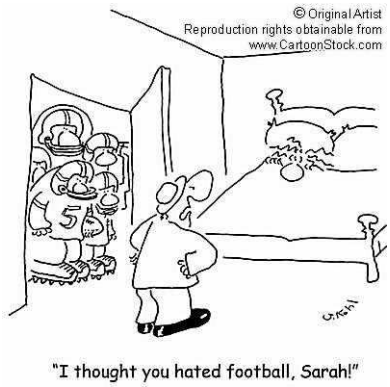
The Internet and Infidelity



My project is titled the Internet and Infidelity and in it I plan to cover issues of privacy and security as they relate to the home. Courts have made it clear when it comes to privacy in the workplace there virtually is none as far as the Internet goes. The equipment in the workplace is the property of the employer as are the data transmission lines and therefore data stored on and transmitted through work computers is also considered the property of the company.

However, privacy in the home is a different question altogether. Here the question becomes does the law of community property trump the rights of individual privacy? Does the fact that it is perhaps easier to spy on your spouse than ever before make it okay to do so? How does the law deal with the issue of privacy vs. technology in a marriage?

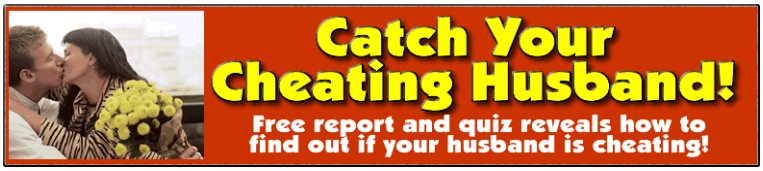
First, we must address the most basic question; are you allowed to spy on your spouse at all?

In the State of New Jersey, the law is pretty clear on the level of privacy a spouse can expect in their marriage. The New Jersey Supreme Court has stated "*"There is no reason whatsoever to allow spouses to perform non-consensual tortuous acts against each other than there is to allow them to perform them against third parties. The right of privacy extends within the confines of the marital home. It is not somehow dissipated into the air upon the taking of marriage vows."* ***[1]***

As in most legal matters that apparently clear language does not mean things are not necessarily clear. The ruling says an individual in a marriage can expect the same amounts of privacy afforded to them in the marriage and in the marital home as they could expect anywhere else. However, as I demonstrated above when it comes to the workplace an individual cannot expect much privacy at all. There is a question as to how much privacy one has in public as well. A December 2006 report issued by the ACLU found that there were 262 surveillance cameras on 125th St. in Manhattan alone.[2]

So if the normal person can't expect any degree of privacy in the workplace and has their privacy infringed on every time they step out into public, how much privacy can they expect from their spouse in the marital home if the standard says their privacy there is guided by the same standards they should expect anywhere else?

Of course this paper is dealing with privacy as it extends to security and computer technology. One of the new technologies that would be immediately impacted by this line of questioning is VoIP, or Voice over IP. VoIP is the technology that moves voice communication from standard phone company copper wires and out of



switching stations and onto the predominantly fiber optic lines of the Internet.

Once again the federal government and the courts need to decide if the same rules that apply to traditional voice transmission apply to VoIP. Is this form of communication the same thing simply because it is verbal communication, or does it fall under a new legal standard because it involved a different technology?

How the federal government treats this matter and how the courts in turn interpret the government's actions will be the first standard by which actions in the marital home are judged.

Towards that end the Department of Justice the Department of Homeland Security have requested that the Community Assistance for Law Enforcement Act of 1994 (CALEA) be extended to include VoIP. [3]Originally VoIP had been exempt from CALEA in order to promote the development of the Internet. But in the interest of national security Justice and Homeland Security have sought to have that changed.

Basically, at this point, in the eyes of the law eavesdropping on a VoIP line is tantamount to illegally tapping into a phone line. Some states have gone so far as to specifically define this as a form of "cyber stalking" and have laid out legal guidelines for what constitutes a breach of an individual's privacy and what the penalties are for doing so.

The primary threat to an individual using VoIP is that from a technological point of view it is easier to tap into a VoIP conversation than it is to tap into a traditional phone conversation.

