

Adultery in the Electronic Era: Spyware, Avatars and Cybersex

By Sharon D Nelson, Esq. and John W. Simek
© 2008 Sensei Enterprises, Inc.

“Adultery is the application of democracy to love.”
H.L. Mencken

Apparently, a lot of us have applied democracy to love, judging by the fact that more than half of us get divorced and some healthy proportion of the rest have committed adultery but stayed with the marriage. What would revered wit Mr. Mencken make of the ease with which so many of us commit cyberadultery? With our inhibitions lowered online, we seem to be a very depraved bunch indeed, profligate beyond the imagination of earlier generations. Online, everyone is as wonderful as your imagination can make them – no one rattles coffee spoons, snores, or has a tendency to flatulence. There are no body odors, no bad breath and no dandruff. And in spite of all the press about computer forensics and what it can recover, we apparently cannot control our behavior online. We still feel anonymous and free to engage in outrageous conduct.

Every time we believe we’ve heard it all, another astonishing set of case facts walks through our door. If you’ve been wondering what kind of electronic evidence one finds in family law cases, here’s a sampling:

- Husband, who is fighting with his wife over custody, spoofs his wife’s e-mail address and begins sending terrible, threatening messages to himself. He introduces these messages in court as having been received by him from wife and wife loses custody. Wife returns to the court and asks for an order to have husband’s computer forensically examined, as her conversation with her experts has convinced her that her e-mail address had been falsified. Husband, who is a smarmy son of a gun, brings in the computer. Upon examination, it is clear that he ceased using this particular computer just before the horrible e-mails started. He made one big misstep though – he’d forgotten that he had set up his “wife’s ID” and tested it once with this particular computer before he began his barrage of vicious messages “sent from the wife.” Complete screen shots of husband setting up the ID were recoverable. Custody was returned to the wife, and the husband faced perjury charges.
- Wife suspects Husband is homosexual and the computer is examined for evidence. A great deal of homosexual pornography is found, but the most interesting part of the case is that Michael (not his real name), who was a househusband, became Michelle as soon the kids were safely on the school bus. Michelle, dressed to the nines and wearing heels and makeup, then went about her

day grocery shopping, etc. Digital photos on the machine showed that Michelle had a penchant for taking photos of herself all dolled up, with one peculiarity – the irrefutable proof of her manhood was always, ahem, seen sticking out. The evidence, as you might imagine, had a bearing on the subsequent custody debate.

- Husband, embroiled in divorce, receives permission to have his wife’s computer examined for evidence of adultery. The torrent of explicit e-mails with his soon to be former best friend is too much for the poor man. Overcome, and unable to cope, he asks permission to take a nap on the conference room floor. Bemused, we nonetheless acquiesce. Four hours later, he awakes, apologizes for monopolizing the conference room and departs to confer with his counsel. Both wife and the friend soon became “exes.”
- Husband, fighting for custody, receives a court order to examine his wife’s computer for adultery. Deleted but recoverable images are found that wife has posted on multiple websites. She is naked and doing all sorts of XXX things to herself on the photos while advertising for a “playmate.” In court, she portrays herself as the perfect “soccer mom” and is dressed for that role. The judge, who has been sympathetic for the wife formerly, examines the evidence from the bench on a laptop. His jaw drops as he views an image, looks over his glasses at wife, views another image, looks over his glasses at wife again, etc., etc. Custody is awarded to the husband forthwith and a considerable judicial tongue lashing is given to the wife.
- Wife finds an electronic receipt for fishnet stockings, high heels and an entire case of KY jelly. Apparently, she knows these items are not for her. Examination of the computer reveals that her powerful and well known businessman husband has a dominatrix mistress, for whom he has bought a house in a nearby town, installing the mistress and her child there. The conversations between them online are explicit, right to down to his enjoyment of the marks of the whip on his posterior. As he cannot allow this evidence to go public, wife makes out exceedingly well in the divorce settlement.
- Husband, who is quite secretive with his laptop, falls asleep at his desk. Wife walks in, finds that the laptop is logged into Second Life (an Internet virtual world) and sees on the screen an avatar (a computer user’s pictorial representation of himself/herself) which has the same name of the woman she suspects her husband is dallying with. So she assumes the identity of her husband’s avatar and begins conversing with the other woman. Through the course of the conversation, she learns that her husband’s avatar has married the woman’s avatar online in a full scale religious service, and that husband’s avatar purchased a diamond ring and wedding band for the occasion. The conversation certainly confirms cyberadultery, if not the real thing.

