Safety and Security
In a Digital Age

AAML Mid-Year Meeting
Las Croabas, Puerto Rico
March 19, 2013

Melissa F. Brown[1]
Melissa F. Brown, LLC
145 King Street, Suite 405
Charleston, SC 29401
843.722.8900 (office)
843.722.8922 (fax)
www.scdivorcelaw.com

Helping Individuals
Cross Thresholds
to New Lives

[1] Substantial research and writing provided by Jonathan W. Lounsberry, Esquire and Ashley Simons, Esquire.

Technology provides valuable information about individuals, their habits, their communications and their whereabouts. Technology is ever changing and evolving. Much technology was created for legitimate purposes but, unfortunately, some users, such as abusive spouses, jealous boyfriends/girlfriends, dishonest employees, cyber thieves and others, misuse it to the detriment of another party.

Family law litigants are often targets of such abuse. Lawyers, litigants, investigators, forensic computer experts and judges should learn about potential abuses to protect the innocent. It is also important to properly use technology so federal and state laws are not violated. The main hurdle, though, is ~~in~~ keeping up with the advances in technology because of its rapid rate of change.

Pre-paid phone cards that spoof callers' use phone numbers; GPS tracking devices installed in cars or cell phones; illegally obtaining someone's computer and/or iPhone password to access their information; following an individual using the "Find my iPhone app;" and various types of computer spyware are just a few examples of the myriad ways others use technology for nefarious means.

Some products are also purchased online easily. Blog sites such as www.chatcheaters.com and www.emailrevealer.com highlight products for purchase that can give one side unfair advantage. Familiarizing yourself with these devices and software is now a necessity in family court cases. Lawyers who fail to recognize this fact could face a malpractice action and/or loss of potential business.

Misuse of Caller ID by Pre-Paid Spoofing Phone Cards

SpoofCards are prepaid phone cards that offer "the ability to change what someone sees on their caller ID display when they receive a phone call."[1] This technology is even accessible as an iPhone app and Facebook application.

The application promotes caller ID spoofing, voice-changing, and call recordings. SpoofCard also allows users to change the gender of their voice to further disguise their identity. While the use of this technology is legal, some states have passed laws making spoof caller ID illegal when it is used "to mislead, defraud or deceive the recipient of a telephone call."[2] On the federal level, the House of Representatives reintroduced a bill to amend the Federal Communications Act of 1934 to prohibit the manipulation of caller identification information in 2009.[3] The Truth in Caller ID Act of 2009 was signed into law on December 22, 2010.[4] As a

[1] SpoofCard Frequently Asked Questions, http://www.spoofcard.com/help (last visited January 14, 2013).
[2] *Id.*
[3] Truth in Caller ID Act, H.R. 1258, 111th Cong. (2009).
[4] Truth in Caller ID Act of 2009, http://www.fcc.gov/guides/caller-id-and-spoofing (last visited January 14, 2013).

result of the Truth in Caller ID Act of 2009 being signed into law, the FCC adopted the following rules to implement the act:[5]

- Prohibit any person or entity from transmitting misleading or inaccurate caller ID information with the intent to defraud, cause harm, or wrongfully obtain anything of value.
- Subject violators to a penalty of up to $10,000 for each violation of the rules.
- Exempt authorized activities by law enforcement agencies and situations where courts have authorized caller ID manipulation to occur.

Fraudulent uses of SpoofCards include someone taking advantage of a credit card companies' method of using caller ID to authenticate a customer's newly-issued credit card. In these situations, where credit card holders are asked to validate their new credit card by calling a 1-800 number from their home phone or cell phone, spoof card technology can intercept the "validation method," and this interception or "spoofing" allows the spoofer to pretend he is the card's true owner and, in essence, "steal" the card. The "credit card thief" can then fraudulently use the other person's credit card without that person's knowledge until the first bill arrives in the mail.[6]

Other fraudulent uses include prank calls. In 2005, SWAT teams surrounded a building in New Jersey after police received a call from a woman claiming she was being held hostage in an apartment. Her caller ID had been spoofed,[7] so the 911 call appeared to come from her apartment. The woman living there was not actually in any danger. Instead, two other young women called 911 and pretended to be a "hostage" so that the 911 operator was tricked into believing the call came from the victim's apartment. The teenagers were later found and charged with conspiracy, initiating a false public alarm, and making a fictitious report to police.[8]

