

Thursday, January 23, 2014

1:30 p.m. – 4:45 p.m.

Law Office Technology

3.0 MCLE Credit Hours; 1.0 LEPR Credit Hours

### Law Office Technology

*Sharon D. Nelson, Esq.*

*John W. Simek*

*Fairfax, VA*

In the first segment, Sharon and John will discuss how lawyers have an ethical duty to be competent and to keep their client data confidential. Clients want to keep their confidential data protected, but all too often, information security is not prioritized by law firms. It costs money to protect data, and businesses frequently resist budgeting for security, even though an ounce of prevention is far less expensive than a pound of cure. Investigating and remediating data breaches is hideously expensive, not to mention the necessity of complying with state data breach notification laws. This session will cover:

- ✓ *How data breaches occur (and the session will specifically cover the South Carolina state data breach)*
- ✓ *How to prevent data breaches using a combination of technology, policies and training*
- ✓ *Secure computing when you're on the road*
- ✓ *Encryption*
- ✓ *The new rules for strong passwords*
- ✓ *Common sources of breaches: User Error, Technology Snafus, Insiders, Hackers and Hactivists*
- ✓ *How to manage smartphones in a BYOD (bring your own device) world*
- ✓ *What you must do after a data breach*
- ✓ *The stories of real-life law firm and client data breaches which will no doubt cause you to reassess the security of your own data*

In the second segment, we will learn that divorce lawyers are no longer looking for the “lipstick on his collar.” Today, they are hunting for his (or her) e-mails, text messages and Facebook posts, where clear-cut evidence of adultery so often exists; Ditto for evidence of Internet porn addictions and concealment or dissipation of marital assets. What can a forensic technologist retrieve from cell phones and computers? What is irretrievable? What happens if your client used spyware – or was the victim of its use? Is it ok to put a GPS on the car of a spouse or lover? What federal laws apply to e-evidence in divorce cases? How are the states handling these questions? Our experts have been grilled by all the national networks – and even Oprah – on these issues. Come prepared with your own questions on how to legally procure and use electronic evidence in divorce cases!

After the break, Sharon and John will discuss how the hunt for the Craigslist killer involved many kinds of digital evidence – and without it, Philip Markoff might never have been caught. The digital evidence included video images, disposable cell phones, text messages, e-mails, cell phone towers, IP address tracing, digitized fingerprints, possible wireless network poaching and Facebook posts. On the framework of this astonishing tale, our experts will flesh out the digital forensics aspects of the case as well as focus on the privacy implications for all of us – innocent OR guilty.

### Agenda

- |                       |   |
|-----------------------|---|
| 1:30 p.m. – 2:30 p.m. | <b>Locked Down: Information Security for Law Firms and Their Clients</b>      |
| 2:30 p.m. – 3:30 p.m. | <b>Perry Mason Goes Digital: Electronic Evidence in Family Law</b>            |
| 3:30 p.m. – 3:45 p.m. | <b>Break</b>  |
| 3:45 p.m. – 4:45 a.m. | <b>On the Trail of the Craigslist Killer: Case Study in Digital Forensics</b> |

**Course Planner/Moderator:** *Courtney G. Kennaday*