LAW OFFICE SAFETY

Recommendations for Creating& Maintaining a Safe Work Environment

Domestic Violence Advocacy Project and Pro Bono Program
Committee on Law Office Safety
2010

Table of Contents

Introduction

For clients seeking divorce and/or parenting plans where domestic abuse is a dynamic within the relationship this may be a highly lethal time. Domestic violence spills into all aspects of life for victims/survivors, but it is a particularly dangerous time when a battered partner attempts to leave the abuser.

This booklet has been developed as a guide to develop a safety plan for the law office. It is critical that law office managers implement policies not just to reduce risk but to reduce the conditions that cause risk. No two offices are alike therefore you should assess your own needs and adapt a plan that is right for you.

This booklet was developed by a sub-committee of the Domestic Violence Advisory Council. The Council coordinates and oversees the work of the Domestic Violence Advocacy Project (DVAP), a collaborative that includes New Hampshire Legal Assistance (NHLA), New Hampshire Bar Association's Pro Bono and Domestic Violence Emergency Project (DOVE) Programs, Legal Advice & Referral Center (LARC), and New Hampshire Coalition Against Domestic and Sexual Violence (NHCADSV). The mission of the Domestic Violence Advocacy Project is to provide access to high quality civil legal services for low-income victims of domestic violence in New Hampshire.

This project was supported by grant 2005-WL-AX-0090 *awarded by Office on Violence Against Women, U.S. Department of Justice. 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 Department of Justice, Office on Violence Against Women.*

Domestic Violence Advocacy Project and
Pro Bono Program
Committee on Law Office Safety

Ms. Chantell B. Wheeler, Chair
Pro Bono Referral Program
2 Pillsbury Street, Suite 300
Concord, NH 03301
cwheeler@nhbar.org

Attorney Joseph Caulfield
Law Office of Joseph Caulfield
23 Factory Street Suite 2
Nashua, NH 03060
josephcaulfield@josephcaulfield.com

Attorney Sunniva Mulligan
Stephen A. Cherry & Associates PLLC
1 Maple Street, PO Box 951
Henniker, NH 03242-0951
smulligan@piercelaw.edu

Attorney Valerie Reed
Wiggin & Nourie PA
670 N. Commercial St., Ste. 305
Manchester, NH 03105
vreed@wiggin-nourie.com

Attorney May Krueger
New Hampshire Legal Assistance
24 Opera House Square, suite 206
Claremnt, NH 03743
mkrueger@nhla.org

Mr. Craig Sander
Bar News Associate Editor
2 Pillsbury Street, Suite 300
Concord, NH 03301
csander@nhbar.org

Ms. Kate Geraci
Law Student
Pierce Law
kgeraci@piercelaw.edu

Mr. Adrian LaRochelle
Law Student
Pierce Law
alarochelle@piercelaw.edu

Securing Your Electronic Information

By Adrian LaRochelle

Generally, there are two types of electronic data that must be secured. The first is what could be termed communication data. Communication data consists of information that is transmitted to another computer either by e-mail or other internet communication. The second is what could be termed access data. Access data consists of the information stored locally on a computer in your office or your home. In order to secure each form, there are some general techniques that, when employed, will help to protect each type of data from any person who does not have authorized access to it.

The following recommendations apply to large and small firms alike. There are many ways to protect your data and research will help determine the approach that works best for your firm or office. The important thing to remember is that information of any value is worth protecting.

Communication Data

E-mail

Being one of the most common techniques for data transfer, e-mail is one of the easiest forms of electronic communication to protect. There are several ways in which to secure your e-mail communication. Generally, it is helpful in all forms of electronic communication, if the material is sensitive, to refrain from giving anyone other than the intended recipient any information as to the content of the communication. This means that the e-mail should be structured in such a way as not to give a casual onlooker any sensitive information. There are two ways in which to accomplish this.

1. Never put sensitive information in the subject line. This includes the names of parties involved and any summary of the e-mails content. This will prevent people from obtaining any information and deter them from reading any further.

2. Try to refrain from sending e-mails to large groups of people. This will limit the risk of a non-privileged person intercepting the e-mail and will force the members of your firm or office to take care in considering who will be receiving the sensitive information being sent.