Another example of spoofing abuse includes breaking into someone else's cell phone voice mailbox. Many cell phone systems are automatically set up to accept calls from the account owner's cell phone number to activate a replaying of all voicemail messages left on the cell phone. SpoofCard technology has the ability to create the illusion that it is a cell phone and the spoofer can then listen in on someone else's voicemail messages. This is a danger that divorce litigants need to know about so their spouse does not use this technology to listen in on their

---

[5] *Id.*
[6] Bruce Schneier, Schneier on Security, http://www.schneier.com/blog/archives/2006/03/caller_id_spoof.html (last visited January 14, 2013).
[7] This incident occurred the year before SpoofCards entered the market. Other spoofing technology was used here.
[8] Second Suspect Arrested in N.J. Standoff Hoax, http://www.foxnews.com/story/0,2933,151546,00.html, published March 25, 2005 (last visited January 14, 2013).

voicemail messages. Attorneys need to warn their clients about this potential danger and advise them to password protect their cell phone voice mail.[9]

Deborah Alexander, a New Jersey divorce attorney, had a client who was a victim of domestic violence. Alexander obtained a restraining order against the ex-husband, and he wanted this order overturned. To "prove" his case, he used spoofing technology to make it appear his ex-wife was calling him incessantly and that his ex-wife did not really fear him. By spoofing, he would call himself using her number so his caller ID appeared as if it was her phone number. The only way Alexander proved her client was not calling her ex-husband was to show that she did not make certain calls at certain times. She proved her case with the use of computer forensic specialists as well as the cell phone providers' cell phone records. Thus, proving someone has spoofed another requires proving the absence of calls or texts from the cell phone number that was spoofed.

TrapCall Cards

TrapCall is another type of prepaid phone card. TrapCall is also manufactured by the makers of SpoofCard. TrapCall cards work differently from SpoofCards. Instead of spoofing another's number, it unblocks and reveals callers' identities and phone numbers even if the caller has paid to block his or her number or paid to have it "unlisted."

Some TrapCall features also provide the caller's full name and billing address. TrapCall is also capable of sending transcriptions of a caller's voicemail as an email message to the TrapCall user's phone without the knowledge of the person who left the message.[10] Additionally, this technology can record incoming calls, retrieve online conversations and even block an unwanted call with a "disconnected" message.[11]

Similar Caller ID technology was utilized in the 1995 murder of twenty-one year old Kerisha Harps.[12] Ms. Harps phoned a friend's house not knowing that her ex-boyfriend was there looking for her. When the ex-boyfriend saw Ms. Harps' phone number and location on the friend's caller ID, the ex-boyfriend used the information to locate and murder Ms. Harps.[13]

Despite frightening stories like this one, TrapCall's manufacturer insists the technology was actually created to help protect domestic abuse victims. The company explains that the technology helps by identifying harassers and provides victims with the ability to record the

---

[9] Bruce Schneier, Schneier on Security, http://www.schneier.com/blog/archives/2006/03/caller_id_spoof.html (last visited January 14, 2013).
[10] TrapCall Features, http://www.trapcall.com/features (last visited January 14, 2013).
[11] TrapCall Frequently Asked Questions, http:// http://www.trapcall.com/faq (last visited January 14, 2013).
[12] TrapCall was not created until 2009. Caller ID was used in this instance.
[13] Emily Friedman, TrapCall Unblocks Caller ID, Exposes Number, http://abcnews.go.com/Technology/AheadoftheCurve/story?id=6899472&page=1, published February 18, 2009 (last visited January 14, 2013).

abuser's message and/or conversation. The company further defends its product by pointing out that abuse victims can counteract TrapCall's features if they purchase a SpoofCard. If the victim must call someone such as a former abusive spouse, the SpoofCard will hide their real number by allowing them to input a different number than the one the caller is actually using, and the company argues the SpoofCards are actually more like "safe cards."

While it is hard for average persons, especially attorneys, clients, judges and even experts to stay abreast of all the new products that come on the market, recognizing the existence of intelligence-gathering technology may help explain situations where a client appears overly paranoid when in reality their paranoia about being spied upon may be very real.