Quite a sampler, yes?

With respect to the last case, cyberadultery is not evidence of legal adultery, though often the cyberadultery references real-life adultery. This was the first case in which we had seen cyberadultery in a virtual world, though undoubtedly it is common. Though the studies vary, most of them estimate that about 35% of online romances become real world liaisons.

A very common source of adultery proof is instant messaging.

Here's the usual story, which applies to both instant messages and text messages. Unfaithful husband and mistress agree that they will instant message each other but will delete the messages. Husband, who is generally older with more power and money, is quite careful to delete the messages in order to avoid discovery. The mistress however, will retain some, for several possible reasons. She is lonely, and "hearing his voice" while re-reading his messages is comforting. If he writes her something sexually explicit that excites her, she'll retain it for later titillation. And, make no mistake about it, she often keeps the messages as a kind of "insurance policy," even though she may or may not be thinking of that consciously.

A common gambit is that the husband tires of the mistress, breaks it off, only to find that she has retained evidence of the dalliance. She may threaten to tell his wife, she may extort money, she may demand that he do her favors. With much at stake, the husband may find it hard to resist any demands. At this point, you have what is wryly known in our office as a "dope on a rope."

Cell phones have come into their own recently. Early 2008 included journalists swarming happily over the steamy text messages sent by Detroit Mayor Kwame Kilpatrick, some 14,000 of them, to his Chief of Staff. Not only were some explicit, but they contained information about the times and locations of their trysts and their plans to cover them up. This after both parties had testified under oath that they had no intimate relationship. A major electronic "whoops."

Within the past year, we have seen perhaps a 200% increase in the number of cell phones given to us for forensic imaging and analysis. Forensics can indeed recover deleted text messages, sometimes going back for years. Why is the use of the cell phones for clandestine affairs increasing? Our theory is that most people are rarely far from their cell phones. It seems more private to them, and less likely to be discovered than misdeeds on the computer. Moreover, being a delusional crowd, most adulterers seem to have convinced themselves that deleted text messages are really gone. While it is true that the phone carriers themselves usually "delete the deleted messages" quickly, the deleted message are written to the phone itself and can remain there for quite a long time.

A new kind of electronic evidence in domestic relations cases is emerging in Britain, where suspicious wives are beginning to hire "hottie" private investigators to test their husbands' fidelity.

Imagine this. You are a married businessman on your way home from work. As is your innocent custom, you stop in for a quick pint at the local pub. A very attractive young lady joins you at the bar and begins to flirt with you. Her “availability” is clear. Are you a bastion of chastity? Or do you decide that the easiest way to get rid of temptation is to surrender to it? Be aware that, at least in Britain, your encounter may be videotaped, for whatever use your spouse may choose to make of it. This remarkable “sting” operation is now dubbed “honey trapping” by British PIs, who say business is brisk.

The depressing result is that 80% of the targets appear ready to shuck their marriage vows when opportunity knocks. Of course, since their spouses are already suspicious enough to hire “hottie” PIs, perhaps that percentage is not so surprising.

Will this new PI tactic make it across the pond and provide a new source of electronic evidence in divorce cases? We haven’t seen this kind of aggressive maneuver yet, but we Yanks frequently imitate our English cousins, so we’re waiting for honey trapping to debut here.

So remember guys, if an attractive young lady comes out of nowhere to flirt with you – smile – for you may well be on *Candid Camera*.

As we admonish divorce attorneys constantly, you need to be thinking about all possible sources of evidence – digital cameras, iPods, PDAs, thumb drives, CDs, DVD, external hard drives used for backup, old hard drives, voicemail and on and on. The first thing we do when a client comes in the door is play a kind of high tech version of “Where’s Waldo?” – and the picture is often equally confusing and complicated.

Now, of course, the good old computer is still often the source of the evidence. A word of caution here: if the computer is a marital asset, either party could back it up – likewise, either party can have it forensically imaged. But, and this is a huge but, they do not have the right to use forensic software, which will blow by passwords, to uncover things that were meant to be kept private. This is disconcerting to many folks because they want to find out what their spouse is up to before filing for divorce. However, before a forensic technologist can legally “go past” the passwords, there must be a court order in place, which means that the divorce action must be filed. Overeager private investigators and techie friends often violate the law, frequently from ignorance.

