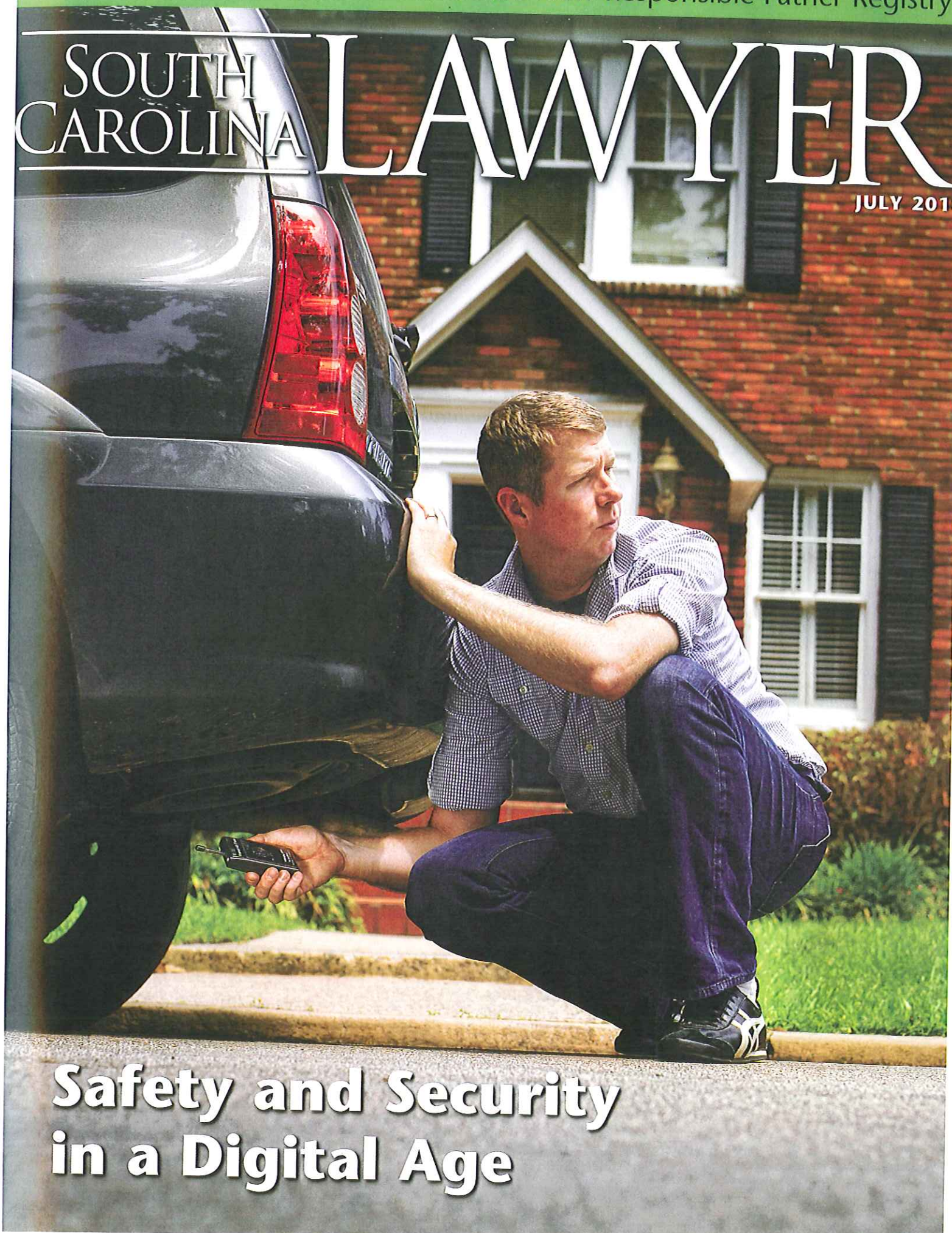
ALSO IN THIS ISSUE: South Carolina's New Responsible Father Registry

SOUTH CAROLINA LAWYER

JULY 2010



Safety and Security in a Digital Age

Safety and Security in a Digital Age

By Melissa F. Brown

New technology is now available for purchase by anyone with access to the Internet that provides valuable information about individuals, their habits and whereabouts. Most of this technology was created for legitimate purposes, but unfortunately, some users, such as abusive spouses, jealous boyfriends/girlfriends, dishonest employees and others, misuse the technology to the detriment of another.