Text Messages

Technology also exists to falsify or spoof text messages. Such services are found at www.thesmszone.com. While spoofing was originally created to allow users to work outside their offices and make business calls or send texts that displayed their work numbers rather than their cell number or the actual phone being used, abusers have quickly learned to use this technology for illegitimate purposes. Abuses include impersonating another person especially to harass and/or harm a competitor's reputation or damage their lawsuit. Angry parents in a custody battle might even use this technology to pretend to be the other spouse and leave a damaging message on a guardian *ad litem*'s voicemail that puts the other parent in a bad light.

An angry spouse could use this as an opportunity for potential misuse as one spouse pretending to be the other's CPA and texting a fax number to send confidential information and using the CPA's "real cell numbers" to make the text appear legitimate. This technology can also be used to send inappropriate text messages using the other spouse's cell phone number. If such abuse occurs, the victim spouse should hire a computer forensic specialist or contact their cell service provider to show that the victim did *not* send the inappropriate text from his or her phone. Sometimes the proof is the omission of such texts from the real phone at the time the spoofed text was sent rather than proving the sent text came from another phone.

Cell Phone Surveillance

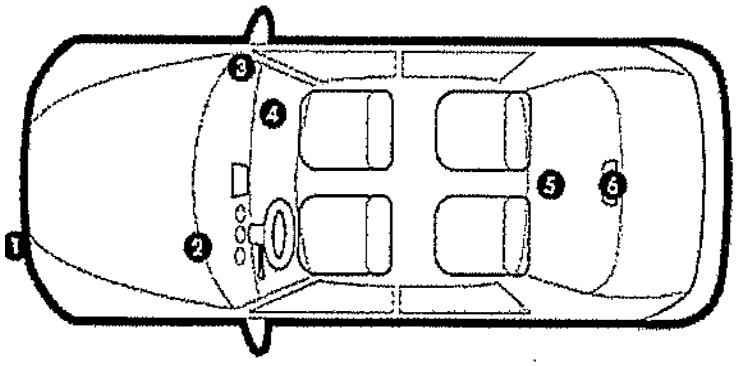
There are many valid reasons to use cell phone surveillance. The app "Find my iPhone," has helped many recover their lost iPhone or iPad. It is legal to use GPS devices on employees' vehicles as long as the employee is aware that such device is installed. Parents also use GPS devices to monitor their teenage drivers and some parents have been known to put GPS software on young children's cell phones in case they stray or for those children who are mentally handicapped and not fully capable of caring for themselves. In actuality, one can easily contact their cell phone service provider and transform a cell phone into a surveillance and GPS tracking device if one owns the device. Although the federal wiretap law prohibits many forms of electronic communication monitoring, 18 U.S.C. § 2510(12)(C) specifically *excludes* signals by mobile tracking devices like GPS. This is huge!

Predictably, some individuals abuse GPS technology and stalk their spouse or significant other. Such misuse is illegal, but these abusers are undeterred by the law. New technology also

exists to illegally register a phone via the internet for GPS surveillance with the thief paying for this surveillance using his own credit card.[14] Therefore, advise clients not to loan their cell phone to anyone whom they do not trust, even for a minute, because it only takes a few moments to add this tracking device to another cell phone. This is particularly frightening because the "stalker" can hide his or her activity by having the bills sent directly to him or her and the charges do not show up on the actual cell phone owner's bill. Clients should also know that soon-to-be-ex-spouses sometimes put GPS software on their children's cell phones for improper purposes, such as monitoring their spouse's movements by following them through the child's phone when the child is in the care of the other spouse.

GPS devices are easily placed in smart phones, pocket PCs, running watches, and vehicle navigation systems (OnStar). It is very easy to hide a GPS device in an automobile. Now, the devices are so small, even a great detective can miss a hidden device if the installer knows where to place it.

Previously, the most popular locations to hide a GPS in a vehicle were inside the plastic bumper, in the gap between the windshield and the hood, inside stereo speakers, in the front dash, under rear dash fabric, or in the rear dash/third brake light. Now, they can be placed almost anywhere and these devices are capable of tracking the cars in real time as well recording the car's speed. The devices do offer beneficial features from confirming that a spouse is cheating, if a spouse is driving dangerously or when a spouse is driving at high speeds when the child(ren) are in the car.



