by counsel had some conceivable effect on the outcome of the proceeding. Id.; *Sanders v. Commonwealth*, 89 S.W.3d 380, 386 (Ky. 2002).

…

In attempting to obtain post-conviction relief, the movant must present facts with sufficient particularity to generate a basis for relief. *Foley v. Commonwealth*, 17 S.W.3d 878, 890 (Ky. 2000).

…

It is not the function of this Court to usurp or second guess counsel's trial strategy. *Baze v. Commonwealth*, 23 S.W.3d 619, 624 (Ky. 2000)."

Claims for RCr 11.42 relief raised just during 2005 include failure to:

- strike a juror
- object to prosecutorial misconduct
- seek alibi witness
- seek mental competency hearing
- explain a plea bargain
- preserve trial errors
- seek funding for expert witness
- investigate and challenge the validity of the search
- conduct a thorough investigation into the facts of the case
- consult with the client on trial strategy
- present a defense
- object to an improper jury instruction
- develop a defense strategy that had any chance of success
- advise the client of the defense of entrapment
- offer certain testimony by avowal

Any of these claims, if proven, could result in a malpractice claim. The lesson of all this is that you should fully advise your client, investigate the case thoroughly, object to everything, keep good notes, and keep your fingers crossed.

"There are very few people who don't become more interesting when they stop talking."

Mary Lowry

For more information about Lawyers Mutual, call **(502) 568-6100** or KY wats **1-800-800-6101**
or visit our web site at **www.lmick.com**

Lawyers Mutual Insurance Co.
of Kentucky
Waterfront Plaza
323 West Main Street, Suite 600
Louisville, KY 40202

PRESORTED STANDARD
U.S. POSTAGE
PAID
LOUISVILLE, KY
PERMIT NO. 879

Malpractice Avoidance Update
Member National Association of Bar Related Insurance Companies

THE RISK MANAGER
Lawyers Mutual Insurance Co. of Kentucky

SUMMER 2005 NEWSLETTER
Volume 16 Issue 3

Contact us
1-800-800-6101
or visit
our web site at
www.lmick.com

"Death is not the end, there remains litigation over the estate."

Ambrose Bierce

Ten Technology Traps And How to Avoid Them

by Mark Bassingthwaighte

Editor's note: Keeping up with computer technology is essential risk management for any lawyer practicing today. Mark Bassingthwaighte, Risk Management Coordinator for the Attorneys Liability Protection Society, in his article "Ten Technology Traps And How to Avoid Them" provides an excellent analysis of current technology issues for lawyers with practical advice on dealing with them. Mark generously has given permission to include a condensed version of his article in this newsletter and place the entire article on Lawyers Mutual's web site, www.lmick.com (go to the Risk Management Subject Matter Index and look under Computers). The complete article includes software information.

1. Laptop Theft: Laptop theft is a leading cause of computer security breaches. Here are a few tips:

- While going through security screening at an airport, always keep your laptop in sight. If you go to the restroom or sit down to use a telephone, do not place your laptop on the floor – it is just too easy for someone to pick up the laptop and disappear into a crowd.
- Never check your laptop with your luggage. It should always travel with you as a carry-on item.
- Tape a business card to the top of the laptop and mark the laptop case to make it readily identifiable and unique.
- Never check a laptop into a hotel "baggage hold" room, and do not leave the laptop in your hotel room throughout the day. Place the laptop in the trunk of your car or carry it with you.
- Be careful about where you leave your laptop. It's too easy for a laptop to become an out-of-site, out-of-mind kind of thing.
- Use password protection on your laptop. Make certain that a screen saver initiates and the system automatically logs out after a period of time – ten to twenty minutes would be a reasonable choice.
- If the laptop contains highly sensitive data, consider using encryption software. Windows 2000 and XP offer file encryption capabilities.
- Remember to periodically back up the laptop's hard drive for protection in the event that it is lost or stolen. If you do local backups (i.e., to Zip Discs), store those backups separately from your laptop – not in your laptop case, but another place such as your suitcase.