Family law litigants are often targets of this misuse. Thus, lawyers, litigants and judges must learn how others misuse technology to protect victims from abusive tactics. It is also important for all to understand how to properly use this technology so one does not inadvertently violate federal and/or state laws.

Pre-paid phone cards that spoof callers' originating phone numbers, GPS tracking devices installed in cars or cell phones, and various types of computer spyware are just a few of the many products available for purchase, and most are easily purchased online. Blog sites such as www.chatcheaters.com highlight many of these products that one might use to gain an unfair advantage against another person. Familiarizing ourselves with these technologies and products is critical in family court cases because one cannot properly prepare his case nor can a judge intelligently rule without keeping up with the many advances in this digital age.

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." SpoofCard Frequently Asked Questions, *available at* www.spoofcard.com/faq (last visited Nov. 9, 2009). This technology is even accessible as iPhone and Facebook applications.

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 from the recipient of their call. 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." *Id.* However, in July 2009, a Florida district court held that the state's recently enacted Caller ID Anti-Spoofing Act was unconstitutional because the Act's effect regulated commerce outside the state, and therefore the Act violated the Commerce Clause of the U.S. Constitution. *Federal Court Strikes Down Florida Anti-Caller ID Spoofing Law, available at* www.newsguide.us/technology/telecommunications/Federal-Court-Strikes-Down-Florida-Anti-Caller-ID-Spoofing-Law (last visited Dec. 12, 2009). 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, and a House committee is currently reviewing the proposed bill. Truth in Caller ID Act, H.R. 1258, 111th Cong. (2009).

Fraudulent uses of SpoofCards include someone taking advantage of a credit card company's use of 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. Bruce Schneier, *Schneier on Security, available at* www.schneier.com/blog/archives/2006/03/caller_id_spoof.html (last visited Nov. 9, 2009).

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, so the 911 call appeared to come from her apartment. This incident occurred the year before SpoofCards entered the market. Other spoofing technology was used here. 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. *Second Suspect Arrested in N.J. Standoff Hoax, available at* www.foxnews.com/story/0,2933,151546,00.html, written March 25, 2005.

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 voice mail messages left on the cell phone. SpoofCard technology has the ability to create the fiction that it is a cell phone and the spoofer can then listen in on someone else's voice mail messages. This is a danger divorce litigants need to know so their spouse does not use this technology to listen in on their voice mail messages. Attorneys need to warn their clients about this potential danger and advise them to password protect their cell phone voice mail. Bruce Schneier, *Schneier on Security, available at* www.schneier.com/blog/archives/2006/03/caller_id_spoof.html (last visited Nov. 9, 2009).

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 that is manufactured by the makers of SpoofCard. TrapCall cards work differently from SpoofCards. Instead of spoofing others' numbers, it is designed to unblock and reveal callers' identities and phone numbers even if the caller paid to block his or her number or 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 voice mail as an e-mail message to the TrapCall user's phone without the knowledge of the person who left the message. TrapCall Features, www.trapcall.com/features (last visited Dec. 9, 2009). And, this technology can record incoming calls, retrieve online conversations and block an unwanted call with a "disconnected" message. TrapCall Frequently Asked Questions, *available at* www.trapcall.com/learnmore (last visited Nov. 9, 2009).

Similar caller ID technology was utilized in the 1995 murder of 21-year-old Kerisha Harps. TrapCall was not created until 2009. Caller ID was used in this instance. Ms. Harps phoned a friend's house not knowing that her ex-boyfriend was at her friend's home 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. Emily Friedman, *TrapCall Unblocks Caller ID, Exposes Number, available at* http://abcnews.go.com/Technology/AheadoftheCurve/Story?id=6899472&page=1 (last visited Nov. 12, 2009).