[1] Inside plastic bumper [2] In gap between window and hood [3] Inside stereo speaker [4] In front dash [5] Under rear-dash fabric [6] In rear dash or third brake light

Sherri Peak, of Seattle, Washington, was stalked by her ex-husband through a cell phone equipped with a GPS that he had attached to the battery of her car.[15] Sherri filed for divorce when her husband became overly possessive and questioned her whereabouts throughout the

[14] Michael Russell, Cell Phone GPS Surveillance, http://ezinearticles.com/?Cell-Phone-GPS-Surveillance&id
=510569 (last visited January 14, 2013).
[15] Dateline MSNBC, "From Husband to Stalker,"
http://www.msnbc.msn.com/id/21134540/vp/19292264 (last visited January 14, 2013).

day. After they separated, her husband began showing up everywhere she went. After six months of this behavior, Sherri asked police detectives to search her car to find out how her husband knew her every move. The detectives found a tracking device made from an ordinary cell phone under her dashboard. The charger was wired into her car's electrical system. Every time Sherri started her car, the phone would charge so he did not have to charge its batteries. Her ex-husband also set the ringer to silent so whenever he called, the phone automatically answered so he could listen in on her conversations. Her ex-husband also equipped the cell phone with a GPS system linked to a companion computer program so he also tracked her every move. (See the link in Footnote 15 for a video account of Sherri's ordeal.)

Ultimately, Sherri's ex-husband was caught and arrested. He pleaded guilty to felony stalking and served eight months in jail. When the police arrested him, they also found keys to Sherri's house, night vision goggles, computer spyware, printouts of emails Sherri sent to other people, and bank account numbers and passwords. This story is not highly unusual; according to one source, three out of every four stalking victims are terrorized by threats of violence or death at the same time they are being monitored and followed. [16]

To avoid having an estranged spouse, stalker or ex-spouse use GPS technology to track a client, advise the client to contact their cell phone service provider and ask if location services were added to her service plan. With iPhones, the client needs to check to see if the "Find My iPhone" feature is turned on, and if so, they should make sure to change their password so their spouse cannot follow them using this option. Clients should also beware of cell phone "gifts" especially if the spouse has pre-downloaded monitoring technology.

In addition, advise clients to set up their *own* cellular phone account. Tell clients to password protect their phones and keep them close to their person so their spouse does not "steal" the phone to use the latest technology developed in Israel that allows one to quickly download all information from an iPhone---even one wiped clean! [17]

Applicable Case Law

Case law and legislation[18] struggle to keep up with technological advancements to draft language that encompasses many ways technology is misused. However, courts have addressed GPS systems as they relate to invasion of privacy. Important cases address this issue, beginning with opinions that focus on surveillance by police officers.

---

[16] Marie Tessier, Hi-Tech Stalking Devices Extend Abusers' Reach, http://www.womensenews.org/article.cfm/dyn/aid/2905/, published October 1, 2006 (last visited January 14, 2013).

[17] The Cellebrite UFED Touch will recover or bypass (your choice) the password on a physical recovery. Physical recoveries of mobile devices allow the examiner to obtain copies of deleted information such as SMS messages and photos. *See* www.abramsforensics.com

[18] A listing of [some] of the 50 states' computer anti-hacking laws can be found at http://www.irongeek.com/i.php?page=computerlaws/state-hacking-laws.

The Seventh Circuit held in *U.S. v. Garcia* that GPS tracking devices did not violate the Fourth Amendment.[19] To determine if a warrant is required for installation of a GPS device by law enforcement, the Court held that the determining factor is whether the installation of the device constituted a "search" or a "seizure." If the GPS device does not borrow power from the car battery, take up any room that could be occupied by passengers, or alter the driving capabilities of the car, the court held there is no seizure.[20] The court also held that installing a GPS device on a vehicle when it is located on a public street does not constitute a search. Their reasoning noted little distinction between physical surveillance and electronic surveillance.[21]

The United States Supreme Court has consistently indicated that there is no reasonable expectation of privacy in "activities that were publicly observable."[22] In *U.S. v. Knotts*, the Court held that "an individual traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements."[23] In holding with the Supreme Court's ruling that using a GPS does not violate the Fourth Amendment, the court in *State v. Sveum*[24] held that police were free to attach GPS devices to vehicles that traveled into and out of public and private areas, even for an extended period of time.