2. Metadata: Metadata is extraneous information about an electronic document that remains attached to the document. As an example, metadata tracked with a document created in Microsoft Office (note: metadata is not unique to Microsoft products) includes your name and initials and the names of your company or organization, your computer, and your network server or hard disk on which you saved the document. In addition to this tracking information, metadata also includes other file properties and summary information, non visible portions of Object Linking and Embedding (OLE) objects, the names of previous document authors, document revisions, document versions, template information, hidden text, comments, macros, hyperlinks and routing information.

- Metadata, once outside of a law firm, could be problematic. You might be unintentionally sharing confidential information.
- The benefit of using metadata removal programs is that they allow you to create a "clean" version of a document that is separate from the original.
- For those of you using Microsoft Office 2003/XP, an add-in is available that will enable you to remove permanently hidden and collaboration data, such as change tracking and comments, from Microsoft Word, Microsoft Excel, and Microsoft PowerPoint files.

3. Spam Filter Deployment: A Spam filter can be quite effective at removing unwanted email. It also often captures legitimate email, particularly in the early stages of deployment. Most law firms should consider the following recommendations when deploying a Spam filter.

- Obtain all clients' preferred email addresses for use during the course of representation and provide this information to your technical support personnel. They will enter this information into the filter's "acceptable" list. Going forward, gather this information during client intake.
- Give attorneys and staff access to the Spam filter's quarantine folder so that they can review this folder for email that has been captured accidentally.
- Make certain that all who have access to the Spam filter's quarantine folder review the folder on a regular basis.

continued

Filters are set up to automatically delete email that has been retained for a predetermined period. Typical automatic deletion periods run from three to fourteen days. Therefore, if the auto deletion period has been set at five days, everyone must review the quarantine folder at least every five days. Review of junk mail is done via a search feature that allows each user to review quarantined email sent to their own email address. Users do not need to review the entire quarantine folder each period.

- Consider placing language in your firm's engagement letters or other introductory materials that requests the client contact the firm via phone if an email has not been acknowledged within twenty-four, or forty-eight hours.
- Require use of the email program's auto responder when staff or attorneys will be out of the office for more than one day and unable to check for email while out. The message sent by the auto responder should contain instructions on whom to contact and how if the matter cannot wait for the staff member or attorney to return.

4. Lack of Professionalism: Email is a place where being casual can be dangerous. Check your spelling and grammar, and make sure your e-mail has a signature block at the end.

5. No Recent Backup: Most law firms understand the need to create periodically a "backup copy" of the firm's computer-based data. The frequency of creating the backup and the number of backup copies made varies widely. Here are a few thoughts in that regard.

- To determine the backup frequency necessary for your office, consider how difficult it would be to redo the work that has been done since the last backup (e.g. calendaring, time entries, file updates, billing, accounting, etc.). The period of time that you are comfortable allowing to pass sets the rotation schedule. For small offices, the frequency typically varies between every other day to once a week. For offices of five or more attorneys, a nightly backup is best.
- General business standards call for a nightly backup. Typically, the nightly backup is done with a tape-based data storage device, and the nightly backup will use one in a series of five or ten tapes. In a five tape series the tapes are labeled Monday through Friday, and in a ten-tape series the same occurs but with a "week one" or "week two" notation added on the tape's label. At a minimum, keep the current day's backup tape off-site and return it the following workday. NOTE: If you decide to store your backup tapes in an on-site fireproof safe, make certain the safe is rated for electronic media storage. Many fireproof safes will not protect electronic media.
- Due to the increase in virus activity, we strongly recommend keeping a second series of backup tapes. This second series of tapes should be a minimum set of three tapes and often goes to six. Use these tapes to create monthly backups and label accordingly. This entire series is stored off-site. The rationale for this second series is that a virus could infect the firm's computer systems and copy itself to the daily backups, potentially rendering the daily backups useless. Some firms permanently archive a monthly or quarterly backup tape.
- An often overlooked but very important step is monthly testing of your backup tapes. It is imperative that you periodically try to restore some files to a test area on your network, or to a test server, and then open and use the stored backup files to ensure that the information is there, is accessible, and is usable. Once a year, and soon after implementing a new backup system, you should use the backup tape to do a full system restoration on a test server or in a designated test area, to ensure that your backup contains everything needed to run and use your computer system.
- All backups should be full backups, and not merely a fast update of altered files only. Partial backup tape volumes can have thirty or more updates on them, and trying to rebuild your system's data from such a tape often will prevent you from fully recovering your system's data and operability.