VoIP technology takes voice conversations and converts them into digital packets that are switched over data line in much the same way any other form on digital communication is. These packets can then be intercepted, again, in the same manner as any other digital packet. Whereas with traditional phone tapping there was a need to somewhere along the line install a physical device to capture phone conversations and record them, this does not have to be done with VoIP. Basically a suspicious spouse could in theory install a program similar to a keylogger on a computer, capture phone conversations as packets of data and apply a decryption program to transpose that data back into voice format.

Should a suspicious spouse employ such technology he is running the risk of a run-in with the law.

However, due to the technology being deployed there are loopholes in the law that allow, at this point anyhow, for vendors of VoIP spyware to continue to market and profit from their products.

While in the eyes of the law hacking into a VoIP conversation meets the same legal definition as wiretapping, one needs to keep in mind that the laws regarding wiretapping were written in a time before the development of digital communication equipment. Wiretapping laws state that it is illegal to tap into the "transmission" of others' conversations. When written voice communication was not stored and it was therefore logical to specify "transmission".

VoIP does not include the seamless transmission of the data. As a person speaks their voice data is converted into digital packets. As the packets are assembled they are temporarily stored before being transmitted. Although they may be stored for intervals so brief as to be beyond human recognition, they are still being stored. It is while in the storage state that many VoIP spyware programs work. Therefore it is the claim of the makers and distributors of these products that they are not indeed breaking wiretapping laws but rather capturing stored

data.

On this issue the courts are split. Courts as high as the appellate level have ruled that such actions are a violation of the spirit of the law, while other courts have ruled that spouses who store data on a computer in a common area of the marital home should have a reasonable expectation that such information can be viewed by others, most specifically their spouse.

Compared to a non-digital situation in the eyes of the law if a wife were to discover a letter to her husband from a lover out in the open, perhaps on the kitchen table, she has a right to read its contents and eventually use the information contained therein in divorce proceedings as evidence of adultery, which is a legal condition for divorce in New Jersey.[4] By leaving the letter on the kitchen table, which of course would be a common area in the marital home, the husband should have had a reasonable expectation that his wife would find the letter. However, if that same husband had left the letter in a locked safe that only he had the combination to and the wife had used a blowtorch to open the safe, the contents of the letter would most likely be dismissed as inadmissible since the husband should have had a reasonable expectation that his privacy was protected by putting the letter in the safe.

If somebody is using their computer on a regular basis and this is a computer that is used by most people in the house, and is kept in a common area, there should be a reasonable expectation that information stored on that computer can be retrieved by others.

Does that include data stored for nanoseconds, such as VoIP transmission? That has yet to be determined and will most likely, with other similar issues, be ultimately decided by the United States Supreme Court.

There are in fact many products commercially available for both the VoIP spy and for the person looking to protect themselves from being spied on. Interestingly, most of the commercial products available for spying don't advertise them as a way to catch a cheating spouse. Rather, they advertise them as being a way to "protect" your children from the dangers of the internet or for employers to "protect" their business. The issue of spousal spying is too much of a hot button topic for them to advertise it that way. What I thought was amusing was that when you do a Google search for ways to spy on your spouse you still get these products as results. So they have told the search engines that is what their product can do, but they don't openly tell the public.

Protection against this form of cyber spying is done by basically the same product names as those that would protect you from most other forms of spyware. Big names like Symantec and McAfee to unknown fly by night firms offer products they claim will protect you against VoIP intercepts. What most of these products will do is look for known spying applications and upon detecting them warn the user and give them the option to have the offending program removed. However, as detection programs get more sophisticated, spyware makers get more sophisticated in their deployment of evasion tactics.

We do return once again to the issue of reasonable expectation. In New Jersey the courts have ruled that if a person password protects their data they are setting up a reasonable expectation that their privacy will not be invaded. Therefore, if a spouse sets up a password protection and that password is hacked by the suspicious spouse, not only would evidence gained in such a manner be illegal, but the offending spouse would be subject to fines and even imprisonment.[5]

Most VoIP companies also offer a routing box that does

not connect directly to the computer. Hacking data out of the box is a clear violation of wiretapping laws.

One of the most common forms of “domestic spying” is through the use of a key logger, or keystroke logger. A key logger does exactly what it sounds like; it logs, or records, each keystroke. Key loggers can also record other actions such as mouse clicks. There are two basic types of key loggers; hardware and software. Hardware key loggers are usually cylindrical devices about the size of a lipstick. They are installed between the keyboard and the computer itself, or are sometimes installed inside the keyboard itself. Hardware key loggers are easily detected with a visual inspection and just as easily removed.