However, the Wisconsin Court of Appeals urged states to enact legislation to prevent warrantless, baseless searches by police. The New York Supreme Court, in *People v. Weaver,*[25] also held that the placement of a GPS tracking device and subsequent monitoring of a car's location constituted a "search" requiring a warrant under the New York Constitution and was, therefore, unconstitutional. The *Weaver* Court differentiated *Knotts* by claiming that improved technology required more restrictions. Therefore, even with a warrant, police are not allowed to track a person's movements for months on end. As technology progresses, it is difficult to predict how courts will rule. It is also difficult to fit new technology into older court opinions while courts apply the old law to modern products. Thus, lawyers and judges must meet this challenge by interpreting the law's intent and applying the law's intent to the use of modern technology.

The Violence Against Women Act of 2005 (herein "VAWA") clarified criminal stalking via GPS. The revised Act reauthorized existing programs combating domestic violence, sexual assault, dating violence and stalking in order to prevent violence against women.[26] Section 114 improved the existing federal stalking law by "borrowing state stalking law language to criminalize stalking by surveillance (this could include surveillance by…GPS) or through an

---

[19] *U.S. v. Garcia,* 474 F.3d 994 (7th Cir. 2007).
[20] Brian S. Batterton, Court Order or Search Warrant Requirements for GPS Tracking on Vehicles for Ongoing Surveillance, http://www.patc.com/enewsletter/legal-answers/4-oct08.shtml (last visited January 14, 2013).
[21] *Id.*
[22] *Constitutional Law—Fourth Amendment—Seventh Circuit Holds That GPS Tracking is Not a Search*, 120 Harv. L. Rev. 2230, 2232 (2007).
[23] *U.S. v. Knotts*, 460 U.S. 276, 281 (1983).
[24] *State v. Sveum,* 769 N.W.2d 53 (*Sveum I*) (Wis. Ct. App. 2009).
[25] *People v. Weaver,* 12 N.Y.3d 433 (2009).
[26] ABA Commission on Domestic Violence, "VAWA 2005 Guide for Attorneys," April, 2006.

interactive computer service and to expand the accountable harm to include substantial emotional harm to the victim." The provision also enhanced minimum penalties if the stalking occurred in violation of an existing protection order.[27] Unfortunately, as of January 2, 2013, the U.S. House of Representatives *failed to re-authorization the VAWA effectively ending the 18 years of protection offered to women under the Act*.[28]

When installing the GPS device, private investigators are likely to be held to less stringent standards than police because no current laws address a private investigator's use of a GPS device. In South Carolina marital situations, for example, either party is authorized to install a GPS tracking device on a vehicle if: the device is a "slap and go" type tracker, if the installer does not trespass upon property when installing the device, if the device does not alter the vehicle in any way, and the device does not use the vehicle's power supply.[29] Investigators may not track government employees on government property unless the investigator has a pass to enter the property.[30] In the event that a tracked vehicle enters government property and the investigator does not have permission to track the vehicle, any information gathered by a GPS device while the government employee is on government property must be destroyed.

Spyware

Spyware is software that monitors a computer user's browsing habits. Versions of this software are also capable of collecting personal information and recording keystrokes. Some spyware contains other features such as taking snapshots of the computer screen; restarting, shutting down, and logging off the computer; controlling the desktop and mouse; and even making the computer talk. Spyware works by sending the information it gathers to the installer's computer via email in the form of detailed "activity sheets." The software is often inexpensive and easy to install, but it is very difficult to detect without the use of special anti-spyware detection software.

Some spyware is also "acquired" when one downloads innocent looking software, music, or online videos, or by opening certain emails, IMs, or text messages. Incredibly, studies show that "…the unprotected rates of PC users globally, the United States ranked the 5th least protected country. It also uncovered that there are 19.32% of Americans browsing the Internet without any protection, 12.25% of consumers have zero security protection installed and 7.07% have security software installed but disabled."[31] Moreover, only 9 years ago, a 2004 study

---

[27] *Id.*

[28] CNN Staff Writer, Backers Hope to Revive Violence Against Women Act, http://www.cnn.com/2013/01/03/politics/congress-domestic-violence/index.html?iref=allsearch (last visited January 14, 2013)

[29] Don Kneece, *GPS Tracking*, S.C. ASSOC. OF LEGAL INVESTIGATORS JOURNAL, Apr.-May-June 2009, at 12-13, available at http://www.scalinv.com/wp-content/uploads/2012/04/Journal-2009Q2.pdf (last visited January 14, 2013).