"No wonder young people are confused. Half are urged to find themselves; the other half are told to get lost."

June Flynn

6. No Legacy Systems: Discuss long term data access issues with your IT staff or consultant including the option of maintaining a legacy system and legacy software.

- As you upgrade or replace systems, consider maintaining a stand-alone PC as the system exists today. In other words, keep a current PC configured with the hardware and software in use today in a file storage location to be available for accessing current data files down the road. Original software programs, including the original recovery and restore disks should be kept in a safe place. Then, if years down the road the electronic data storage files being created today are no longer accessible on the then current system, you have a legacy system with which to access these files.
- Another idea is to store files in widely used formats such as tif or PDF because they will likely have a longer life span. Printer drivers that save files in a tif format are available from Informatik (www.tiffdriver.com) and they are inexpensive. An Adobe Acrobat program (files can be written in PDF format) is also available for under $200.

7. Misdirected Email: Most misdirection errors will not likely cause significant harm to the client. However, when you need to send your client some highly confidential information via email, and you aren't using email encryption, there is an alternative. Consider using an electronic "envelope within an envelope" approach to email transmission, and keep a record of the emails sent using this approach.

- The "envelope within an envelope" approach works as follows. The confidential information is sent as an attachment, and the text of the email contains only the email disclaimer language and information that identifies the intended recipient and specifies what the attached document is. If the email is mistakenly sent to opposing counsel, counsel is on notice that the attached document contains information not intended for counsel's eyes.

8. Delete is not Delete: Far too many computer users still mistakenly believe that deleting a file permanently removes the file from the computer, making it unrecoverable.

- Files that are deleted do remain on the hard drive. Deleting a file simply erases the file name and a "pointer" that directs access to the file's location. The "deleted" information may remain on the hard drive indefinitely if the computer does not need the space that "deleted" files occupy. Even reformatting a hard drive will not prevent recovery.
- To fully remove the "deleted" information from your computer, you must "electronically shred" the information. Overwriting the data with gibberish will accomplish this. The U.S. Department of Defense has established an electronic shredding standard known as DOD 5220.22-M. This standard requires that a file be overwritten seven times, using a different set of random data for each pass.

9. Failing to Take Care of What Antivirus Programs Miss: There are other types of programs that are potential security risks. Many people refer to these other programs as "malware."

- Most computer users are unaware of malware programs because they do not necessarily damage a computer system, and they quietly download from the Internet in the background and run in the background, usually without the user's knowledge. Malware programs come in different forms, and can include such malicious functions as password crackers, spyware that monitors your Internet activity and relays that information back to a third party, virus creation tools, and "adware" that creates those annoying advertisement "pop-ups" that keep appearing on your monitor's screen. Other types of malware programs enable a remote computer to monitor your machine or scan your computer network.
- PestPatrol, Inc (http://www.pestcontrol.com/) offers a software solution to the malware problem.

10. Delete is not Delete – Revisited: Unless deleted files are appropriately overwritten, they remain available for possible discovery. At the end of the day all network users must abide by a simple rule while on the firm's network or using any computer that might touch the firm's network such as a Blackberry, PDA, laptop, or home computer that is used for business even on a limited basis.