The recipient also has some responsibility in securing the information you have sent. The longer e-mails remain in a user's inbox, the more likely it is that the information may be accessed by someone else. The best way to prevent this is to tell the recipient to save the e-mail as a file or to copy and paste the content of the e-mail into another document for safe storage. The recipient should then delete the e-mail from their inbox. This will make it more difficult for others to access the e-mail once it has reached the recipient.

Ultimately, one of the best ways to protect your e-mail communication is through the use of e-mail encryption. Cryptographic systems for protecting communications from eavesdroppers are surprisingly common. Software such as OpenPGP for e-mail, encrypted tunnel software for sustained communication using secure protocols such as SSH and SSL, and numerous other tools can be used to ensure that data is not compromised in transit. In person-to-person communications, of course, it can sometimes be difficult to convince the other participant to use encryption software to protect these communications. However, this protection is often of critical importance. Talk to your clients or coworkers and see if encryption is something your firm or office may want to implement.

Internet Traffic

The internet is a great tool but can also carry with it some serious security concerns. Any record of one's use of the internet may indicate more than simply their interests. A record of an individual's web traffic may also lead to the exposure of vital information about that person as well as other individuals with which that person has had contact. There are a few general rules regarding internet usage that will help keep your information and that of your client private.

1. Make sure your browser erases private data automatically. Each web browser has the capability to erase stored information including browsing history, saved passwords, and information from any completed online forms. Setting your browser to erase this information automatically will

keep a subsequent user of the same computer from viewing or using this information without your consent.

2. Do not post personal information on the internet. Any information you place on the internet, however secure it may appear, is potentially available to the public. Personal information includes your name, e-mail address, date of birth, place of employment, etc. As a general rule, do not make your personal information readily available on the internet.

3. When signing up for online services, it is best to limit the use of your work e-mail address. As honorable as many companies are, your work e-mail address should not be available for distribution or use by any other company.

Ultimately, it is important to be aware of any information about you on the internet and about any potential use of that information by others. Stay up to date and make sure you and your co-workers are cautious about internet usage and about how that usage might relinquish or allow access to sensitive information.

Access Data

With the evolution of computer usability and storage space, people have become accustomed to storing all of their electronic information in one place for easy access. The storage of files on a desktop computer is often referred to as local storage. Although convenient, this approach is not necessarily secure, because with a single password someone can use or destroy all of your personal and/or vital information. There are several ways in which to secure computers in your firm or office to help prevent unauthorized access or, in the worst case, destruction of data.

Password Protection

Make sure every computer in your firm or office has a password. This is the first line of defense in terms of protecting your electronic data. Later in this chapter, we will discuss effective password creation, but for now, each local computer must be password protected. The best way to do this is to create unique passwords for each computer and to inform only those who frequently access these computers of the necessary passwords.

Also, change these passwords often. Every six to twelve months is usually sufficient, but they must be changed. In addition, if there is ever a breach of security, the passwords should be changed immediately. Although inconvenient, changing you passwords will prevent unauthorized users from obtaining a password giving them unlimited access to your sensitive information.

External Storage

For information that is extremely sensitive, it is often a good idea to store that information separately from the rest of your electronic data. The best way to do this is with a local server. However, not every law firm or office will have this capability. Alternatively, the use of encrypted external hard drives would be sufficient. The access to these external hard drives can be structured in whatever way makes sense to you and your firm or office. Each person can have their own drive with their own password, or there can be several drives that are used every day or week for systematic file backup of sensitive materials. After the files have been stored on these drives, the drives should be stored in a safe place with limited access. That way, your files are not stored locally, making them more difficult to access.

Backup Your Data

It is always a good idea to create a backup of your local files on a regular basis. As in the previous section, this can be accomplished using external drives, servers, or tape systems. Ultimately, every week or so, all local computers should have their data backed up onto an external drive to prevent data loss in the case of a power outage or hardware malfunction.

Use Anti-virus and Malware Protection Software

Unfortunately, there is no particular way to identify that your computer has been infected with malicious code. Some infections may completely destroy files and shut down your computer, while others may only subtly affect your computer's normal operations. Be aware of any unusual or unexpected behaviors. Running anti-virus and malware protection software is helpful because it will often alert you that malicious code has been found on your computer. The anti-virus and malware

protection software may be able to clean or remove the malicious code automatically. There are many packages available. Some anti-virus and malware protection software packages are free, while others may require a yearly subscription fee. Choose whichever option works best for your firm or office and make sure to keep your anti-virus and malware protection software up to date. Software updates are discussed in depth later in this chapter.

