DEFINITIONS

- **Stalking** occurs when a person willfully, maliciously, and repeatedly follows, harasses, or cyberstalking another person. § 784.048(2).

- **Aggravated Stalking** occurs when a person willfully, maliciously, and repeatedly follows, harasses, or cyberstalking another person and makes a credible threat to that person. § 784.048(3).

- **Cyberstalking** means
  - To engage in a course of conduct to communicate, or to cause to be communicated, words, images, or language by or through the use of electronic mail or electronic communication, directed at a specific person; or
  - To access, or attempt to access, the online accounts or Internet-connected home electronic systems of another person without that person’s permission, causing substantial emotional distress to that person and serving no legitimate purpose. § 784.048(1)(d).

- **Harass** means to engage in a course of conduct directed at a specific person which causes substantial emotional distress to that person and serves no legitimate purpose. § 784.048(1)(a).

- **Sexual Cyberharassment** means to publish to an Internet website or disseminate through electronic means to another person a sexually explicit image of a person that contains or conveys the personal identification information of the depicted person without the depicted person’s consent, contrary to the depicted person’s reasonable expectation that the image would remain private, for no legitimate purpose, with the intent of causing substantial emotional distress to the depicted person. Evidence that the depicted person sent a sexually explicit image to another person does not, on its own, remove his or her reasonable expectation of privacy for that image. § 784.049(2)(c)

- **Course of Conduct** means a pattern of conduct composed of a series of acts over a period of time, however short, which evidences a continuity of purpose. The term does not include constitutionally protected activity such as picketing or other organized protests. § 784.048(1)(b).

- **Credible Threat** means a verbal or nonverbal threat, or a combination of the two, including threats delivered by electronic communication or implied by a pattern of conduct, which places the person who is the target of the threat in reasonable fear for his or her safety or the safety of his or her family members or individuals closely associated with the person, and which is made with the apparent ability to carry out the threat to cause such harm. It is not necessary to prove that the
person making the threat had the intent to actually carry out the threat. The present incarceration of the person making the threat is not a bar to prosecution under this section. § 784.048(1)(c).

### COMMON METHODS OF ELECTRONIC STALKING

Stalkers can be creative as well as cruel. Unfortunately, they are able to practice both qualities within a world in which technology changes rapidly. As with other online services, a stalker may spoof a friend account to gain access to the victim’s profile. The havoc wreaked by electronic stalking can be devastating. In *Cyber Self-Defense* by Alexis Moore and Laurie J. Edwards, published by Lyon’s Press (2014), Alexis Moore recounts that even after escaping physical abuse from the man she once considered to be her “dream man”, he continued to make her life miserable for four years by electronically draining her banking accounts, cancelling her credit cards, destroying her credit, and tampering with her email, until she was finally able to extricate herself from him.

Due to constant changes in technology, the common methods of electronic stalking listed below are not exclusive; rather, this list covers some of the more common methods of electronic stalking. Courts should take care to focus on the particulars of the case in front of them to be sure that one of the less common methods of electronic stalking is not overlooked.

- **Social Media Stalking**

  **Facebook Stalking.** By the fourth quarter of 2019, Facebook had almost 2.5 billion monthly active users. Compare that to the end of the calendar year 2012 in which there were over one billion registered users.¹ The sheer number of users coupled with what some have viewed as lackadaisical privacy protections have made Facebook stalking an oft-seen form of cyberstalking.

  A common form of cyberstalking on Facebook is the use of so-called “clone accounts,” fake accounts of real people made by another person, not the real person him- or herself. The most common procedure for stalking via clone account is as follows:

  - The stalker selects the name of someone connected to the target, creates a fake profile, and adds legitimate information about the person named, including pictures, occupation and other personal information gleaned from a brief internet search.

  - The stalker sends out friend requests to people that the clone account and the target have in common - again, determined by viewing the real profile being spoofed, or by an internet search, or by information known or gotten by offline means. The stalker can add a personal message to the friend request, an innocuous message explain the friend request.
Once enough common friends have accepted the friend request, the clone account sends a friend request to the target Facebook user. The profile looks authentic, and with upwards of 130 or more friends, it may often be hard to know who one has already friended and who might have been accidentally unfriended. Once the target accepts the request, the cyberstalker has access to every bit of information that the target has posted on Facebook.2

Twitter Stalking. Like Facebook, Twitter has experienced phenomenal growth. Begun in 2006, Twitter had over 245 million active registered users as of January 2014, making it one of the top ten most frequently visited websites on the Internet.3 In the first quarter of 2019, the number of monthly active U.S. Twitter users amounted to 68 million.4 The site allows users to write small messages of 140 characters or less (called “posts”) and share them with their “followers” (accounts that have elected to see the user’s posts). If an account is not following a specific user, that account will usually not be able to see the posts.