Despite stories like this, TrapCall's manufacturer insists the technology was actually created to help **protect** domestic abuse victims so they could identify the harassers calling them as well as provide these victims with the ability to record the 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. SpoofCards are made by the same manufacturer as TrapCall cards, and SpoofCards can display a false number if the abuse victim wants to hide her real number so the abuser cannot identify her location or real phone number. In situations involving child custody and constant contact between estranged parents, SpoofCards are potential "safe cards" to hide a spouse's real phone number from the other spouse.

Clearly the development of new technology moves so rapidly that only those in the technology world are able to keep up with all the new products. While it is hard for the average person, including attorneys, clients and judges, to stay abreast of all new products, it is important to recognize the existence of intelligence-gathering technology even when the "gatherer" is miles away from the victim. Thus, before one assumes a client is overly paranoid about a spouse spying on him or her, recognize this paranoia may be real. In addition, warn your clients to take steps to uncover whether their privacy was breached illegally invaded or their information stolen by the opposing party.

Text messages

Technology also exists to falsify or spoof text messages. Such services are found at www.thesmszone.com or www.fakemytext.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 the number of the actual phone they were using, abusers have quickly learned how to use this technology for illegitimate purposes. Abuses include impersonating another person and negatively harming the reputation of another person or even a product. Angry parents in a custody battle might even use this technology to pretend to be the other spouse and leave damaging messages on a guardian's voice mail that puts the other parent in a bad light.

An angry spouse could use this technology to send inappropriate text messages using the other spouse's cell phone number to malign the other spouse's reputation or credibility. If such abuse occurs, the victim spouse should hire computer forensic specialists or contact his or her cell service provider to show that the victim did *not* send the inappropriate text from his or her phone. Again, the proof is often 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. Employers often need to track employees during work hours. As long as the employees know the GPS is on the vehicle, it is legal to use the devices. Some parents also use GPS devices to monitor their young children, particularly those who may stray or are not old enough to care for themselves. Parents of teenagers commonly use GPS devices to track their teenage drivers. For a small fee, one can easily contact his or her cell phone service provider and transform the cell phone into a surveillance and GPS tracking 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.

Predictably, GPS technology is sometimes abused by individuals wanting to stalk their spouse or significant other. Obviously, such misuse is illegal, but many abusers are undeterred.

New technology also exists to illegally register a phone via the Internet for GPS surveillance, with the thief paying for this surveillance on his own credit card. Michael Russell, *Cell Phone GPS Surveillance, available at* http://ezinearticles.com/?Cell-Phone-GPS-Surveillance&id=510569 (last visited Nov. 9, 2009). 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" hides his or her activities by having the bills sent directly to him or her so 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 with the other spouse.

GPS devices are also easily placed in PDAs, pocket PCs, running watches and vehicle navigation systems (OnStar). GPS devices are frequently hidden in automobiles. The most popular locations to hide a GPS in a vehicle are 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. It is easy to hide these devices, and many devices are capable of tracking the cars in real time as well recording the car's speed. The features are particularly useful to confirm a spouse is cheating or, more importantly, if a spouse is driving dangerously or driving at high speeds when the child(ren) are in the car.