And this brings us to the current nemesis of errant spouses and lovers, spyware.

Spyware has made the notion of peeping through keyholes wonderfully quaint.

How much simpler it is to record your spouse/lover/significant other’s every keystroke and know for sure what they are up to without ever leaving the comfort of your computer station.

Who would ever imagine that the authors would be interviewed by NBC, ABC, CBS, USA Network, NPR and Oprah’s “O” magazine, each interview focusing on the

obviously sexy topic of spyware and divorce? Clearly, this is a subject which has caught the public's interest.

The legality of spyware used to be murky, at best. The courts have spoken of it only infrequently, so there is precious little guidance. How does a lawyer appropriately advise the client who wants to employ spyware, or who already has? How does a lawyer appropriately advise the client who believes that someone has used spyware to conduct surveillance on their computer usage? It is a dicey business, and fraught with risk for lawyer and client alike.

Before plunging into the legality of spyware, let us set the stage.

Generally speaking, spyware is software installed on a computer without the target user's knowledge and meant to monitor the user's conduct. Most of the time, in domestic practice, the target is e-mail, instant messages, Internet activity and chat rooms, but the software will record everything the user does, including financial record keeping, the preparation in a word processing program of letters to counsel, or the keeping of business records. Some spyware is used to gather personally identifiable information like passwords, credit card numbers and Social Security numbers, all useful for those interested in fraud and identity theft. Some spyware programs will hijack your web browser, reset your home page, add toolbars, alter search results or send popup ads that cannot be closed, all intended to hawk some vendor's products.

Spyware has become insidiously clever recently – many programs come with a reinstaller – as soon as you attempt to remove it, it reloads itself. Many forms of spyware hide in Windows system files and even mimic the file names so the average user would have no idea that the files are in fact shielding spyware.

These days, there are so many spyware manufacturers that it is well nigh impossible to list them all. They have such names as eBlaster, IamBigBrother, SpyAgent, Spy Buddy, Spector Pro, Keylogger Pro, Invisible Keylogger and 007 Spy Software. They have different features and have slightly different operating characteristics but they are all intended to spy on someone else's computer use – stealthily. There are also hardware keystroke loggers such as KeyKatcher, a small, dongle-like device that fits in between the keyboard and the PC. It's a modern day "bug" with a memory capacity of 64K, 128K, 256K and 4MB, able to store several weeks' worth of typing, after which it can be removed and all the text downloaded onto another machine. The drawback, obviously, is that this requires that the person placing the KeyKatcher have continuing physical access to the machine. KeyKatcher is therefore primarily used by husbands and wives residing together. In point of fact, having analyzed hundreds of computers in divorce cases, 100% of the time, a software spyware application was used instead of a hardware logging device.

Some of the older programs acted like cameras, taking a picture of whatever was on the screen every few seconds. The picture play back was like a herky-jerky film from the 1920's. Many of the programs would send the log files of the activity to an e-mail

address so that you can “play back” the sessions. Today, most of the software actually records keystrokes, so you can see every chat message or e-mail in its entirety, along with the Internet sites visited, documents composed and financial transactions conducted.

A screen shoot from the control panel of the spyware eBlaster is shown below.



How much does spyware cost? Not much - \$30-\$100 is a common range, a cheap price for a heinous invasion of privacy. Two of the most devious spyware applications, eBlaster and Spector Pro, cost \$99.95.

Will the user know that spyware has been installed? No – these applications are exceedingly clever. They change their install dates, don't show up as a running program, don't show up in your list of programs, don't show up in the “Add/Remove” function, and change their names to something that sounds like a benign – and boring – system file. Who would ever give the file name windowstht.dll another thought?