Cyberstalking a person on Twitter differs from cyberstalking someone on Facebook. While Facebook requires people to use a registered name (and relies on the idea that people will use their given names), Twitter allows for any username, and does not require that a given name or personal picture be associated with a Twitter account. Thus, finding a victim’s account may be somewhat difficult, especially if they do not connect the Twitter profile to any personal identifying information. However, if the user “follows” (selects to have tweets from a user automatically post on their account home page) a user or a group of users who do include personally identifying information, the cyberstalker may have somewhat more ease in determining which account is the victim’s account.

Further, as no personal identifying information need be used, Twitter users often have “followers” (the category of people who on who’s page updates from the followed person automatically appear) that they may not recognize, or have never met. As a user has no advance control over who may follow him or her (the user may block a follower after the fact) and receives no notice of a new follower, a cyberstalker may begin following the victim without the victim even knowing. Stalkers may be able to gain information as to the victim’s location, mood, day-to-day habits, and other personal information with which they can then stalk and harass the victim, online or offline.

Instagram, Google, and LinkedIn Stalking

Like Facebook and Twitter, other social media outlets such as Instagram, Google, LinkedIn, and Tinder enable stalkers to track online by seeing where someone has been and with whom he or she is interacting.5 In March 2020, a California resident was
sentenced to more than five years in prison for cyberstalking families of the victims of the 2018 shooting at Marjory Stoneman Douglas High School in Parkland, Florida. Evidence at trial showed that between December 2018 and January 2019, the twenty-two-year-old stalker used several Instagram accounts to threaten and harass families of the victims. In some messages he impersonated shooting defendant, Nikolas Cruz.

Foursquare Stalking.

Foursquare, launched in 2009, is a location-based social networking. As with other online services, a stalker can spoof a friend account to gain access to the victim’s profile. The Foursquare model of business was a fairly popular one; as of the end of 2013, Foursquare boasted approximately forty-five million registered users, however following a split into two apps, the future of Foursquare is in question. Even its founder, Dennis Crowley, wonders if its new phone-tracking feature, Hypertrending, is “creepy” or not.

Cross-Service Cyberstalking. It is not enough that stalkers can access each of these web services separately. To increase visibility, ad revenue, and web presence, the web services discussed above can be interconnected. A user of Facebook and Foursquare can choose to have Foursquare auto post to Facebook whenever the user checks in to a location on Foursquare. Twitter, Foursquare, and Facebook have become so interconnected that a stalker may not need to actually friend the victim on more than one service to gain access to enough information to make the victim’s life very unpleasant.

• Stalking Via Devices That Control the Home

The recent popularity of digitally-controlled devices installed in homes has a downside—the devices may open the door to victims of domestic violence being controlled remotely by their abusers. Often marketed for their convenience, doorbells, locks, thermostats, cameras, and other devices are now being used as means for “harassment, monitoring, revenge, and control.” Although these devices are often touted as making a person feel safer in their home environment, in reality, the opposite may be true. Abusers can use apps on their smart phones to connect electronically to these home devices and control them remotely. Even after a partner or abuser leaves a home, he or she can still control the devices to “intimidate and confuse” the person remaining in the home. This type of electronic stalking has become more prevalent lately according to those working with victims of domestic abuse. The disabling of a home device by the victim can also have dire consequences as it may cause or escalate a conflict with the abuser and isolate the victim.

Recognizing the dangers inherent within this type of electronic stalking, the Florida Legislature enacted § 784.048(1)(d), which defines cyberstalking as accessing, or attempting to access, the online accounts or Internet-connected home electronic systems of another person without that person’s permission, causing substantial emotional distress to that person and serving no legitimate purpose.
- **Geo-tagged Photos.**

  Almost every picture-taking device available on the market is equipped with the ability to save the location at which a given picture was taken. This feature is often referred to as “geo-tagging.”

  The mechanism is relatively uncomplicated. All current cellphones, as well as the vast majority of smart cameras and video cameras, come with a built-in global positioning system (GPS) device. When a photograph is taken, the camera (or cell phone) automatically retrieves the GPS coordinates where the photo was taken. The software then writes the GPS coordinates into the code that creates the picture.

  Whenever the photo is copied and shared or displayed, that background code, along with the GPS data, is automatically copied and shared as well.