- The rule is this. If you are not comfortable having a personal or work related email read by a jury, an electronic note to a file read by the client, or your personal browsing history known publicly, don't write the email or note and don't visit the Internet site.
- Users are recording everything that they do on a computer and erasing a record once created can be extremely difficult. Worse yet, electronic erases leave their own record of events. Responsible use of technology is the safe play.

Post Conviction Motions to Vacate or Set Aside a Sentence Signal a Malpractice Claim for Ineffective Assistance of Counsel May be on the Way

By Senior Status Judge Stan Billingsley

Editor's Note: This article is one of a series that LawReader.com has agreed to provide for Lawyers Mutual's newsletter as a bar service. LawReader.com provides Internet legal research service specializing in Kentucky law. For more about LawReader go to www.LawReader.com.

Representing criminal clients is a dicey business. You can always expect that those sentenced to custody will consider filing an RCr 11.42 motion to vacate, set aside, or correct the sentence. Questioning your competence may be their only hope to avoid a prison sentence. In capital cases, you can expect the Department of Public Advocacy to assist in criticizing your work. The rule seems to be if all else fails, blame the lawyer.

"Every clarification breeds new questions."

Arthur Block

It is not unusual in such situations for a malpractice claim to follow an RCr 11.42 motion. For example, on June 10, 2005 the Kentucky Court of Appeals considered a case in which the defendant, after losing such a motion, claimed malpractice by defense counsel for ineffective assistance of counsel. This appeal suggests that an update on the standards for effective assistance of counsel in terms of malpractice is timely.

The first thing to consider is that in Kentucky, "The two-pronged test for ineffective assistance of counsel is: 1) whether counsel made errors so serious that he was not functioning as 'counsel' guaranteed by the Sixth Amendment, and 2) whether the deficient performance prejudiced the defense." *Martin v. Commonwealth,* (U) NO. 2002-CA-002529-MR.

Next, note that in June of this year the U.S. Supreme Court in *Rompilla v. Beard* (545 U.S.___, 2005 WL 14211390 (2005)) expanded standards for legal competence required of defense counsel. Defense counsel concluded from the client's and his family's statements that an investigation of his early childhood would have been counterproductive. The Court ruled he should have investigated regardless of the client's statements.

Finally, read the recent Kentucky Supreme Court decision in *Mills v. Commonwealth,* (No. 2002-SC-000216-MR, Ky. 05/19/2005). It provides a full discussion of RCr 11.42 issues and standards. The key points made are:

"*Strickland v. Washington*, 466 U.S. 668, 687, 104 S.Ct. 2052, 2064, 80 L.Ed.2d 674 (1984)…requires that Appellant show that his lawyer's performance was deficient, which requires showing that the lawyer made errors so serious that he was not functioning as the "counsel" guaranteed by the Sixth Amendment. Appellant must also show that the deficient performance prejudiced his defense, i.e., that there is a reasonable probability that but for counsel's error the result of the proceeding would have been different.

…

… a defendant is not guaranteed errorless counsel or counsel that can be judged ineffective by hindsight, but rather counsel rendering reasonably effective assistance.

…

… we must consider the totality of evidence before the jury and assess the overall performance of counsel throughout the case in order to determine whether the identified acts or omissions overcome the presumption that counsel rendered reasonable professional assistance.

…

An evidentiary hearing on an RCr 11.42 motion to set aside or vacate "is required if there is a material issue of fact that cannot be conclusively resolved, i.e., conclusively proved or disproved, by an examination of the record." *Fraser*, 59 S.W.3d at 452. See also *Newsome v. Commonwealth*, 456 S.W.2d 686, 687 (Ky. 1970).

…

Conclusionary allegations which are not supported with specific facts do not justify an evidentiary hearing because RCr 11.42 does not require a hearing to serve the function of discovery. *Stanford v. Commonwealth*, Ky., 854 S.W.2d 742 (1993).

…

A reasonable probability is the probability sufficient to undermine the confidence in the outcome. Id. at 694, 104 S.Ct. at 2068, 80 L.Ed.2d at 695. It is not enough for the defendant to show that the error

continued