Hidden File Data

With the evolution of computer software comes the ability to create and manipulate documents in new ways. Simultaneously, programs have been designed to do more of the work for you. This means that programs now include "metadata" when they create or alter documents. "Metadata" includes information such as proofing comments, personal information about the creator, and so on. This information is often useful during the revision process but can be dangerous if left untouched upon completion of a document.

It is important to remember that "metadata" exists and to learn how to erase it. Microsoft Office is the most common creator of "metadata." Now, however, it is easier than ever to find and erase "metadata" from documents created using Microsoft Office. In Microsoft Office 2007, all a user must do is click on the Microsoft Office button, choose Prepare, and select Inspect Document. The program will then inspect the document and will allow the user to erase whatever "metadata" they choose before saving the document. However, be careful when erasing "metadata" because the information you are erasing may still be necessary for further revision.

General Tips

Whenever dealing with computer security there are several simple things a user can do to secure data and to protect their personal information and that of their clients.

Use Strong Passwords

One of the simplest ways to improve security is to use a password that is not easily guessed by brute force attacks. A brute force attack is one where the attacker

uses an automated system to guess passwords as quickly as possible. Passwords that use numbers, include special characters and spaces, use both capital and lowercase letters, and avoid words in the dictionary are much more difficult to crack than your mother's maiden name or your birth date. It is also important to remember that by adding just one character to the length of your password, you significantly increase the total number of possibilities that must be tried during a brute force attack. In general, anything less than eight characters is considered far too easy to crack. A password with ten, 12, or even 16 characters is preferred. Just make sure your password is not too long to remember or too difficult to type.

A Good Perimeter Defense Is Priceless

Not all security occurs on the desktop. It is a good idea to use an external firewall or router to help protect your computer. Retail routers can be purchased at many common electronics stores, and for a lower price will provide sufficient protection for some offices. Although more expensive, firms and offices can get managed switches, routers, and firewalls from "Enterprise" class vendors such as Cisco Systems, which provide an even greater level of protection. Remember that, in general, routers allow for the highest level of security, and firewalls are a necessity.

Keep Your Software Up To Date

For almost every contemporary computer program, the vendor must provide security patches or updates for your systems. Ignoring security updates for too long can result in the computer's increased vulnerability to unauthorized access. This is why it is important to keep your computers up to date. The same applies to any malware protection software and anti-virus applications (if your system needs them), which are only as effective as they are up to date.

Monitor Systems for Security Threats and Breaches.

Never assume that once a firm or office has completed a checklist of security preparations they have eliminated the possibility of unauthorized access. Firms and offices should always institute some kind of monitoring routine to ensure that suspicious activity becomes apparent quickly in order to afford the firm or office the opportunity to follow up on what may be serious security threats. This sort of

attention should not only be spent on network monitoring but also on other local system security monitoring techniques such as simply checking the logins and logouts of your local computers.

Securing the Property (Inner and Outer Office)

By Craig Sander

A key component of creating a comfortable workplace and an efficient staff is the establishment of an overall sense of security for employees, clients and office guests. Considering the nature of some areas of law practice, securing a law office can pose a larger challenge than other office environments. There are many ways to begin instilling a greater sense of security in every part of your office, from the parking lot and front office to the deeper recesses of the office facility.

Building Exterior

Regardless of the risk level of the office and practice in question, every employer should first look at the building exterior when completing an overhaul of security policies and should consider the variety of procedures and equipment that can be reasonably used to create a more secure first line of defense.

Parking Lot

The parking lot of your office is often the first point of contact a person has with your office, even if your building is only one of many units inside. Therefore, it is imperative that you take the proper steps to ensure a welcoming, but also safe and secure parking area. If you are not the owner of the building, you can speak with the owner about the following points of importance.

- Gated lots – The safest and most secure parking lots are those that are gated and monitored by security staff. If a gated lot is not a feasible option, consider hiring a part-time security person to patrol the lot. Companies such as Securitas can often provide a security person to randomly patrol your lot.

- Lighting – Lighting alone is known to be a significant deterrent to crime, so be sure that your parking lot is adequately lit. There should be enough lighting units to eliminate any dark shadows. Landscape and architectural lighting

should also be utilized. Aside from being attractive, these lights also provide an extra deterrent to would-be burglars.