So how does spyware get installed? Clearly, if the spouses reside together, it is easy for one party or the other to install spyware. However, if the parties live apart and the spouse wishing to install spyware doesn't have physical access to the other party's machine, then there are methods of remotely installing spyware. As a for instance, the husband might send an electronic greeting to the wife saying how he sorry is for the pain he's caused, etc. etc. He sends the card as an attachment with a cover e-mail that says, “Honey, I'm so sorry for all the pain I've caused – the attached card helps me to express my real

feelings.” Whether she loves him or hates him, she’s going to want to see the card so she opens the attachment. And bada-bing, the spyware downloads (invisibly) right along with the greeting card. In the same mode, perhaps he sends some cute photos of the kids when he took them to the beach. Irresistible to the wife – she opens them and the spyware, piggybacked on the photos, covertly installs itself and begins monitoring her online activities.

Fortunately, spyware programs cannot hide from skilled forensics examiners who know where these stalkers hide. This is one of the most difficult parts of computer forensics because you are specifically looking for something which intends to be invisible. In the vast majority of cases, the authors have found that significant amounts of data can be uncovered, most notably the e-mail address to which the reports were sent. Once an attorney has that, if there is not currently a divorce proceeding on file, the attorney can file a John Doe suit and serve a subpoena on the Internet Service Provider to learn the identity of the account holder.

As of February, 2008, there is no federal anti-spyware law. The House of Representatives has continuously passed bills designed to punish those who install spyware on people's computers without their knowledge. This charade has gone on for at least five years, with the bills stalling when they get to the Senate, reputedly due to the lobbying efforts of the Direct Marketing Association. All such bills say they will pre-empt state law, so it will be fascinating to see what Congress agrees to, assuming it ever agrees

Most states currently have legislation which is intended to outlaw some kinds of spyware. Sometimes the laws are anti-spyware specific, sometimes they are computer trespass, unauthorized computer access or privacy laws and sometimes they are wiretap statutes which apply to electronic communications.

How about other laws, not specific to spyware? Herein lays many a trap in which a lawyer might unwittingly step. First, let us consider the federal laws:

- The Electronic Communications Privacy Act of 1986 prohibits the interception and disclosure of wire and electronic communications. It also applies to those who use information they know or have reason to know was intercepted. Though the law was in flux for some time, it is now commonly accepted that the use of spyware would violate this act.
- The Computer Fraud and Abuse Act prohibits a person from accessing a computer without authorization or from exceeding authorized access and thereby obtaining certain governmental, financial or consumer information. Clearly, spyware is often used for these purposes.

Because this area is indeed a sand trap, there are also a number of state laws that may apply. Some examples include:

- Computer privacy laws
- Wiretap laws
- Computer trespass laws
- Fraud laws
- Harassment laws
- Stalking laws

Not only may spyware violate a myriad of laws, some of them do and some of them don't carry with them a clause excluding the admission of illegally obtained evidence. And where they don't contain such a clause, especially at the state level, it is generally held to be at the discretion of the trial court whether or not to admit the evidence. Pass the Advil.

Though we see a lot of cases in court, most opinions simply reference electronic evidence without the electronic evidence itself being a source of controversy. One often cited case is *White v. White* (N.J., 2001), in which a wife accessed the husband's e-mails which were stored in an America Online file cabinet on the marital computer. No password was required to get to the e-mails, though the husband was unaware of that. The court held that the wife had violated no laws in getting to that e-mail.

In *O'Brien v. O'Brien* (Florida, 2005), the wife installed spyware to monitor her husband's conduct. He had begun playing dominos with a woman he met through Yahoo, and then began playing, well, something more than dominos. Under the Florida Wiretap Act, the data gleaned from the spyware was not required to be excluded; however, the trial court had chosen to exclude it. The appellate court found that the exclusion of the data was within the trial court's discretion and it therefore declined to disturb the lower court's decision.

What are your clients up to? Attorneys who do domestic relations work can answer this question easily. If you want to check out what your clients are reading online, just type "cheating spouse" in Google and prepare yourself for a slime bath. One typical site is <http://www.chatcheaters.com/>, which contains real life stories, ads for keystroke loggers, advice on how to catch cheaters, and even a PI and lawyer directory. Most of the time, clients will have surfed all over the Net on this subject and purchased/installed/used spyware before they ever consult an attorney. They will arrive in your office with printouts of e-mails that scorch your eyebrows as you read them. They are generally quite pleased with their resourcefulness and blissfully unaware that they may have broken a law or multiple laws. The common belief is that "the computer belongs to both of us so I can do anything I want." When told they may have broken a law, they become ashen-faced, and are stunned to think that the "guilty" party now may have a cause of action against the "victim."

