

THE ELECTRONIC PEEPHOLE: E-EVIDENCE IN FAMILY LAW CASES

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

Electronic evidence in family law cases cuts a wide swath these days. It consists of e-mails, text messages, instant messages, word processing documents, GPS data -and who knows what the next generation of mischief will bring? But let us begin with the diva of evidence in family law cases – 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. Adultery is as old as time, but who would ever guess that cyber-adultery would be a commonplace phenomenon, and often the genesis of divorce?

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?

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 attempt to set the stage.

First and foremost, what constitutes spyware?

No one quite agrees, but generally speaking, it 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 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 identify 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 persistent 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. The latest wrinkle with spyware is that it can turn the infected machine into a spam zombie. This means that your computer is being used as a relay point to send spam messages without your knowledge.

What are some of the spyware programs commonly in use?

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 major advantage of the KeyKatcher is that no software will be able to detect its presence. 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. It is certainly cheap, beginning at \$32.99. But 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.

How much does software 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 card to the wife saying how sorry he 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 often 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.

What is the status of laws explicitly dealing with spyware?

As of October, 2008, there is no federal anti-spyware law. The House of Representatives has passed (again) two 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.

Many states currently have legislation which is intended to prevent 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. According to the National Conference of State Legislatures, as of March 24, 2008, there were 14 states with specific anti-spyware statutes: Alaska, Arizona, Arkansas, California, Georgia, Indiana, Iowa, Louisiana, Nevada, New Hampshire, Rhode Island, Texas, Utah and Washington.

Note that Virginia is not mentioned, which makes us nervous about the accuracy of the NCSL's information. Below is an excerpt from Virginia's Computer Trespass law, which clearly includes the use of spyware in paragraph eight (but note the possible exception for a machine which is marital property). Also note that it was clear under the previous spyware law that interspousal interception was prohibited – however, the 2007 changes to the law added the “computer owner's authorization” language.

§ 18.2-152.4. Computer trespass; penalty.

A. It shall be unlawful for any person, with malicious intent, to:

8. Install or cause to be installed, or collect information through, computer software that records all or a majority of the keystrokes made on the computer of another without the computer owner's authorization

How about other laws, not specific to spyware?

Aha, an excellent question. 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. Distinctly not a good thing if your client has violated 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
- Voyeur laws

Not only may spyware violate a myriad of laws, some laws do and some 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. If admitted, the illegality goes toward weight.

What are the leading cases in this area?

An oldie but a goodie, *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 those e-mail messages.

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.

The case of *Potter v. Havlicek* (S.D. Ohio, 2007) involved the question of whether evidence obtained via monitoring software on a family computer could be introduced even though the act of obtaining the evidence may have violated the Electronic Communications Privacy Act. The court noted that the ECPA applies only to “oral and wire communications” and not electronic. Judge Rose noted that several courts, including the Sixth Circuit, have concluded the Congress intentionally omitted illegally intercepted electronic communications from the category of cases in which the remedy of suppression is available. He also noted that “this is not to imply, however, that disclosure of the information in state court by {the husband} or his attorney might not be actionable civilly or criminally under 18 U.S.C. Sec. 2511.” With respect to the husband’s argument that the e-mail were not intercepted in transit by the monitoring software, Rose discerned “some merit in the position of Judge Reinhardt who opposes a hyper-technical application of the contemporaneous requirement emasculating the ECPA” (referring to *Konop v. Hawaiian Airlines, Inc.* (9th Cir. 2002)). The same position was adopted by the *First Circuit in U.S. v. Councilman* (Fla. Dist. Ct. App. 2005), applying a law similar to the ECPA. Rose further noted that there is no interspousal exception to the ECPA.

For the record, the authors believe that Judge Rose articulates the correct view of the law, and one which we believe is beginning to prevail across the nation.

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.”

But what about monitoring kids?

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. The data contents of the transmission may be unreadable as more and more software packages are encrypting the communications prior to sending the information.

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 of 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 instruct 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 certainly violates federal law, and possibly Virginia state law as well, depending on the facts.

