

Adultery in the Electronic Era: Avatars, Cybersex and Hottie Honeypots

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 for 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 bizarre case walks through our door.

From the case files: 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 her husband’s avatar purchased a diamond ring and wedding band for the occasion. The conversation certainly confirms cyberadultery, if not the real thing.

In law, of course, cyberadultery is not evidence of 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 becoming increasingly common. More often, we see cyberadultery in instant messaging.

Here’s the usual story. 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” for when he dumps her, even though she 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, and 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. Witness 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.

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 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 messages are written to the phone itself.

A new kind of electronic evidence 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 “honeypot 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*.

Elliot Spitzer is now painfully aware of the power of data. It was his frequent cash transactions that finally led to his financial accounts being “red-flagged” by an automated system. His own bank turned him in, following the provisions of the poorly named Bank Secrecy Act of 1970. As originally constituted, the Act required banks to report on cash transactions of \$10,000 or more. Those who wished to evade the Act simply took out or put in lesser amounts in a short period of time. These days, the banks have a formula for determining cash in/cash out in a given period of time. The law requires banks to track politicians more closely as they are “politically exposed persons.” Now, you would think Spitzer would have known this, as he has used bank reports under this law previously to dethrone (we just can’t help ourselves here) the “emperors” of Wall Street.

Now, as a member of the Emperor’s Club (what a tribute to hubris in a name!), Spitzer himself is alleged to have tried to dodge the law by making smaller but frequent cash transactions. He apparently made enough of them to trigger a report to the IRS by his own bank, which subsequently resulted in a wiretap, and oh well, you know the rest. So much for the governorship of New York.

We are sure he was less than delighted to find that his paramour Kristen had a MySpace page, adding further ignominy and irrefutable electronic evidence to a situation that could hardly be worse. One moral among many here is that it pays to remember how automated our society is. In many ways, the “Sheriff of Wall Street” was gunned down by the same technology he embraced in so many of his investigations.

Welcome to the new high tech world of adultery and the multitudinous ways in which we may make our private affairs public!

*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*