What else may your client be up to? Not uncommonly these days, they may have installed a GPS vehicle tracker. Bad move? It depends (in our own state) on who owns the vehicle. See Virginia Sec. 46.2-1088.6, which says that recorded data may only be accessed by the motor vehicle owner or with the consent of the motor vehicle owner or the owner's agent or legal representative; except for 1) a contracted service such as LoJack 2) service of vehicle or 3) access by an emergency responder service. If both parties own a vehicle, you're probably fine, but our observation has been that these devices are being used willy-nilly without respect to ownership.

What are the ethical implications for a lawyer with regard to spyware? Under the scope of representation rule (Rule 1.2), "a lawyer shall not counsel a client to engage, or assist a client, in conduct that the lawyer knows is criminal or fraudulent." You may, of course, discuss the subject of spyware with a client who may have used it or is considering using it, but only for the purpose of explaining its probable illegal nature. Though we have heard lawyers argue passionately that they do not believe that spyware is illegal, especially in particular states, we believe these attorneys are sorely mistaken and leaving themselves open to sanctions and disciplinary proceedings if they act upon their belief in counseling their clients.

Under Rule 1.6, a lawyer is released from the attorney-client privilege and may reveal, as the lawyer believes necessary, "such information which clearly establishes that the client has, in the course of the representation, perpetrated upon a third party a fraud related to the subject matter of the representation."

The same rule requires that a lawyer promptly reveal "the intention of a client, as sated by the client, to commit a crime and the information necessary to prevent the crime, but before revealing such information, the attorney shall, where feasible, advise the client of the possible legal consequences of the action, urge the client not to commit the crime, and advise the client that the attorney must reveal the client's criminal intention unless thereupon abandoned, and, if the crime involves perjury by the client, that the attorney shall seek to withdraw as counsel." Moreover, the attorney must promptly reveal "information which clearly establishes that the client has, in the course of the representation, perpetrated a fraud related to the subject matter of the representation upon a tribunal" (first asking the client do so).

Rule 8.4 states unequivocally that 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 or deliberately wrongful act that reflects adversely on the lawyer's honesty, trustworthiness or fitness to practice law; or
- (c) engage in conduct involving dishonesty, fraud, deceit or misrepresentation which reflects adversely on the lawyer's fitness to practice law.

Therefore, two things you may not do:

- Continue to represent a client who uses spyware after receiving the attorney's advice that use of such software is illegal
- Use illegally intercepted communications or information gleaned from unauthorized access to a computer (under the Virginia Wiretap Act, this is expressly forbidden in any event)

One last point: the general rule is that someone who creates a password (outside of the work environment, where the employer has a right to monitor computer conduct) has created an expectation of privacy and denied authorized access to anyone (including a spouse) who has not been given the password. It does not matter that the computer is marital property because it is not a property right that is being protected – it is a privacy right.

What about monitoring children? You do have the right to monitor your minor children. However, you absolutely may not use the software installed to monitor your children as an excuse to ALSO monitor your spouse, ex-spouse, etc. To the extent that there are communications, for instance, between an ex-spouse and a child that show up in the child's e-mail, you are (so far as current cases are concerned) ok in having those communications. However, the point must not be to spy on the spouse – there should be a concern involving the child which motivates the usage of the monitoring software.

What should you advise a client who thinks there may be spyware on his/her computer? If it sounds to you like the facts warrant it, you'll want to have a forensic technologist find and document the spyware's existence. This software is so squirrely that the evidence a lay person can get, if any, is so fragmentary as to be worthless in court. Far better to let an expert find and document the spyware. In any event, you don't want someone trampling all over the evidence, changing access dates, etc. Sometimes, the expert's advice will be to let the spyware continue operating briefly while a sniffer is employed to determine precisely where the information is going once it leaves the target network.

Clearly, an attorney cannot threaten a criminal charge. However, we've seen the use of spyware used as a trump card time and again. Once the use of the spyware is proven, all the attorney needs to do is communicate that fact to the other side's counsel for the implications to be clear. Sometimes, this is done in the course of a deposition where the deponent will deny under oath having used spyware, only to have the evidence shown to them. Likewise, if they take the Fifth, but the evidence is extant, it is clear to all what the risks are. To put it bluntly, cases in which the use of spyware can be proven tend to settle quickly.