The FBI is generally credited with developing the first key logger. They had developed the key logger to gather evidence in racketeering cases against the mafia. Details of the technology behind the program have been kept secret as the FBI claimed divulging these details would compromise national security and the courts backed them up.[6]

The FBI remains at the forefront of developing key logging technologies. Originally the FBI needed to gain physical access to the target’s home or office in order to install the key logger. They then had to retrieve the device in order to pull the data.

Although the actual technology is still classified it is believed the FBI now has key loggers remotely by email without having to use the normal Trojan strategy of using an attachment and hoping it gets opened. Rather just opening the email will install the program. The data is then accessed and analyzed remotely.

The legal and technological issues surrounding keyloggers, which are primarily used to capture email and Instant Message (IM) communications, are pretty much the same as those raised by VoIP, as the transmission and capture of such information is similar, if not parallel and is also relatively new technology that the law has not completely caught up on.

There are still legal questions about whether or not you can actively use a keylogger without somebody’s permission that revolve around the technology being used. If you look at the standards for what is protected – transmission of data, a reasonable expectation to privacy – and what is not – stored data kept in a common location – you can see how lawyers would be the people making the most money on this question.

It could indeed be considered a philosophical question. Could any court definitively decide whether or not a tree that falls when nobody is around makes any noise? We know that the laws of physics say that it does, but can you bring evidence to a court that would prove beyond a reasonable doubt that any given tree did in fact make noise if there was nobody around to hear it? Even if you brought a videotape or an audiotape to court a smart enough lawyer could argue that the presence of electronic surveillance meant that somebody was there to hear it thus disproving the theory it would be unheard if there was nobody. Got it?

Here is the question as being argued in the courts. If a keylogger records the actual stroke of a key, and not the transmission of that stroke, is that in fact the same as wiretapping? Would the same people who say it is okay for a parent to use a key logger to ensure his child’s safety on the Internet say it was not okay for that same parent to use that same program on his spouse? The technology involved in these types of communication is different than that used when wiretapping laws were put in place so the courts have whole new challenges ahead of them.

Is it then any more clear cut as to whether a spouse can videotape a spouse without their knowledge, or record conversations not taking place on the phone? One product I came across while doing this paper – Stealth Keylogger 4.5 – actually advertised that it not only logged keys but also recorded all noises with a small radius of the computer.

Actually, it is not. Video surveillance equipment has taken great leaps in recent years. Nanny cams jumped in popularity as more and more families became two income homes. It was only a matter of time before they also were advertised as a way to catch a cheating spouse.

The general rule of thumb regarding what is allowed when videotaping and what is not allowed had been whatever is viewable by the public is legal to videotape. But as the law struggles to keep up with technology old rules of thumb may not always apply anymore. If a woman lives on the 35th floor of an apartment building should she have a reasonable expectation of privacy if she decided to get dressed with the shades up? Prior to the age of 220X zoom digital cameras and digital image enhancement she might have. But then does it mean because technology has advanced people need to adjust their perception of what a reasonable expectation is? This is the kind of question courts and juries will no doubt have to dispute for a long time to come. Generally speaking the courts are beginning to lean towards the rights of the individual. In New Mexico it is legal to videotape your spouse without their knowledge but only if there is no accompanying audiotape.

Videotaping technology has advanced to the point where high quality cameras can come in very small sizes so as to be nearly undetectable. Cameras can be hidden in clocks, teddy bears, smoke detectors and even in the head of a pen.

There is a hidden danger to using a hidden camera or nanny cam to spy on your spouse. Most of these spy cams are wireless and come with a software package you use to record and view the images on your own computer. However, these wireless signals can be intercepted by other people. The New York Times, following up on an urban legend that had a woman finding a porn tape of her and her husband on the internet, did confirm how easy it is for people to have their nannycam signals intercepted.

A recent drive around the New Jersey suburbs with two security experts underscored the ease with which a digital eavesdropper can peek into homes where the cameras are put to use as video baby monitors and inexpensive security cameras.

The rangy young driver pulled his truck around a corner in the well-to-do suburban town of Chatham and stopped in front of an unpretentious home. A window on his laptop's screen that had been flickering suddenly showed a crisp black-and-white video image: a living room, seen from somewhere near the floor. Baby toys were strewn across the floor, and a woman sat on a couch.

