CELL PHONE LOCATION, PRIVACY AND INTIMATE PARTNER VIOLENCE

by Kaofeng Lee & Erica Olsen[*]

This article was published in Domestic Violence Report, August/September 2013, Vol. 18, No. 6.

"Can you hear me now?" is one of the taglines for Verizon Wireless. A more accurate statement should be: "Do you know where I am?" Almost everyone has a cell phone that reveals their location every minute of every day. In most cases, sharing one's location is benign and quite helpful. For example, for most users it is useful to get off a plane in a different time zone and have their phones automatically update to the current local time or to be able to pull up nearby restaurants along with reviews, menus, and directions when in a different city. It is even more useful when someone is in an accident or is lost, and the police can trace the person's location based on the cell phone signals.

Sharing one's location can be quite dangerous, however, when a stalker or abuser uses this information to stalk, harass, and threaten. For victims of domestic violence, assault or stalking, knowing how much information may be inadvertently shared about them is key to planning for privacy and safety. For service providers, there is often a concern that abusers may be able to track victims to the shelter or program. Some programs have questioned if the solution is to ban cell phones in shelter. In reality, however, this response will not eliminate the feared risk. Additionally, it is not feasible for survivors to give up their cell phones, which for many is a life line to safety, help, and support. The better solution is to understand how location gets shared, minimize the amount of information that is being shared, and help survivors take back control by creating thorough safety planning and changing privacy settings.

A person's location gets shared in many ways. This article will focus specifically on location sharing via cell phones. It is important to keep in mind, however, that location information also may be revealed when visiting social media sites or sending emails or through finding general personal information online (e.g., online people search engines, employee staff listing, etc.).[1]

Cell Phones & Location

Abusers and stalkers may misuse cell phones in various ways in order to access a victim's location. These ways may include misrepresenting the victim to the cell phone provider to gain information, using a location service on family plans with or without the victim's knowledge, installing cell phone spyware on the phone, monitoring phone activity through phone bills, or installing an app that provides location information about the victim's phone. Each of these tactics is described below. As victim advocates, in order to help survivors with safety planning strategies, it is critical to understand the different ways an abuser can monitor a survivor's location through a cell phone.

---

[*] Kaofeng Lee is a Senior Technology Safety & Communication Specialist and Erica Olsen is a Senior Technology Safety & Housing Specialist, with the Safety Net Project at the National Network to End Domestic Violence, Washington, D.C. Ms. Lee can be reached at kl@nnedv.org and Erica Olsen can be reached at eo@nnedv.org.

[1] Additional information on these types of data sharing is available at NNEDV's Safety Net Project resources at www.nnedv.org/safetynetdocs.

Most cell phones can be tracked simply from the way the device is designed and operated. Even without actively using the GPS in the phone, simply by triangulating the cell towers—measuring the distance between the phone and the three nearest cell phone towers—the approximate location can be discovered. Wireless carrier companies also have other methods of determining a phone's location, including GPS information or network usage information that includes location (when connecting to Wi-Fi, for example). In general, the phone must be turned on and be connecting with cell towers in order for the carrier to gather location information. This information is typically only accessible to the wireless carrier and may be obtained by law enforcement with the proper warrants or authorization. This type of tracking makes it important to note if the batterer has access to wireless carrier accounts or could possibly obtain that information from the wireless carrier.

Most abusers and stalkers will typically misuse the GPS in the victim's phone in order to track and monitor them. One of the most comprehensive ways a stalker can track a victim is by installing a tracking program or spyware onto the victim's cell phone. In most cases the abuser will need *physical access* to the phone in order to install a monitoring program.[2] This can occur if the abuser or an accomplice of the abuser has access to the phone or if the survivor inadvertently installs such a program without knowing what it does.

Location Tracking Applications

Some location tracking services come in the form of family locator applications (apps) that can be downloaded onto smartphones. Most wireless carriers have their own family locator apps and can be installed by the wireless carrier, although users can also download family locator apps through app stores and the Internet. The focus of most family locator apps is for parents to keep track of their children via cell phones. Many of these apps have additional features beyond disclosure of the location of the cell phone. Some features allow the monitoring person (potentially, the abuser) to be notified if the targeted person goes outside of a certain geographic boundary (known as "geofencing"), be notified if the targeted person goes to a certain place or address, be sent notifications of a targeted person's location at specific times, or see a history of where the targeted person has gone throughout the day or week.

In general, users will know that a family locator type application is running on their phone by going through the applications on their phone or by contacting their wireless carrier. Some of the major wireless carriers may even send periodic text messages or updates to let the user know that a location app is running on their phone. Depending on the phone, it is possible for the abuser to change the name of the application, calling it something innocuous so the user doesn't know that a location app is on their phone. Victim advocates should encourage survivors to look at all the apps that are running on their phones.