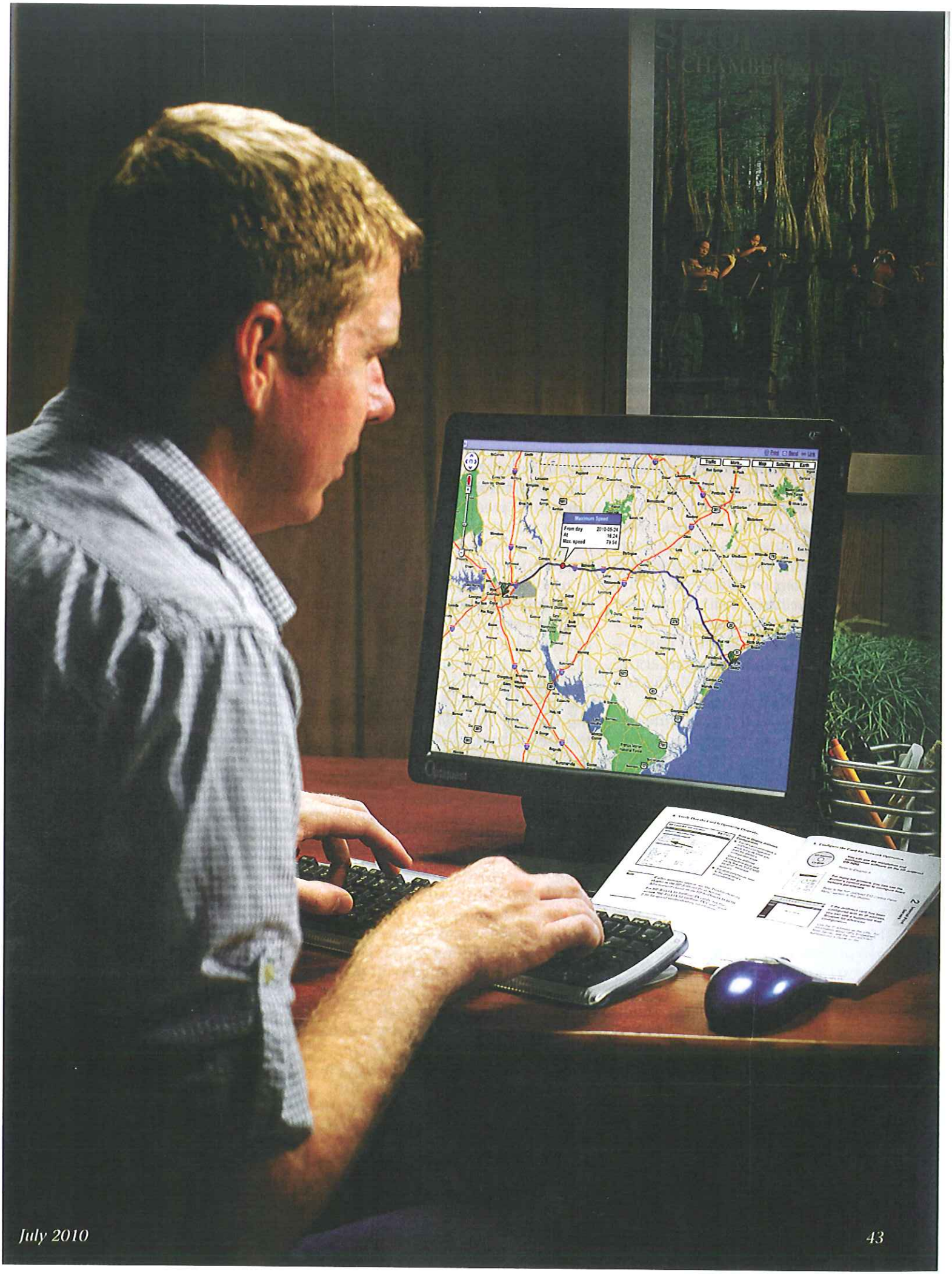
Sherri Peak, of Seattle, Washington, was stalked by her ex-husband through a cell phone equipped with a GPS that her ex-husband had attached to the battery of her car. Dateline MSNBC, "From Husband to Stalker," *available at* www.msnbc.msn.com/id/21134540/vp/19292264 (last visited Nov. 9, 2009). Sherri filed for divorce when her husband became overly possessive and questioned her whereabouts throughout the 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, and he listened to her conversations. Her ex-husband also equipped the cell phone with a GPS system linked to a companion computer program so he could track her every move.

Sherri's ex-husband was ultimately 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, print-outs of e-mails 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. Marie Tessier, *Hi-Tech Stalking Devices Extend Abusers' Reach, available at* www.womensenews.org/article.cfm/dyn/aid/2905/ (last visited Aug. 7, 2009).

To avoid having an estranged spouse, stalker or ex-spouse use GPS technology to track a client, advise the client to contact his or her cell phone service provider and ask if location services were added to his or her service plan. In addition, advise clients to set up their *own* cellular phone account and make it password protected so no one else can access account records or change account settings. Clients should also beware cell phone "gifts." The reason for this warning is that the cell phone may have GPS and other monitoring technology downloaded on it, and the recipient may not want the giver to have the ability to track down his or her whereabouts. Finally, tell clients to set Bluetooth to "hidden" and GPS to "911 only," especially when in public areas. As to GPS devices attached to vehicles, find a knowledgeable detective or car repairman familiar with the hiding places to locate any hidden devices.