[30] *Id.*

[31] Gary Davis, 2012 Online Safety Survey – Majority Of Americans Do Not Feel Completely Safe Online http://blogs.mcafee.com/consumer/online-safety-survey2012 (last visited January 25, 2013)

conducted by America Online and the National Cyber Security Alliance concluded that, seventy-seven percent (77%) of those surveyed did not think they had spyware on their computers, but eighty percent (80%) of the computers tested were infected with some sort of spyware program.[32] You and your clients should be aware of the danger when not taking steps to protect data from malicious software.

Spyware is used legitimately by parents monitoring their children's computers. Employers can install spyware on their employees' work computers as long as the employee knows he~~/she~~ is being monitored.[33] However, when this information is obtained from an employee's computer without the user's knowledge, the employer violates the "Unlawful Access to Stored Communications" Act 18 U.S.C. § 2701. The Act states one may not "intentionally access without authorization a facility through which an electronic communication service is provided . . . and thereby obtain[], alter[], or prevent[] authorized access to a wire or electronic communication while it is in electronic storage in such system … ."

There are simple ways to protect yourself or your client from spyware. Advise clients to only install software from web pages they trust. Tell clients to carefully read the fine print in licensing agreements and to look for any reference where they might have agreed to a company's collection of a person's computer's information. Also, advise clients to be wary of popular free music and video file-sharing programs. Web links found in email spam or other unsolicited messages frequently contain spyware. Installing quality anti-spyware programs that find and delete spyware as well as running the anti-spyware programs once a week will better protect one's computer especially PC's. Apple computers, on the other hand, are known generally as being fairly safe from computer viruses and Trojans except those that use software such as Parallels that works with software run on PC's.

Spousal Abuse and the Legal Implications of Using Spyware

Mental and emotional abuse from a controlling spouse is exacerbated by the use of spyware. Currently, few laws address one spouse's intrusion upon another spouse's right to privacy through abusive spy methods. Clearly, spyware that tracks a partner's moves by observing and monitoring all computer activity such as websites visited, emails sent and received, instant messages sent and received, as well as all passwords and PINs entered by the spouse without their knowledge is illegal in most states.[34]

The use of such illegally obtained information as evidence in court proceedings is prohibited by law. The Federal Wiretap Act prohibits use of communications obtained through

---

[32] Sharon D. Nelson and John W. Simek, "Spy v. Spy," 28-WTR *Fam. Advoc.* 20, 21 Winter 2006.

[33] Spyware and the Law, http://www.spamlaws.com/spyware-laws.html (last visited January 14, 2013).

[34] See chart for individual state laws. "Electronic Surveillance Laws," National Conference of State Legislature, available at http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/ElectronicSurveillanceLaws/tabid/13492/Default.aspx (last visited January 14, 2013).

wiretapping in violation of the Act admitted into evidence at trials or hearings.[35] In 2009, a law firm in Chattanooga, Tennessee, was sued for two million dollars ($2,000,000) for allegedly using illegally obtained email evidence in a divorce action.[36] Purportedly, the estranged wife used email spyware to intercept communications from her husband's computer, and her attorney "used or tried to use" the communications in the divorce action. As of last year, the District Court for the Eastern District of Tennessee awarded husband $10,000.00 in punitive damages after he successfully sued (under both Federal and state wiretapping laws) his wife over her use of spyware to intercept his emails.[37]

Attorneys, for both ethical and legal reasons, ***must*** clearly advise clients not to use any illegal spyware devices even if the client suspects their spouse is cheating. Further, the Model Rules of Professional Conduct address the serious ethical violations that could arise if an attorney encourages or condones a client's use of such spyware.[38] Therefore, it is imperative for clients to understand the differences between legal and illegal surveillance so both the attorney and client avoid costly mistakes.