There are also location apps that are marketed specifically for spying on someone else. These location apps may run undetected, without the user's knowledge. Some of these programs are known as cell phone spyware. Cellphone spyware shares all activities that occur on the phone with the monitoring

[2] The exception to this general rule is if the location tracking application is installed by the wireless carrier. Applications that are provided through the wireless carrier can be added by an account holder. If the victim's phone is part of a family plan or the phone's account holder is the abuser, it is easy for the account holder to add this location feature onto the victim's phone.

person (potentially, the abuser), including all messages sent and received, apps downloaded, phone calls, voicemail received, and location information. Some spyware will even allow the monitoring person to call the phone and, without the user realizing, use the cell phone as a listening device to hear conversations occurring around the user. Unlike some family locating programs, the location feature on spyware can operate without sending any notifications to the user.

Survivors often suspect that spyware is on their phones when the abusive person hints that he or she knows about conversations, messages, or activities that occur when the survivor is using the phone. Other clues that spyware is on the cell phone is if the phone has excessive battery drain or increases in data usage. In most cases, spyware needs to be manually installed onto the phone, so if the abusive person has had no access to the phone or the survivor has not installed anything onto the phone without knowing what it was, the monitoring and stalking might still occur but it would be done by using other methods.

To remove locating programs, whether it is a family locator plan or spyware, the first step is to identify what program is installed on the phone. The survivor can scroll through the phone to see if there are any apps or programs that are operating without his or her knowledge. If apps are running on the phone that the survivor does not know the purpose of or the reason why it is on the phone, the survivor can consider deleting that app and not having it on the phone. If it is a family locator plan that is provided through the wireless carrier, the survivor can contact the wireless carrier and ask for it to be removed. Note that only the primary account holder may be able to make these changes. If the survivor is not a primary account holder for the phone, then she/he may want to get a new cell phone (with a new account or a new wireless carrier). In some cases, if the abuser is alerted that the survivor knows the phone is being tracked, this may escalate the danger. If this is a concern for the survivor, then an option may be to figure out how to continue using the phone but in a way that minimizes the information that is being shared to the abuser.

Social Location Apps

In addition to programs that are installed for the sole purpose of monitoring location, social location apps, such as FourSquare, Facebook, Sonar, or Grindr, allow users to share their location with either a group of friends or for the purpose of meeting new friends. Sometimes it may not be the survivor who uses these apps but the survivor's children or family members. An additional danger occurs because abusers often will monitor the social locations apps of family members or friends of victims, especially if the abuser cannot monitor the survivor through the survivor's technology.

Some social location apps have privacy settings that limit who can see what, while some are meant to be completely public. Survivors and their family and friends should review the privacy settings of the app to determine who might be able to see what they share. Since the purpose of social media is to connect, even if an account is completely locked down, it may still be possible that the abuser can access that information through a mutual friend, perhaps because of the way the social network is set up,[3] or the mutual friend may forward the information to the abuser. Also the survivor should keep in mind that

[3] An example of this is Facebook's friends of friends' privacy setting that allows friends of friends to see what the user posts. To ensure that only the user's friends see what the user shares, it is important for the user to select "friends" as the privacy option.

social media accounts may be searchable via online searches such as Google or Bing, which may make it relatively easy for someone to Google the name of a survivor and find her/his social media account and the information that she/he shares, possibly including location.

With all the ways in which location information can be shared, whether purposefully or inadvertently, the first instincts of many survivors may be to get rid of their cell phones. However, survivors should keep in mind that in many cases it is the programs and applications on the phone that is using the phone's GPS capability to reveal the location of the user. The more feasible solution is to determine what application is being used and get rid of that application or maximize the privacy settings to reduce or eliminate risk. Privacy settings in the phone itself (through general privacy settings) and in the individual app (through settings within the app) may offer options to make the app safer to use without evoking a concern for location information being shared. In cases where the survivor has no control over her or his cell phone and the abuser constantly has access to it, then it might make more sense to get a new cell phone that the abuser will not know about or not have access to.

Safety Tips

Safety Tip #1

Safety first. While it may be tempting to get rid of a compromised cell phone immediately, the survivor should think about the abuser's potential behavior. In many cases, when control is taken away, abusive individuals escalate their dangerous behavior. If they cannot monitor or contact the survivor easily, they may try to find them in person. The survivor should trust her/his instincts about what the abuser may do. If removing the tracking app may be more dangerous, it is important to develop a safety plan regarding how to continue using the phone so that the abuser does not become suspicious, and the survivor should simultaneously create a plan concerning how to communicate with others and move about safely until the program can be removed completely.

Safety Tip #2

Keep a log. Knowing the pattern of the abusive person's behavior and what information they know can help the survivor narrow down how the abuser is getting his or her information. Abusers are creative and can find many ways to monitor and stalk a victim, often using more than one technology or method. For example, if the abusive person seems to know where the victim is only when she is with certain friends, but not everywhere she goes, then perhaps the abuser is tracking the location of the friends. If the abusive person seems to only know location but no other information, then it may be a location program. If the abusive person seems to know everything, including phone conversations and the content of text messages, then it may be spyware. Another option is to consider leaving the cell phone at home for a day or two to determine if the abuser's knowledge is coming from the cell phone or another source.