Applicable case law

Case law and legislation struggle


Maximum Speed
From day 2010-05-24
At 16:24
Max. speed 79.94

to keep up with technological advancements to draft language that encompasses the many ways technology is misused. However, courts have addressed GPS systems as they relate to invasion of privacy. Following are important cases that address this issue, beginning with opinions that focus on surveillance by police officers.

The Seventh Circuit held in *U.S. v. Garcia* that GPS tracking devices did not violate the Fourth Amendment. 474 F.3d 994 (7th Cir. 2007). 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. Brian S. Batterton, *Court Order or Search Warrant Requirements for GPS Tracking on Vehicles for Ongoing Surveillance, available at* www.patc.com/enewsletter/legal-answers/4-oct08.shtml (last visited May 20, 2009). 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. *Id.*

The U.S. Supreme Court has consistently indicated that there is no reasonable expectation of privacy in "activities that were publicly observable." *Constitutional Law—Fourth Amendment—Seventh Circuit Holds That GPS Tracking is Not a Search*, 120 Harv. L. Rev. 2230, 2232 (2007), *available at* www.harvardlawreview.org/issues/120/june07/recentcases/united_states_v_garcia.pdf. 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." *U.S. v. Knotts*, 460 U.S. 276, 281 (1983). In holding with the Supreme Court's ruling that using a GPS does not violate the Fourth Amendment, the court in *State v. Sveum* 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. 769 N.W.2d 53 (Wis. Ct. App. 2009).

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,* 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. *Id.* 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 clarified criminal stalking via GPS. The revised Act "reauthorized existing programs to combat domestic violence, sexual assault, dating violence and stalking, and created new ones to meet emerging needs of communities working to prevent the violence." The National Alliance to End Sexual Violence, *available at* www.naesv.org/VAWA_2005.html (last visited Aug. 19, 2009). 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 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. ABA Commission on Domestic Violence, "VAWA 2005 Guide for Attorneys," April 2006.

When installing the GPS device, private investigators are likely 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. Don Kneece, *GPS Tracking*, S.C. Assoc. of Legal Investigators Journal, Apr.-May-June 2009, at 12-13, *available at* www.scalinv.com/pdf/apr-may-june-09.pdf. Investigators may not track government employees on government property unless the investigator has a pass to enter the property. *Id.* 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.

Currently, most states allow private investigators and individuals to use GPS tracking devices for legitimate purposes. Georgia, though, is the first state to try to pass a law prohibiting anyone other than law enforcement, parents/guardians and business owners monitoring employees from attaching GPS tracking devices to cars to track others without their consent. *Georgia Bill Would Ban Hidden GPS Tracking Devices, available at* www.wsbtv.com/news/18588494/detail.html#-(last visited July 7, 2009). Georgia House and Senate Conference Committees were appointed to attempt to reach an agreement for proposed House Bill 16. As drafted, House Bill 16 prohibits private investigators from using GPS devices unless the investigators first obtain consent from the person they are tracking (which is highly unlikely) or obtain "an order authorizing the use of a tracking device from the Superior Court of the county in which the person who is subject of

the tracking device resides." H.B. 16, 2009 Gen. Assem. (Ga. 2009), *available at* www.legis.ga.gov/legis/2009_10/search/hb16.htm (last visited Nov. 2, 2009). Those convicted of code violations are guilty of a misdemeanor. Private investigators from other states are closely watching this legislation because they fear it will not only negatively affect their livelihood, but also their personal safety and their clients' wallets.

Potential liability of attorneys hiring private investigators

Hiring a private investigator or detective can create potential liability against the attorney and client. Laura W. Morgan, *Divorce Litigation,* "Liability of an Attorney or Spouse for Torts Committed by a Private Detective," *available at* www.divorcesource.com/research/dl/expert/99dec247.shtml. 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, the attorney and/or client are potentially liable for the investigator's tortious activity. *Id.* This situation could arise if the attorney exercises independent control over an investigator or the attorney instructs his investigator to find incriminating evidence by saying something to the effect of "I don't care how you do it." *Id.* 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.