If your objective, particularly in a case involving modest assets, is to simply get the spyware off, you can have the client try running a reputable anti-spyware program, such as Webroot's SpySweeper or Sunbelt's CounterSpy. They may not find ALL spyware,

but they will find most of it. Beware, however, because the installation of these programs will be detected by the spyware, thereby alerting anyone monitoring computer activity that you are “on to them.” At that point, they may well use remote technology to order the software to remove itself and delete all traces of its existence.

If your choice is to simply find and eradicate the software, just be mindful that you will have no evidence of the computer spying to use in the future. Also, you must stress to your client that they should never again open an attachment from anyone likely to be interested in remotely installing spyware.

A caveat: Some people are convinced that there is spyware on their computer when there is not. If you have a competent computer forensics expert and they say there is no spyware, the client is probably the one mistaken. One frequent explanation – the spouse has guessed or cracked a password – which is also illegal – so make sure you consider all the alternatives!

What should you advise a client who is using spyware to monitor someone else’s computer activity? Get it off. Now. No excuses. It is probably illegal in your state and certainly illegal under federal law. It is important to explain to anyone who has used spyware that they may be compelled to take the Fifth in depositions or in court.

In real life, we have seen some attorneys, after counseling the removal of spyware, nonetheless use data collected through the spyware to determine how best to use the resources of private investigators to glean proof of (for instance) adultery. Some attorneys have advised that they see no ethical concern here, though the authors believe that this constitutes an impermissible use of poisoned fruit.

Be prepared for arguments, especially in domestic relations cases. Over and over again, we have to patiently explain that it doesn’t matter if the computer is owned jointly. In our state of Virginia, you may search a spouse’s car, briefcase, and wallet but there is a specific statute that says you may NOT install spyware. Violation will subject the offender to both criminal and civil penalties.

It is also a fact of life that many clients seem unable to “pull the plug” on their spying. Remarkably enough, the spying itself often becomes an addiction and the perpetrator is unwilling or unable to break the addiction. It may be necessary to be quite forceful, stating unequivocally that you will have to withdraw from the case if possible criminal conduct continues.

In a number of instances, we have seen those who installed spyware on someone else’s computer religiously monitor correspondence between the victim and his/her attorney. Clearly, no attorney can have anything to do with such conduct under the disciplinary rules!

What do I advise a client who is fairly certain there is significant evidence on a marital computer? No spyware. Wrong solution and it will likely end up getting the client in

trouble rather than the spouse who is actually engaging in bad conduct. The first thing you'll want to do is have a forensic image made of the computer. This can be done without the spouse knowing while he/she is at work or away on a business trip. Generally, if a computer is received in the morning, a forensic technologist can make and verify the image, returning the computer in the afternoon. At this point, at least you have a record. You will not want to authorize the technologist to analyze the image until a court order has been received, which will protect both attorney and client against any civil or criminal claim of computer trespass or invasion of computer privacy. If the court order is not a current possibility, and perhaps no divorce action is underway as yet, you still have a forensic image to examine when the time is right and you have the court's imprimatur.

As excruciatingly slow as Congress is, the outcry over spyware will probably lead to the passage of a federal law explicitly outlawing spyware. When that day comes, once the national definition of spyware becomes clear, lawyers will have an easier time dealing with spyware cases. For now the best advice is to treat it as though it is illegal, even where some doubt exists. Certainly, there is no doubt in our state of Virginia as to the illegality of spyware. For the sake of professional reputation, never mind more dire consequences, it is imperative that lawyers take the higher road and avoid the stench of the "spyware swamp."