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.

It is 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.

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.

What about cell phones?

What if a spouse brings us a cell phone that is marital property? If there is no PIN required to access the phone, what law prevents her from authorizing the accessing of the phone’s data, assuming it is marital property? We can’t think of one. With the PIN of course, the phone owner has established an expectation of privacy - with that being the case, we will “freeze” the data by imaging it if possible (some phones will not allow for data extraction while a PIN is active), but we will not analyze it without a court order.

Can you go to the cell phone provider for text messages? Not usually. AT&T says it stores the actual text of cell phone messages only for 48 hours. Verizon has recently said it will hold the text message for two weeks. There is no blanket statement to make here: the carriers all have different rules and change them constantly.

And about that GPS

Perhaps the hottest surveillance device of the last year has been the GPS, which many a spouse or lover has resorted to in order to track the location of the spouse or lover suspected of wanderlust. In Virginia, it is illegal to place a GPS tracking device on a vehicle in which you do not have an ownership interest. In the average family law case,

the cars are marital property, but there are a significant number of cases in which the car is titled in only one name, or the car is leased. If you own the car, you can track it. If you don't own the car, you can't. Need the law to prove it?

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.

It has been our experience that private investigators use these devices regularly, remaining blissfully unaware of the law. In fact, many a lawyer has disputed our assertion that Virginia has such a law until we produce the actual statute! It is very much a case of "say it ain't so!" But wishing it were otherwise doesn't change the law.

Note that cell phone monitoring chips are frequently intended to monitor the use of children, a very legitimate purpose. But there is nothing to keep them from being used as a device to monitor a spouse's location.

What about filming bad behavior?

Out of luck there, if the law violates Sec. 18.2-386.1. Unlawful filming, videotaping or photographing of another; penalty. A portion of that law is excerpted here:

It shall be unlawful for any person to knowingly and intentionally videotape, photograph, or film any nonconsenting person or create any videographic or still image record by any means whatsoever of the nonconsenting person if (i) that person is totally nude, clad in undergarments, or in a state of undress so as to expose the genitals, pubic area, buttocks or female breast in a restroom, dressing room, locker room, hotel room, motel room, tanning bed, tanning booth, bedroom or other location; or (ii) the videotape, photograph, film or videographic or still image record is created by placing the lens or image-gathering component of the recording device in a position directly beneath or between a person's legs for the purpose of capturing an image of the person's intimate parts or undergarments covering those intimate parts when the intimate parts or undergarments would not otherwise be visible to the general public; and when the circumstances set forth in clause (i) or (ii) are otherwise such that the person being videotaped, photographed, filmed or otherwise recorded would have a reasonable expectation of privacy.

Nowhere do we see an interspousal exception. So a webcam in the bedroom, which is frequently suggested by surveillance sites, does not seem like a stellar idea.

How about obtaining phone records via pretexting?

You could do it once, but no more. Check out The Virginia Code § 18.2-152.17, Fraudulent procurement, sale, or receipt of telephone records. If telephone records have

been obtained under false pretenses, a lawyer dare not even accept the proffered documents without violating the law. Though this law was enacted in 2006, a good many Virginia lawyers remain blissfully unaware of it. The federal government passed the Telephone Records and Privacy Protection Act of 2006, which was signed into law in January of 2007, also outlawing pretexting. Like the state law, the act of receiving the documents may also constitute a crime. The days of private investigators routinely obtaining phone records for lawyers via pretexting are officially, and probably forever, over.

Final words

As excruciatingly slow as Congress is, the outcry over spyware will probably lead to the passage of a federal law explicitly outlawing spyware, probably when the economy has, if indeed it will, settle down. As for state law regarding spyware and other forms of surveillance, you can probably anticipate a lot of tinkering. One of the problems with the new technology and the consequent new laws is that we have so little case law to guide us. The vast majority of these cases settle. Added to that, no sooner has the law caught up to technology than technology leapfrogs the law, which again limps gamely behind it, playing a never-ending game of catch-up.

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