DEFINITIONS

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

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

- **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).

- **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).

- **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, causing substantial emotional distress to that person and serving no legitimate purpose. § 784.048(1)(d).

COMMON METHODS OF ELECTRONIC STALKING

The methods for stalking via electronic means are increasing exponentially. As such, this list of common methods of electronic stalking should not be taken as a complete list; rather this list covers 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 more uncommon methods of electronic stalking is not overlooked.
Social Media Stalking

**Facebook Stalking.** As of the end of the calendar year 2012, the social media site Facebook has over one billion registered users.\(^6\) Further, the average Facebook user has 130 friends, and is a member of 80 groups.\(^7\) When you add to that the fact that Facebook no longer allows users to hide their profiles from public searches by name,\(^8\) it’s no surprise that Facebook stalking is fast becoming an often-seen form of cyberstalking.

One of the more common forms 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.\(^9\)

**Twitter Stalking.** Twitter, a so-called “micro-blogging” website, was started in 2006, and as of January 2014 is one of the top ten most frequently visited websites on the Internet.\(^10\) In fact, there are over 645 million active registered users, who together produce a combined total of over 58 million “tweets” (as postings on Twitter are

---


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 is both easier and more difficult than cyberstalking someone on Facebook, depending upon the situation. 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. And 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.

Foursquare Stalking. The web service Foursquare bills itself as a location-based social networking site. The concept is fairly simple; a Foursquare user may “check in” whenever he or she goes somewhere. Each check-in gains the user points at that location. The user with the most points for a given location during a given time period is given the title of “Mayor of” that location, a title that can be displayed on the user’s profile and in the user’s check-ins. The Foursquare model of business is a fairly popular one; as of the end of 2013, Foursquare boasts approximately forty-five million registered users.7

As with other online services, a stalker may spoof a friend account to gain access to the victim’s profile. As Foursquare requires and displays a complete name for each user, a stalker will have an easier time finding his or her victim than if the users were not required to display their complete names. Once the stalker has gained access, he or she may select Foursquare’s “always on” feature, which means he or she receives automatic notifications every time the victim checks in at any location. Further, if the victim is a frequent patron of a location, the stalker may be able to access that frequency information, especially if the victim becomes “mayor” of a location. And if

11 Id.

that weren’t enough, if the victim is a “mayor” of a given location, beyond giving the stalker information about where the victim frequents, the stalker may be able to wait at that location, knowing that the victim will very likely show up at that location again.

**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.

**Geo-tagged Photos**

Almost every picture-taking device available on the market today - from digital camera to cellphone - comes equipped as factory-standard 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 fairly simple, once the terms are unraveled. 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 by default turned on; 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.

There exist a number of software programs that act as cellphone spyware. An example of this is “Stealth Genie.”¹² This software, touted as the most powerful spyware program available, is very easy to install on a victim’s phone. With nothing more than two minutes of unfettered access to the phone, a stalker can download and install the application. Then, without any further physical contact with the phone,
the stalker can use the application to do such things as record phone conversations, view texts, turn on the phone’s microphone and record the sound even if no call is in progress, and remotely control the phone, allowing the stalker to effectively block the victim from using the phone at all. This is just one of a number of programs that are commercially available to anyone, with no regard for intent or outcome. The cost of such a program? Stealth Genie, the example above, costs between eight and sixteen dollars per month, depending on the features desired.13

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. An example of such a service, Sprint’s Family Locator service,14 advertises that with the service one can, “see your loved ones’ location - instantly, any time.”15 While this may be comforting to a parent, an abuser may see this as a golden opportunity to track the victim’s location without the victim having any idea.

Further, this GPS tracking isn’t limited to cellphones. Standalone GPS devices have become compact, light-weight, and ultra-portable. Some are advertised as being smaller than a quarter.16 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.”17 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.18 Once connected, the intruder can:

- remotely control the vulnerable phone;

15 Id.
18 Id.
- intercept or reroute communication;
- send and read text messages; and / or
- place or monitor phone calls.¹⁹

All of these actions can be taken without the intruder leaving any sign of his or her actions.

**Keystroke Logging**

Keystroke logging is an older technique, but it’s one that’s being continually refined and tweaked, making it more and more difficult to detect. The basic concept behind keystroke logging is simple: the abuser uses a software program, or a device that he or she connects to the computer, to record every key that the victim types. This record is transmitted to the abuser, so that the abuser can learn the victim’s passwords, commonly visited websites, and other computer-based habits. In only a few minutes of unobserved time with the victim’s computer, the abuser can install the program or device. Once installation is complete, the abuser may never need to physically access the computer again.

These services - device or software - range in price from as low as twenty dollars to as much as several hundred dollars, depending on various factors, but all are available commercially on the internet. And all of them are designed to blend in with the computer’s normal functions or hardware. The software options are written to operate in the computer background, making them just another part of the landscape and thus very difficult to identify unless the victim knows what to look for. The hardware options are similarly designed. As they do not install any software onto the computer, they are truly invisible from an internal process point of view. Thus, as with the software, the only way a victim can know the hardware is attached to their computer is to physically see it and recognize it for what it is. As a result, the hardware options are packaged in very small cases, often less than an inch in length, and match the general color patterns and shapes used by most computer companies.

**Telephone ID Spoofing**

The final technology to be discussed is another older technique, telephone ID spoofing. In the age of automatic caller ID on cellphones, ID spoofing 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. As such, the victim can believe he or she is getting a call from a trusted loved one, when in fact it is the abuser. The victim has no way of knowing in advance that the ID is spoofed. These services range in price, but most are inexpensive, charging less than a dollar per call.

As long as the victim has a cellphone and relies on it - trusts it to keep him or her connected to friends and family - the victim is vulnerable to caller ID spoofing. The abuser can use the spoofing services to turn the phone from a safety item into another avenue for abuse.

**CRAFTING COURT ORDERS**

In addition to knowing about these forms of technological abuse, the court can provide specific protections to victims who have evidence of such abuse. By crafting very specific orders tailored to the situation at hand, the court can ensure than 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.”\(^\text{20}\) 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:

- The Respondent may not personally or through a third party use, access, purchase, or otherwise engage the services of any Caller ID spoofing service.
- The Respondent shall not contact or cause a third party to contact Petitioner via Facebook, Twitter or any other social media platform.

The foregoing language is a suggestion only; courts are encouraged to develop their own standard language to address situations where technological abuse is present. By crafting narrowly tailored orders, the court can exercise greater control to protect the Petitioner from further harm and hold the Respondent accountable for any future attempts to engage in technological abuse.

\(^\text{20}\) See any of the final injunction order forms, Florida Family Law Forms 12.980 (d)(1), (d)(2), (l), (p), (s), and (v) (2013).

This project was supported by Grant No. LN967 awarded to the Florida Coalition Against Domestic Violence (FCADV) by the state administering office for the STOP Formula Grant Program. The opinions, findings, conclusions, and recommendations expressed in this publication/program/exhibition are those of the author(s) and do not necessarily reflect the views of the FCADV, the state or the U.S. Department of Justice, Office on Violence Against Women.