EVIDENCE COLLECTION
In Stalking Cases

By Detective Rande Christiansen

[WCSAP: Related to the previous article, Det. Christiansen shares a law enforcement perspective on the collection and preservation of evidence in stalking cases that include technology. Some of these guidelines will also apply to similar cases of harassment. As he points out in this article, stalking cases are so varied and complex, that it is crucial for advocates to share with survivors information about evidence collection for a possible criminal case, and to support them in making crucial decisions about their safety.]

"EVIDENCE COLLECTION" IS A TERM usually reserved for law enforcement and most training on this topic is devoted to them. We need to understand that cases that involve obtaining and collecting technological evidence also involve the victim and advocates. Many times victims being stalked are not terrorized by just the old fashioned ways of following and surveillance, but now also with technology. This can vary from emails, text messages, instant messages, and using various Internet sites (i.e. MySpace, Facebook, etc.) to monitor the victim. We need to advise victims correctly for both evidence collection and safety, with technology being so prevalent.

Cell phones in urban and now in rural areas are common. Many households now use the cell phone as the primary line opposed to a hard-wired line. Victims carry their phones "everywhere" they go, and can now be monitored by various means. Cell phones can be monitored or tracked with GPS, Bluetooth, or other functions now available on the phones. If a victim believes this is happening, they should consider turning off certain functions on the phone. If possible and economical, victims should discontinue use of that phone and get a new service through another carrier with security access only by the victim.

While doing instruction of investigation of stalking cases, one of my main points is not to have the victim change their phone number. In years past, the advice was to have victims change their number and the stalker would just move on. The advice that I now give incorporates both evidence collection and safety. Changing their number can be problematic in that the number probably will be released or found on the Internet. The "evidence" in the form of text and voice messages will be lost in most cases if the victim changes the phone number. The major safety reason for not changing the number is that once the number becomes "unpublished" or not available to the stalker, there is a high probability that the stalker will try to find the victim in person to give his/her message.

Text messages have an extremely short retention period with the service providers, so that even law enforcement may not be able to collect them for evidence in time. Victims should be instructed that the messages need to be downloaded by a forensic expert, or in most cases digitally photographed for preservation. Law enforcement should take these photos for proper chain of evidence, and so as not to put advocates in the position of a being called as a witness for the case. Most phones now seem to have large storage capability, but when maximum capacity is reached the older messages, both text and

voice, will be eliminated. Another point of retaining and recording text and voice messages will assist persons tasked with threat assessment to read and interpret possible future problems and actions of the stalker.

Previous research studies of stalking behavior used to show that following and surveillance were at the top of the list and the use of technology was low. I have found that working stalking cases now, most, if not all, involve the use of some type of technology harassment. Many of the cases that are presented to the street Officer did not mention any emails or similar harassment as part of the case. I have found that many victims need to be asked if they have received the unwanted technology contact as part of the harassment/stalking. Many don't mention this in the original report unless asked.

The primary report may list the stalking behavior to the effect, "He hacked into my MySpace account," as many of the victims are college age or young adults. It is a necessity nowadays to be familiar with the various Internet sites to include MySpace, Facebook, etc., when giving advice on either preservation of evidence or collection for prosecution.

One very good thing about technology is the response suspects give to victims telling them to "leave me alone." In almost all cases I have investigated, when the victim sends an email, text message, instant message or other electronic message to "leave me alone," the stalker will usually respond. Saving and preserving this response is imperative for victims to show that the suspect was told the contact is unwanted, but also starts a time line in investigations for stalking if it continues. This also involves a protective factor, in that the victim doesn't have to see the stalker in person to deliver the message.

Service providers and technology experts advise victims to delete any unknown or unsolicited email. This is extremely valuable advice except in stalking cases. Listen to the victims in these cases, and when they receive a "strange," unsolicited, or masked email they believe is from the stalker, they are probably right. Then comes the double-edged sword advice of "to open or not to open." Opening one of the emails may give rise to the possibility of infecting their computer with viruses or other infections.

Opening one of these emails may also be the route by which a stalker infects the victim's computer with a type of spyware without their knowledge. The information presented here is not a secret and has widespread usage to track victims. The problem is that if victims use a type of spyware detection software, it will generally find, quarantine, and wipe out any of the "evidence" needed for proof of where the information is being sent. The actual analysis should be completed by a computer expert that can collect, document, and testify on the information located, if a victim believes that their computer is infected with spyware. The problem is in finding someone to do the analysis, since most law enforcement departments may have limited or no services to complete the analysis. The criteria for accepting a computer for this analysis will require more than, "he hacked into my MySpace account."

◀It is a necessity nowadays to be familiar with the various Internet sites to include MySpace, Facebook, etc., when giving advice on either preservation of evidence or collection for prosecution.

As a law enforcement investigator I think the one thing that I would work to take away is the "DELETE" button. In hundreds of cases I have heard the victim state to the effect, "I just couldn't listen to his voice anymore," or "I just couldn't take one more text", so she deleted the "evidence." We need to understand that victims hitting the "DELETE" button is a coping mechanism, and assist in educating victims that not using the button may increase their survival or get the stalking to stop.

Technology is here to stay, and it is imperative that as either advocates or law enforcement giving victim safety information, we must have basic understandings of the function and preservation of evidence. Armed with the basic information and resources, this will empower victims to gain back their sense of normalcy in these cases where technology has invaded their lives. +

Detective Christiansen has been with the Seattle Police Department for 19 years. He has been a Detective in the Domestic Violence Unit for 13 years, with majority of cases involving harassment and stalking.