- Security Cameras – Surveillance cameras serve double-duty in terms of protecting a building exterior: firstly, they are a deterrent in that thieves, aggressors and burglars are much less likely to commit a crime with an eye watching them from above; and secondly, they provide valuable evidence against a criminal unaffected by the deterrence factor.

- Buddy System – In buildings where lighting and surveillance cameras are unavailable – and even those where they are – the employees should utilize a buddy system, with which an employee would never enter or exit the building alone. A criminal is much less likely to target a couple or group.

- Electronic Locks – Every office, regardless of practice, should be utilizing the latest electronic entry systems, which require a key-card to enter the building. If such building-wide systems are unavailable, then the electronic locks should be installed at every interior entrance to the office, including fire exits, back stairway entrances and reception area entrances to the offices.

Building Interior

If the building exterior is adequately protected, then completing a security overhaul of the building interior will be much easier. There are two main building areas to consider when establishing a proper building security system: the reception area, and the office network in the center of the office environment.

Reception Area

The ideal office reception area is one that allows free movement of staff within the office network while limiting access to visitors to the office.

- Be Vigilant – The reception area of your office should never be left empty; from the moment the office is opened for the day until the moment the office is closed for the night, there should be someone always at the reception desk. This ensures

that all guests are greeted and that their business at the office is known. This not only adds another layer of security to your office, but also ensures that customers and clients are met with a human face every time they enter your office.

- Reception Desk/Counter – The ideal reception desk is not a desk, but rather a waist high counter that separates the reception area from the entrance to the interior office network. Having a “blockade” like a reception counter will often foil more aggressive visitor’s attempts to enter the interior offices. It will also provide an escape route for the receptionist should a visitor become violent. If this is not feasible, a large desk placed between the lobby area and the office entrance will accomplish a similar function.

- Electronic Locks – If possible, there should be electronic locks on all interior entrances to the office network. This includes locking the doors of the offices in the reception area, any other entrances to the office fire exits and other emergency doors. The locks can be programmed to work in unison with the exterior building locks to eliminate the need for multiple keys.

- Logbooks/Visitor Tags – Utilizing logbooks ensures that there are no unknown visitors wandering the halls of your building. Having every visitor sign in can also be helpful in

- Alarm Systems – The entire office should be protected by an alarm system. Systems vary in terms of cost and extensiveness, but all systems should include door and window sensors to detect unauthorized opening when the alarm is armed, a passkey code or turnkey to activate and deactivate the system, and motion sensors in hallways and open areas of the office.

- Panic Buttons – Panic buttons are buttons wired to alarm systems which trigger an alert that is sent to local police. At least one panic button should be installed at the reception area, but others can also be placed throughout the interior office network.

Interior Offices

Although the reception area should provide the majority of your security needs, there are several things you can do in the interior office area to make sure that your facility is properly secured.

- Telephone Access - Every room in your office network should be equipped with a telephone; this includes storage areas and workrooms. This will provide access to emergency services should the need to hide in these areas arise.

- Storage/Filing Cabinet Locks – Every filing cabinet containing sensitive information should have locks. Also, employee work areas should include at least one large drawer with a lock to accommodate employee valuables. If this is not feasible, a locker room should provided where employees can store valuables during work hours such as cell phones, purses, etc.

- Safes/Lock Boxes – Cash should always be kept in a lock box or safe; it should never be placed in a desk or filing cabinet. Especially sensitive documents and information should also be stored in safes or lock boxes to provide an extra layer of protection for these items.

- Floor Plan – A detailed floor plan of the building, with emergency exits and evacuation paths clearly marked, should be placed at every workstation and in every non-office room. This will provide with staff and visitors with a detailed explanation of evacuation procedures in the event of an emergency.

Managing Aggression

By Joseph Caulfield

Managing aggression is no different from managing anything else. One must control oneself, control the environment, and act proactively.