Safety Tip #3

Use security settings. If the survivor is feeling secure that the cell phone is currently safe, the survivor can help keep it that way by ensuring that programs do not get installed on the cell phone without his/her knowledge. The survivor can put a lock code on the phone. It important for victim advocates to discuss with survivors the need to be cautious when installing anything on the phone.

Survivors should be careful not to install programs that are unknown, especially if the suggested app is from the abuser or mutual friends. Survivors should also make sure that family and friends do not download apps onto their phone without knowing about it or knowing what the app does. Additionally, smart phones are mini-computers and should be protected from viruses and malware in the same way, so survivors should install and run mobile anti-spyware/malware software.

Safety Tip #4

Use privacy settings. If a location program is already on the phone, the user should learn about its settings and features.[4] Some apps allow the user to choose when to share location, while other apps will automatically pull the location from the phone's GPS. Many of these apps have different features and privacy settings. Knowing what controls are available may allow the survivor to continue using the service while maintaining privacy and control. For example, some programs may allow the user to set a static or fake location, so the survivor can set the location to someone else's house while visiting with a victim advocate.

Safety Tip #5

For short periods of time, a survivor can cut off communication from the phone by putting the phone on airplane mode or turning the phone off and taking out the battery. While the phone is off, the survivor's whereabouts will not be communicated via the phone. However, the survivor should be aware that when the phone is turned back on, all communications will continue and location information may be shared again. If the tracking program cannot be removed, the safest step is for the survivor to get a new cell phone.

Safety Tip #6

When getting a new cell phone, the user should not import everything from the old phone to the new one. Some wireless carriers will offer to copy over everything from the old phone to the new phone for convenience. Porting over all the data may inadvertently install the tracking application as well. The user should re-download apps, change passwords to accounts, manually input contacts, and double check all privacy and location settings.

Other Apps that Require Location

In addition to applications whose purpose is to track location, many applications simply require location information in order to function. Apps that help users find their way around, such as maps or bus apps; find nearby deals, restaurants or stores, such as Yelp or Groupon; and a variety of other apps, including camera, bank, and weather apps—all require or ask for location in order to deliver location-specific information or to measure who is using their services and where.

When using these apps, it is important for survivors to know if their location are shared or stored in a way that might be discoverable by others. Camera apps, for example, are of particular concern for survivors because if the location setting is turned on for the app, precise location information could be

[4] When doing research on monitoring software, research should be done from a safe device. If a cell phone or computer is being monitored, doing research on how to remove monitoring software may tip off the abusive person that the survivor knows that s/he is being monitored and is trying to remove the abuser's control.

stored in the picture's metadata (the data that is attached to the picture electronic file). When that picture is posted online, it may be possible for someone to extract the metadata from that picture and learn the exact location of where that picture was taken.

Apps that allow users to sign into an account may also store location data and other usage activities. For example, Facebook and Gmail stores general location and Internet Protocol (IP) information every time anyone accesses her or his Facebook or Gmail account (whether from a computer or a phone). If an abuser has access to a survivor's account, the abuser may be able to access location information by logging into the account.[5]

The Future of Location: Next Steps for Safety

Survivors can enhance their privacy by being vigilant about what applications are on their phones and how much information is being collected and stored by the third party offering the app. Victim advocates should be aware of these issues as well, so they can engage in safety planning and properly advise survivors on how to strategize for their safety. Companies and policy makers can help survivors stay safe by ensuring that users are aware of and educated about the types of information that is being collected, how it can be shared, and to whom it is shared. This knowledge is critical for survivors in making informed decisions in determining their safety and managing the abuser's abuse and control.

Consent and notice are crucial pieces in ensuring privacy and safety. Users, especially survivors, should be allowed to decline (opt-out of) their location being monitored, tracked, and shared by companies. Location monitoring apps should send periodic notices or a setting should exist in the application that provides clear notice that location information is being collected. Knowledge and information will give power and control back to the survivor. For more information on best practices around location-based services, look at the Wireless Association's (CTIA) *Best Practices and Guidelines for Location Based Services*.[6]

In December 2012, Senator Al Franken (D-Minn) introduced in Congress the Location Privacy Protection Act of 2012 (S. 1223) that would require companies to obtain consumers' consent before the companies start collecting location information and also would ban applications that secretly monitor a user's location.[7] Currently, the only way that survivors and advocates can manage their location being tracked and used against them is to try to stay one step ahead of the abuser, use a combination of guesses and instincts to figure out how the stalker is stalking the victim, and learn as much as the user can about the various ways technology can be used to track someone. Establishing laws that give more control of personal location to individual users, ensuring that apps whose sole purpose is to monitor and stalk someone is illegal, and encouraging companies to provide more notice and transparency for their users will go a long way toward ensuring that survivors can stay safer and in more control of their own information.

---

[5] It will also record the time, date and IP address of the abuser when he or she logs into those account.
[6] CTIA. *Best Practices and Guidelines for Location Based Service.* Volume 2.0. March 23, 2010. Available at: http://files.ctia.org/pdf/CTIA_LBS_Best_Practices_Adopted_03_10.pdf
[7] http://www.govtrack.us/congress/bills/112/s1223