  This geo-tagging feature is turned on by default; thus, an unsuspecting user could be broadcasting GPS coordinates without his or her knowledge. The good news is that this geo-tagging feature can be turned off. Each device has its own process, which can make turning off the geo-tag feature tricky, but there are numerous websites that can assist users in navigating through the process for their particular device.

- **Cellphone “Bugging”**

  While cellphones have made communication easy and virtually instantaneous, they have also opened up the door to a variety of abuses. In particular, they make “bugging,” or covertly listening in on the victim’s conversations, remarkably easy and virtually undetectable unless the victim knows what to look for. Although popular cellphone spyware program “StealthGenie” was discontinued when its CEO was arrested in 2014 for conspiring to “market and sell a surreptitious wiretapping device”, other programs, such as Highster Mobile http://www.highstermobi.com/, and Hoverwatch http://www.hoverspyapp.com/, are apps that remotely control a phone, enabling a stalker to record conversations, view texts, and turn on the phone’s microphone. Some programs, such as Highster Mobile, tout their ability to “Safely monitor your children, employees and loved ones with the top cell phone monitoring solution!” (See http://www.highstermobi.com/).

- **Cellphone and GPS Tracking**

  In addition to bugging, cellphones can serve as location tracking devices, broadcasting GPS coordinates of the victim in real time to a watchful abuser. Numerous programs allow a user to be made aware of the location of another user’s phone; some of these programs are offered by the cell service providers themselves.

  Further, this GPS tracking isn’t limited to cellphones. Stand-alone GPS devices have become compact, light-weight, and ultra-portable. Although they are designed with concerned parents in mind, the technology can easily be abused by a stalker intent on
tracking his or her victim. The size and weight of these devices makes detection by the victim virtually impossible, and they appear to be designed to have a very long lifespan. An unsuspecting victim could carry around such a device for months - even years - without having any knowledge of its existence, during which time the abuser could know in real-time, any time, exactly where the victim is located.

- **Cellphone and Bluetooth Hacking**

The use of the Bluetooth mechanism on a cellphone is a useful tool, especially when one is connecting to peripheral devices (Fitbit, car communication equipment, etc.). When the phone has Bluetooth capability turned on, the default setting for this mode is “discoverable.” If the phone is “discoverable, and is not currently “paired” with a peripheral device, certain web applications can allow intruders to “discover” the vulnerable phone and connect to it, enabling the intruder to: remotely control the vulnerable phone; intercept or reroute communication; send and read text messages; and/or place or monitor phone calls. All of these actions can be taken without the intruder leaving any sign of his or her actions.

- **Telephone ID Spoofing**

Spoofing is an older technique which has been modified to be able to do a number of different things. The most basic of these is where the Caller ID spoofing service simply fails to provide an identity, transmitting an “ID unavailable” notice to the victim’s cellphone. More advanced caller ID spoofing services allow a caller to specify what name and telephone number he or she would like to appear on the recipient’s caller ID so that the victim may believe he or she is getting a call from someone he or she trusts, when in fact it is the abuser. The victim has no way of knowing in advance that the ID is spoofed.

As long as a victim relies on his or her cellphone to keep him or her connected to friends and family, he or she is vulnerable to caller ID spoofing. The stalker can use the spoofing services to turn the phone from a safety item into an avenue for abuse.

---

**CRAFTING COURT ORDERS**

In addition to learning about these forms of technological abuse, the court can provide specific protections to petitioners who have evidence of such abuse. By crafting specific orders tailored to the situation at hand, the court can ensure that the abuse does not continue.

In each of the final protection orders, there is a space provided for additional provisions “necessary to protect the Petitioner from domestic violence.” It is here that the court can specify what forms of technology cannot be used and/or in what manner they can or cannot be used. The court can use such language as the following:
• Respondent may not personally or through a third party use, access, purchase, or otherwise engage the services of any Caller ID spoofing service or spyware.

• Respondent shall not contact or cause a third party to contact Petitioner via Facebook, Twitter, Instagram, or any other social media platform.

• Respondent shall not install, use, disable, or control any digitally-controlled device intended for use at or in petitioner’s home, including, but not limited to, thermostats, locks, doorbells, speakers, lights, or cameras.

The above are suggestions only; courts are encouraged to stay abreast of technological developments and to use their own language to address situations where technological abuse is present. By crafting narrowly tailored orders, the court can exercise greater control to protect Petitioner from further harm and hold Respondent accountable for any future attempts to engage in technological abuse.

REFERENCES AND RESOURCES