Concerning controlling oneself, this control must be both mental and physical. Both of these skills involve remembering to breathe. Try to breathe as if from your lower belly, rather than from high up in your chest. Not only will this keep you calm, but, remaining in control of something as basic, yet important, as your breathing will give you self-confidence and focus. As you try to breathe from your lower belly, keep your weight low as well. Bend your knees slightly. Try to relax your shoulders and upper body. Keep some distance between you and any aggressive person, about two arm lengths. Do not stand facing this person squarely. Take a half step back so that you are at an angle. This psychologically defuses a confrontation and also puts you in a balanced position and one from which you can more easily move in any direction, as needed.

Control Your Environment

If the incident occurs in your office, it is your office. A little thought as to what you would like to have handy in your office, how you would like to have the furniture arranged, which doors you would like to have locked, whom you would like to be near, where you would like to be able to easily go, will all give you an overwhelming advantage. And, more importantly, all these steps in controlling your environment occur at your leisure with as much thought as you wish to put into it, long before the incident begins.

When the incident begins, continue to control your environment. Utilize those advantages you have previously given yourself. Move to maximize your advantages. Move toward that portion of your office that gives you an advantage. Move away from that portion of your office that gives you a disadvantage. Lead or subtly move the aggressor to those portions of your office which will result in him

or her being at a disadvantage. Perhaps something as clever as through a doorway, from which you merely step back and lock the door.

Being Proactive

Of course, what I've discussed above all involve being proactive, but it is so important I wish to discuss it in its own right. Being proactive is fundamentally acting, rather than being acted upon. You must do everything to suppress those actions through which the aggressor seeks to control you and encourage those actions through which you seek to control the aggressor.

Now, with these principals in mind, I will discuss specific applications.

In order to determine the appropriate response to, say, a disgruntled client, one must have some knowledge of the different stages of anger. Is this a client who can be easily appeased or redirected? Is this a crisis which is likely to have a bad ending or an opportunity which is likely to have a good ending? The beginning of anger is often a feeling of being wronged. Many feel wronged, and do nothing about it. Others seek "justice," whatever "justice" means to that person. This first stage is called the grievance stage.

Next, is the ideation stage. The person feels that only taking action can right the wrong and that he or she is justified in taking action.

The third stage is called anger leakage. At this stage, one begins "acting out." In this stage, the individual begins to make threats, posture, raise their voice, etc.

The next stage is called the defiant stage. This is a continuation of the anger leakage stage but now the acting out is focused on the object of his or her anger, you. This is the dangerous stage because now the aggressor will seek to move close enough to you to endanger you. In other words, closer than the two arms lengths I spoke of above. Obviously, objects, be they an ashtray or a hand gun, change this spatial limit.

The last stage is called confrontation. This is usually a physical attack of some degree or other.

Whether aggression manifests through correspondence, over the telephone, or in person, the methods for defusing it are the same. As I discussed above, you must control yourself, your environment, and the aggressor. Do not let their anger make you angry. Let them be irrational, you be rational. Let them be blinded by their emotions, you stay in control of yours. First and foremost you must remain professional, someone worthy of respect. Although in the situation it may seem illogical, the way to strive to maintain that position, the position of respect, is to show respect to the aggressor. The aggressor will seek to drag you down to his or her level or below. Do not cooperate. Maintain the high ground in every sense. Do not mirror mammalian posturing and aggressive body movements. Remain relaxed, centered, in an angular stance. Do not yell and scream back. Try to speak calmly and distinctly.

In that the aggressor is in an emotional mode, seek to control the aggressor by leading the aggressor into a logical mode. Ask questions of the aggressor. See what the aggressor wants. Engage the aggressor in explaining specifically what the issues are, what can be done. This is not a time to "cross-examine" the aggressor. Do not ask leading questions. Do not ask yes or no questions. This is a "direct examination." Ask questions which require that the aggressor think, and think of something other than doing you ill.

Restate the wrong or injustice as the aggressor has described it. This is not the time to tell the aggressor that he or she has it all wrong! This is the time to show empathy. This showing of empathy will do more to bringing this matter to a successful resolution than you can imagine. Only after you have demonstrated empathy, should you attempt to explain how you see the same situation. Do not come across as arrogant. As morally outraged and as victimized as you feel by the aggressor, the aggressor feels equally or more morally outraged and victimized, or you and the aggressor would not be in this event together. Having listened to the aggressor, demonstrated that you understand the situation, showed empathy to the

situation, you will be more successful in having the aggressor show you the same courtesy. However, if it's not working, don't push it!