Quick E-Evidence Tips for Family Law Practitioners

1. **What you're looking for:** Typically, family law attorneys are looking for e-mails and cell phone text messages. That's where the evidence of adultery is usually to be found. In many cases, chat and instant messages are not recoverable because they are not written to the hard drive. You'll need to explain exactly what applications were used to your computer forensic expert before you can know what is likely to be recoverable and what is not. E-mail, including web-based mail, is generally recoverable. Ditto for cell phone text messages, though the forensic acquisition of some cell phones is not yet supported. You may also be looking for Internet history, perhaps to show an Internet sex addiction, a fascination with something particularly disturbing for someone who has partial or full custody, or to show the purchase of gifts for a third party. You may also be interested in financial records to prove that there are hidden assets or that there has been a dissipation of assets. Never forget those little gems of information, social networking sites such as Facebook, MySpace and AdultFriendFinder.
2. **How you get what you're looking for:** If the computer or phone itself is password-protected, or if it is not a marital asset, you need to get a court order to forensically image and analyze. If it is a marital asset, and e-mails, text messages etc. are password protected, you will need to get a court order. Courts abhor fishing expeditions so the requests should be specific. File a Motion to Image and Analyze a Computer (or other device).

3. **How do you protect privacy rights?** Besides being specific, make sure the court understands that your forensic expert will turn over the results of any searches to the opposing counsel for review and production. Alternatively, the other side may perform its own forensics and searches – however, it is key that the parties agree on what the search parameters are. Sex-related terms are common, as are date restrictions, or searches for particular e-mail addresses. Quite often, we have seen parties agree that the search can be for evidence of adultery, sexual conduct on the Internet, or asset dissipation or concealment without further parameters. Again, this is a matter for agreement between counsel – or the judge will be happy to decide for you.
4. **What about the ISPs?** Internet Service Providers do not like to retain deleted data – they hose it as quickly as possible (almost always in 30 days or less) to avoid the subpoenas. With respect to e-mail, unless you are only interested in current activity, you are going to have to get the computer of the sender or the recipient. You can get activity logs from ISPs, but they will not contain the content of communications. This is also true for most cell phone providers. Verizon recently stated that it holds the data for two days. Not to worry, the data is on the phone itself.
5. **What happens if child pornography is found?** Any competent examiner is going to turn the evidence over to the police, as required by law. Sometimes, when child pornography is suspected, it is wise for counsel to consider how the wife will support herself and the children before getting access to a computer containing contraband. Once the rabbit is out of the hat, it is a near certainty that criminal charges will be brought and defendant will be financially ruined – and incarcerated if guilty.
6. **How much does the usual divorce case cost in terms of computer forensics?** It isn't cheap, so there is always a calculation to be made when deciding to proceed down this road. If the assets are modest, it may not be worthwhile, unless there is a serious child custody issue involved. A small case, one involving both forensic imaging and forensic analysis, is one that comes in under \$10,000. More than 80% come in under this amount. The remainder generally do not exceed \$15,000. Only cases with considerable financial or other complexities (such as e-mails in a foreign language) tend to exceed that amount. Remember that there are additional charges for producing a forensic report (very time-consuming) or appearing in court.
7. **How long will it take to do the imaging?** This depends on the size of the hard drive and how intensively the computer has been used. A common amount of time is 4-6 hours.
8. **Can the person then have the computer back?** Absolutely, your computer forensic expert will work on the image of the evidence.

9. **How long will the analysis take?** This varies by company, but you need to anticipate a minimum of 2-4 weeks after the forensic image has been made. Sometimes, they can expedite the analysis and sometimes these cases are stacked up like patients on gurneys in a hospital corridor.
10. **How do I maintain chain of custody?** FedEx, or any other tracking number system, will work just fine. A chain of custody form should be used each time the evidence is transferred.
11. **How much deleted data can you find?** Attorneys hate this answer, but it just plain depends – once again, on the size of the hard drive and how intensively the machine was used. A small hard drive, written to intensively, will overwrite data faster, thereby making it unrecoverable as compared to a “mega” hard disk volume, which has a lot of extra space available for storage of deleted data. If the other side has tried to use a wiping program, much or all of the deleted data may be truly gone – however, virtually all such programs leave evidence of their existence, often quite damning as evidence of spoliation.
12. **Any special concerns with sending phones/computers to my expert?** Yes, don't try to pack the computers yourself. Have the experts at a mailing service like FedEx do it –and make sure to insure it. If the cell phone is off, leave it off. If it is on, make sure it is fully charged and then send it for overnight delivery.

The electronic era has certainly complicated the life of the family law practitioner. We've come a long way from the days of Perry Mason, who had trusty PI Paul Drake to help him solve his cases. Now the detectives are digital and the cases often blossom into a *CSI* script – but they are rarely solved in 60 minutes!

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology and computer forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com