After showing the nanny-cam images, the man, a privacy advocate who asked that his name not be used, drove on, scanning other homes and finding a view from above a back door and of an empty crib. [7]

Try as I might I was unable to find a legal precedent for what happen when somebody distributes a tape obtained in this manner. I should clarify; it is legal to obtain the tape but it is unclear whether it would be legal to distribute it. The law covering this area says it is illegal to tape somebody without their knowledge. In this case the person being taped is the person who set up the camera.

There is, of course, the expectation of privacy, but the camera covered in the article comes with a user manual that clearly states the signal can be detected up to a quarter mile away. So if you've set up the camera and you have a written warning that the signals can be detected outside the home do you still have the right to expect privacy?

The bottom line is this is an evolving and fluid situation. It would be difficult, if not impossible to expect the law to catch up to a technology that advances at such a rapid pace. Further is the consideration that while the civil libertarians battle for increased rights to privacy the government will fight to make sure there is not so much protected expectations as to prohibit surveillance deemed vital to national security.

One article I read when I first began to research this paper began by saying spouses have been spying on each other as long as there have been spouses. This is a supply and demand question; laws against using digital technology are not going to stem demand. If the laws get tougher all that will happen is evasion tactics will become more advanced. Cameras are going to get smaller and give better quality images and audio devices are going to get more sensitive and unfortunately, spouses are going to keep cheating.

---

[1] M.G. Plaintiff v. J.C., Defendant, 254 N.J. Super 470 (Ch. Div. 1991), extracted from http://www.aaml.org/files/public/Gruber_-_Spying_On_Your_Spouse.htm#_ftn3, extracted May 2, 2007

[2] NYCLU Report Documents Rapid Proliferation of Video Surveillance Cameras, Dec. 14, 2006, http://www.aclu.org/privacy/spying/27686prs20061214.html, Extracted May 2, 2007.

[3] Voice over IP: Does Powerful New Technology Need Protection to Develop?, American Constitution Society, August 27, 2004, http://www.acsblog.org/ip-and-tech-law-voice-over-ip-does-powerful-new-technology-need-protection-to-develop.html, extracted May 2,2004

[4] Although evidence of adultery cannot be used in New Jersey when determining distribution of assets or parental custody.

[5] Spying On Your Spouse, Significant Other, Or Domestic Partner - Legal Consequences, Mark Gruber, Esq., J.D., L.L.M., http://www.aaml.org/files/public/Gruber_-_Spying_On_Your_Spouse.htm, extracted May 2, 2007

[6] United States v. Nicodemo S. Scarfo, et al. Criminal Action No. 00-404 (NHP) http://www.epic.org/crypto/scarfo/opinion.html, extracted May 2, 2007

[7] Nanny-Cam May Leave a Home Exposed, John Schwartz, April 13, 2007, http://www.securityprousa.com/nanmayleavho.html, extracted May 2, 2007

Brian P. Fisher, Sr.

A man returning home a day early from a business trip, got into a taxi at the airport. It was after midnight and while enroute to his home, he asked the cabby if he would be a witness. The man suspected his wife was having an affair and he intended to catch her in the act.
For $100.00, the cabby agreed.
Quietly arriving at the house, the husband and cabby tiptoed into the house and then to the bedroom. The husband switched on the lights, yanked the blanket back and there was his wife in bed with another man. The husband put a gun to the naked man's head.
The wife shouted, "Don't do it! This man has been very generous! I lied when I told you I inherited money. He paid for the Corvette I bought for you. He paid for our new cabin cruiser. He paid for your season New York Giant's tickets. He paid for our house at the lake. He paid for our country club membership, and he even pays the monthly dues!"
Shaking his head from side-to-side the husband slowly lowered the gun. He looked over at the cab driver and said, " What would you do?" The cabby replied; "I'd cover his ass with that blanket before he catches a cold."

Cheating Wife Cartoon from CSL Cartoon Stock, http://www.cartoonstock.com/directory/c/cheating_wife.asp, extracted 3/6/2007

Cheating Wife Joke from JibJab Joke Box, http://www.jibjab.com/jokebox/jokebox/jibjab/id/499620/jokeid/114061, extracted 3/6/2007

mailto: fisherb1@mail.montclair.edu