\\_sec\\_18\\_00002265----000-.html](http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002265----000-.html)
- [12] [http://www.law.cornell.edu/uscode/18/usc\\_sec\\_18\\_00002261---A000-.html](http://www.law.cornell.edu/uscode/18/usc_sec_18_00002261---A000-.html)
- [13] [http://www.law.cornell.edu/uscode/html/uscode18/usc\\_sec\\_18\\_00002261----000-.html](http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002261----000-.html)
- [14] [http://www.law.cornell.edu/uscode/html/uscode18/usc\\_sec\\_18\\_00002262----000-.html](http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002262----000-.html)
- [15] [http://www.law.cornell.edu/uscode/html/uscode18/usc\\_sec\\_18\\_00000922----000-.html](http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00000922----000-.html)
- [16] [http://www.law.cornell.edu/uscode/html/uscode18/usc\\_sec\\_18\\_00000875----000-.html](http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00000875----000-.html)
- [17] [http://www.law.cornell.edu/uscode/html/uscode47/usc\\_sec\\_47\\_00000223----000-.html](http://www.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000223----000-.html)
- [18] [http://www.ncvc.org/src/main.aspx?dbID=DB\\_Register204](http://www.ncvc.org/src/main.aspx?dbID=DB_Register204)
- [19] <https://www.privacyrights.org/fs/fs14a-stalking.htm>
- [20] <http://www.victimsofcrime.org/docs/src/state-address-confidentiality-programs.pdf?sfvrsn=0>
- [21] <https://www.privacyrights.org/fs/fs19-cid.htm>
- [22] <https://www.privacyrights.org/online-information-brokers-list>
- [23] <https://www.privacyrights.org/fs/fs11-pub.htm>
- [24] <https://www.privacyrights.org/fs/fs10-ssn.htm>
- [25] <https://www.privacyrights.org/fs/fs17a.htm>
- [26] <https://www.privacyrights.org/fs/fs3-hrs2.htm>
- [27] <https://www.privacyrights.org/fs/fs9-wrtp.htm>
- [28] <http://www.rcfp.org/reporters-recording-guide>
- [29] <http://www.Cyberangels.org>

[30] <http://www.Haltabuse.org>  
[31] <https://www.privacyrights.org/fs/fs18-cyb.htm>  
[32] <http://www.janedoe.com>  
[33] <http://www.domainwhitepages.com/>  
[34] <http://www.victimsofcrime.org/>  
[35] <http://www.victimsofcrime.org/our-programs/stalking-resource-center>  
[36] [http://bwjp.ilinc.com/perl/ilinc/lms/recording\\_launch.pl?pvr\\_id=916561&session\\_id=tfjkjvtz](http://bwjp.ilinc.com/perl/ilinc/lms/recording_launch.pl?pvr_id=916561&session_id=tfjkjvtz)  
[37] <http://www.thehotline.org/>  
[38] <mailto:ndvh@ndvh.org>  
[39] <http://www.nnedv.org/>  
[40] <mailto:safetynet@nnedv.org>  
[41] [https://fbcdn-dragon-a.akamaihd.net/hphotos-ak-prn1/851584\\_613437522011141\\_1298974833\\_n.pdf](https://fbcdn-dragon-a.akamaihd.net/hphotos-ak-prn1/851584_613437522011141_1298974833_n.pdf)  
[42] <http://www.866uswomen.org/Get-Help-Now.aspx>  
[43] <mailto:crisis@866uswomen.org>  
[44] <http://www.haltabuse.org>  
[45] [http://wiredsafety.org/index.php?option=com\\_content&view=category&id=96&layout=blog&Itemid=41](http://wiredsafety.org/index.php?option=com_content&view=category&id=96&layout=blog&Itemid=41)  
[46] <http://www.cyberangels.org>  
[47] <http://womensissues.about.com/od/violenceagainstwomen/a/CyberPrevention.htm>  
[48] <http://www.ncadv.org/resources/StateCoalitionList.php>  
[49] <http://www.esia.net>  
[50] <http://www.feelsafeagain.org>  
[51] <http://www.atapworldwide.org>  
[52] <https://www.privacyrights.org/category/topics/harassment-stalking>  
[53] <https://www.privacyrights.org/taxonomy/term/129>  
[54] <https://www.privacyrights.org/category/tags/cyberstalking>  
[55] <https://www.privacyrights.org/category/tags/harassing-phone-calls>  
[56] <https://www.privacyrights.org/category/tags/stalking>