The use of spyware in intimate relationships to control a partner is not a form of domestic abuse currently recognized by law.[39] Few criminal statutes effectively address the issue of marital spying. Some civil causes of action exist that might encompass spyware, but these laws are not well-developed or targeted to put an end to this form of abuse.[40] Even the Federal Wiretap Act, 18 U.S.C. § 2510, falls short of completely protecting a spouse who is

---

[35] 18 U.S.C. § 2515.

[36] "Attorneys Sued on Alleged Use of Email Obtained from Spyware," *Chattanoogan News*, *available at* http://www.chattanoogan.com/articles/article_153998.asp (last visited June 29, 2009).

[37] *Klumb v, Goan*, No. 2:09-cv-115 (District Court E.D.Tenn., July 19, 2012) and *Klumb v. Goan*, Case No. 2:09-cv-115 (District Court E.D. Tenn., November 4, 2011).

[38] MODEL RULES OF PROF'L CONDUCT R. 1.2(d) (2002). Scope of Representation and Allocation of Authority between Client and Lawyer: "A lawyer shall not counsel a client to engage, or assist a client, in conduct that the lawyer knows is criminal or fraudulent…"
MODEL RULES OF PROF'L CONDUCT R. 1.6(b)(2) (2002). Client-Lawyer Relationship: Confidentiality of Information: "A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary: to prevent the client from committing a crime or fraud that is reasonably certain to result in substantial injury to the financial interests or property of another …"
MODEL RULES OF PROF'L CONDUCT R. 8.4 (2002). Maintaining the Integrity of the Profession: Misconduct: "It is professional misconduct for a lawyer to: (a) violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so, or do so through the acts of another; (b) commit a criminal act that reflects adversely on the lawyer's honesty, trustworthiness or fitness as a lawyer in other respects; (c) engage in conduct involving dishonesty, fraud, deceit or misrepresentation…"

[39] Katherine F. Clevenger, "Spousal Abuse Through Spyware: The Inadequacy of Legal Protection in the Modern Age," 21 J. *Am. Acad. Mat. Law*. 672, 653-76 (2008).

[40] *Id.*

unknowingly tracked, monitored and controlled by the other spouse. In fact, hardly any legal remedy exists until the controlling spouse becomes physically abusive.

The criminal definitions of domestic assault, stalking, invasion of privacy, computer tampering, and violating state wiretap acts fall short of including marital spying as a criminal offense.[41] The likely reason is that these statutes and acts were passed well before the rise in the use of computers and the Internet. Possible causes of action against a spouse who uses spyware against another spouse are negligent infliction of emotional distress, intentional infliction of emotional distress, invasion of privacy, trespass to property, and possibly violation of a state's wiretap act.[42] Again, proving each element required for each cause of action is difficult. Therefore, it is imperative that state legislatures and the federal government update civil and criminal laws to include spyware and other digital and technological advances to prevent harassment by one person against another.

Potential Liability For Attorneys Who Hire Private Investigators and/or Detectives

Hiring a private investigator or detective can create potential liability against the attorney and client.[43] In the course of an investigation, if one's private detective goes too far and commits a tort such as defamation, invasion of privacy, trespassing, or intentional or negligent infliction of emotional distress,[44] the attorney and/or client are potentially liable for the investigator's tortious activity. This situation could arise if the attorney exercises independent control over an investigator or the attorney instructs their investigator to find incriminating evidence by saying something to the effect of "I don't care how you do it."[45] Thus, it is imperative for divorce attorneys to hire trusted, professional, licensed private investigators and to refrain from ever instructing or even insinuating that the detective should violate any laws.

Conclusion

Judges, lawyers, clients and the "average Joe (or Jill)" need to educate themselves about the many technology devices and software that can infringe upon their privacy and cause them and others harm. Our laws struggle to keep pace with the rapid development; still, though, understanding the myriad ways technology is abused is critical to our family law practices. The bottom line is that keeping abreast of technology helps protect your clients, friends, family, and you from electronic abuse and it also helps prevent inadvertent misuse of technology.

---

41 *Id.* at 656-62.
42 *Id.* at 663-68.
43 Laura W. Morgan, *Divorce Litigation,* "Liability of an Attorney or Spouse for Torts Committed by a Private Detective," available at http://www.famlawconsult.com/archive/reader200303.html (last visited January 14, 2013)
44 *Id.*
45 *Id.*