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 e-mail 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 e-mails, IMs or text messages. In a 2004 study conducted by America Online and the National Cyber Security Alliance, 77 percent of those surveyed did not think they had spyware on their computers, but 80 percent of the computers tested were infected with some sort of spyware program. Sharon D. Nelson and John W. Simek, "Spy v. Spy," 28-WTR *Fam. Advoc.* 20, 21 Winter 2006.

Spyware is used legitimately by parents on their children's computers. Employers can install spyware on their employees' work computers as long as the employee knows he/she is being monitored. Spyware and the Law, *available at* www.spamlaws.com/

spyware-laws.html (last visited Aug. 4, 2009). However, when this information is obtained without the user's knowledge, 18 U.S.C. § 2701, the "Unlawful Access to Stored Communications" Act is violated. 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, and tell clients to carefully read the fine print in licensing agreements, looking for any reference to agreeing to a company's collection of a person's computer's information. Also, advise clients to be especially wary of popular free music and video file-sharing programs. Web links found in e-mail 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.

KeyKatcher

KeyKatcher is a spyware program that some divorce litigants have used to illegally monitor and spy on their spouses. Sharon D. Nelson and John W. Simek, "Muddy Waters: Spyware's Legal and Ethical Implications," ABA, *available at* www.abanet.org/genpractice/magazine/2006/jan-feb/spywarelegalethicalimplications.html (accessed August 4, 2009). KeyKatcher software is easier to use when the couple lives together and the "spy" has constant physical access to the computer. A KeyKatcher is a small device resembling a flash-drive that is connected to a computer's keyboard or tower and records up to 262,000 keystrokes, or more than 160 pages. ThinkGeek KeyKatcher Page, www.thinkgeek.com/gadgets/security/5a05/ (last visited July 15, 2009). After the keystrokes are recorded, the "spy" can remove the device and download the information onto another computer. To prevent the use of KeyKatcher on a computer, clients should check the keyboard port on the back of their computer tower. If they find a foreign device, they should physically remove the device and have a qualified forensic computer expert analyze it.

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, e-mails 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. "Electronic Surveillance Laws," National Conference of State Legislature, *available at* www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/ElectronicSurveillanceLaws/tabid/13492/Default.aspx.

The use of such illegally obtained information as evidence in court proceedings is also prohibited by law. The Federal Wiretap Act prohibits use of communications obtained through wiretapping in violation of the Act admitted into evidence at trials or hearings. *Id.* at 673 and 18 U.S.C. § 2515. A law firm in Chattanooga, Tennessee, was recently sued for two million dollars for allegedly using illegally obtained e-mail evidence in a divorce action. "Attorneys Sued on Alleged Use of Email Obtained from Spyware," *Chattanoogan News*, *available at* www.chattanoogan.com/articles/article_153998.asp (last visited June 29, 2009). Allegedly, the estranged wife used e-mail spyware to intercept communications from her husband's computer, and her attorney "used or tried to use" the communications in the divorce action. Attorneys, for both ethical and legal reasons, ***must*** clearly advise clients

not to use any illegal spyware devices even if they suspect 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. Therefore, it is imperative for clients to understand the differences between legal and illegal surveillance so both the attorney and their clients 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. 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). 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. *Id.* Even the Federal Wiretap Act, 18 U.S.C. § 2510, falls short of completely protecting a spouse who is 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 each fall short of including marital spying as a criminal offense. *Id.* at 656-62. The likely reason is that these statutes and acts were passed well before the rise in 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. *Id.* at 663-68. Again, proving each of the elements 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.

Conclusion

Judges, lawyers, clients and the "average Joe" need to educate themselves about the various types of technology that can infringe upon their privacy and potentially cause them and others much harm. Currently, our laws are unable to keep pace with the development of new technology and hardware. Thus, it is imperative to understand the potential for abuse and to warn clients, friends and family from ever using any illegal means to obtain evidence about another individual without that individual's knowledge, unless permitted by law, so they do not inadvertently violate any privacy or wiretapping laws.

Melissa F. Brown handles complex family law matters in Charleston at her firm, Melissa F. Brown, LLC. She acknowledges Ashley Simons, a rising third year law student at Charleston School of Law, and Katie F. Perkins, Esq., for their assistance with this article.