If things haven't gotten worse, begin the process of negotiating a solution. Don't give up on this aggressor. There is still the potential that he or she may become your friend for life. If you can reach an accord, immediately demonstrate that you intend to follow through with this agreement by taking an initial step, then and there. If you cannot reach an accord, attempt to schedule an opportunity in the future to sit down with this person and attempt to reach an accord. Perhaps you actually intend to have another meeting, perhaps you don't. In any event, this is the time to try to end the confrontation. I am confident that you will succeed!

I am so sorry you did not succeed, because now we must talk about more unfortunate and ill-omened ways of dealing with aggression. When to attack or when to retreat are very difficult things to gauge. And, of course, are specific to the situation. A 70 year old lawyer is unlikely to outrun an 18 year old disgruntled client, but anything is possible. On the same token, a 70 year old disgruntled client is unlikely to outrun an 18 year old secretary. But again, anything is possible. However, both the lawyer and his or her secretary have previously given thought to just this situation and the office/parking lot/foyer/courthouse/restaurant/home environment. The 18 year old disgruntled client will, of course, run slower if a chair is thrown across his or her path.

But, if retreat eludes you, and if rescue is not imminent, then you will be in the position of having to defend yourself. I'll discuss weapons later.

If an attacker grabs you, with very few exceptions you are only trapped if you submit to being trapped. Say your wrist is grabbed. It's only your wrist that's grabbed. That leaves you the rest of your body to move, either to retreat or attack. If you must attack, attack viciously. An ineffectual attack is going to do nothing except make matters much worse. Do not seek to strike the testicles. That's such an obvious attack, everyone knows to guard against. The eyes, the throat, the ears, raking, gouging, scratching, shrieking the whole time. That ought to do it. Then, see if an avenue of retreat has opened up.

Weapons. I am not a believer in anyone other than a trained marksman, who consistently trains, shooting a gun indoors. Bullets don't stop at office walls. In a confrontation, twenty year veteran police officers routinely fire multiple shots at close range and miss. Also, a gun is only a thrusting weapon. It can only harm what's directly in front of it. A knife, however, is both a thrusting weapon and a slashing weapon. It can harm what's in front of it and also to the side of it. Some desk letter openers are very sharp. Similarly, some office decorations are very hard. Outside the office, at a farther range, guns have more utility. Again, they should only be considered by a trained marksman who trains regularly. They do have a deterrent value, of course. If the weapon is taken away from you, though, the deterrent value is lost.

Additional Safety Tips for Working with Victims of Domestic Abuse

Appointments

- Scheduling appointments in your office is best. Assess potential security risks for both the interior and exterior of your office
- If you operate out of your home, try to identify a safe location to meet with your client. The NH Bar Center has meeting rooms available for member use.
- Avoid meeting with clients in their home.
- If a client can not travel to your office, find out if they can meet you at a crisis center agency instead. Some crisis centers have satellite offices that may be closer for the client.
- Check with your local agency to see if they have resources to assist clients with transportation and child care.
- Meeting in public spaces may compromise confidentiality, so, that is not recommended. If the client can not arrange for transportation, then, consider meeting on the phone and handling things by mail.

Office Safety

- Obtain pictures of abusers and share with office staff. You may want to consider making this a request that goes out in your typical new client correspondence.
- Abusers may be technically savvy. Be cautious using email correspondence with your clients. See *Securing Your Electronic Information* section of this booklet.
- Assess potential security risks for both the interior and exterior of your office. See *Securing the Property (Inner and Outer Office)* of this booklet.

Personal Safety

- Get your private information off the internet. Do a search on Google to see where your information comes up. For example - white pages may have a map directing people to your home. You can email them to let them know that you want this information to be unlisted and they will take it off. Some of the more sophisticated sites i.e.: ones that people pay for - may be more

difficult, but, start with Google and getting the easy-to-access information off the internet.

- Set your Facebook, MySpace, other social network sites to the ultimate privacy setting available and remove any identifying information such as date of birth, address, phone number, place of employment, etc.

Courtroom Safety

- Notify the bailiff of the potential risk when both parties are at the courthouse. Perhaps you can wait in a meeting room out of view from the abuser.
- Request that the abuser be detained from leaving the building until you and your client have been able to leave the property safely and without being followed.
- Do not let abusers see you walk out to your car after court. They may follow you or try to access your information through the DMV.