

ETHICS IN THE ELECTRONIC ERA: AVOIDING THE ICEBERGS



Fairfax Bar Association
Bermuda

Sharon D. Nelson, Esq.
John W. Simek
Sensei Enterprises, Inc.
www.senseient.com
snelson@senseient.com
jsimek@senseient.com

ETHICS IN THE ELECTRONIC ERA: AVOIDING THE ICEBERGS

Technology makes everything easier and faster. In fact, it makes it possible to commit malpractice at warp speed. We can fail to represent diligently, lose our clients data, perform incompetently, and violate the rules regarding attorney advertising. All in sixty seconds or less. There are so many ways to potentially commit malpractice with technology that it is impossible to list them all. Still, let us make a credible stab at some of the more common missteps.

50 WAYS TO GET IN ETHICAL TROUBLE WITH TECHNOLOGY

1. **Use illegal software.** You know who you are. You buy academic versions of software and use them in your law office. You buy a single license for an application and install it on three computers, contrary to the license agreement. You find a neat piece of software that is free for personal use, and you use it on your law office computer. “Naughty, naughty” is all we’ll say, but the Business Software Alliance (BSA) will say far more. Potential liability for EACH copyright violation: \$150,000. Average out-of-court settlement: \$80,000. Have they been in our area? Yes, at least six times that we know of. Yes, they’ve come to law firms. They come with a U.S. Marshal and immediate ex parte authority to inspect your computers. If you are in violation of the copyright law at the time of inspection, you are toast. Intent is irrelevant. The moral? Make sure that you are properly licensed – and if you have a reasonable size firm, conduct an annual software audit. For heaven’s sake, have all the licenses in a single file.
2. **Give legal advice in your blog.** Blogs are not the place to give legal advice. Moreover, if someone in your firm has a blog, you need to be very sure that it conforms to insurance industry requirements. A great many insurers will not insure a law firm if anyone in the firm blogs and more and more are beginning to offer specific statements as to the kind of blogs they will – and will not – cover.
3. **Spam to market.** It is very tempting to market using some sort of bulk e-mail, but it simply is not legal to bulk market to folks who have no pre-existing business relationship with you. The CAN-SPAM act has done little to control spam, but for a law firm, both real spam and the appearance of spamming can be deadly. This is a sure fire way to get your domain name blacklisted. This has happened to multiple law firms in our area – and to courts!
4. **Get involved with a client via e-mail and give advice prior to the proper formation of a contract.** This is all too easy to do, especially since many lawyers now have their e-mail addresses up on the Web. It is important to get the retainer

agreement signed before the advice is the given, lest complications arise. Remember that your e-mail will leave a trail, so exercise extreme caution with anything that remotely seems like legal advice.

5. **Get in trouble with your state disciplinary board and decide to create your own defense by falsifying a document.** Lest you think this far-fetched, a Fairfax County attorney did exactly this. After a complaint was filed for failure to take any action in a case and letting the statute of limitations lapse, the attorney created a back-dated letter, purporting to show that he wrote the client closing the case, supposedly upon her specific instruction. The metadata that accompanied the document proved that the letter had been created two days before his response to the disciplinary board was due. He is no longer practicing law in Virginia.
6. **Keep slipshod trust account records.** The rules here are no different than they were in the paper world. We've seen attorneys who took in guns, jewelry, cars, etc. which were duly reported in their electronic trust accounts, but without any attempt at valuation. Moreover, the electronic records speak eloquently when attorneys fail to reconcile them, or dip into them when fees have not been earned. Worst of all are the many cases where attorneys put monies in the operational account, when they clearly should have been escrowed. If the firm uses a good accounting package, such as Quickbooks, any attempt to "fiddle the books" will be logged. Honesty remains the best policy.
7. **Send a document to a client to sign and don't PDF and lock it.** All too commonly, clients take it into their heads to alter a document sent to them by their lawyer. THEN they sign and send it back. Be careful – PDF and lock down all important documents – the exception is when you are working on drafts of a document, when it is easier to use Word and the "Track Changes" feature. However, once done, PDF and lock the document before it is sent around for signature!
8. **Miss a court date because the e-mail notice was trapped by your spam filter.** Don't laugh – this just happened to a respected firm in Colorado. The court was not amused by counsel's failure to show up and assessed sanctions against the firm, requiring it to pay for the opposing counsel's time. For heaven's sake, whitelist the domain of the court – and important client domains at well. Remember that you cannot shift the blame to a third party service provider, however much you might like to. Why? Because court rules say you can't.
9. **Don't proofread.** The difference between "I will consider a \$100,000 settlement" and "I will not consider a \$100,000 settlement" is vast. This is but one of many examples of how attorneys get in trouble by not proof-reading. At the very least, they often sound like hapless sixth graders who haven't got a grip on the simple declarative sentence, much less the spelling of fairly complicated words. You wouldn't send out a real letter that way – don't send out an e-mail that way. This is especially true if you use voice recognition software. Although the programs

are good at what they do, they are not perfect, by a long stretch – in fact, many judges cite the failure to adequately proof documents generated by voice-recognition software as a chief peeve.

10. **Open an attachment from someone you don't know or from someone you do know but where the circumstances are suspicious.** Dumb, even if you DO have a good antivirus program. Just because you have good, even great protection doesn't mean you can't be the first kid on your block to get a virus for which there is not (yet) an anti-virus signature to defeat it. E-mail addresses can be spoofed – easily. Therefore, if you get an e-mail from a client that contains an attachment and you were not expecting it – and there is no explanation in the text of the message that makes sense, don't open it. Call the client and verify that they sent you something.
11. **Go to a place on the Internet you wouldn't like Mom (or the Senior Partner) to know about.** This is precisely how spyware gets on your machines. Adult sites are particularly notorious for doing this, but many sites (even those with screensavers, computer utilities, recipes, etc.) do this to make extra money. Even a judge once called us after opening a “farm girls and their animals” e-mail attachment. He found himself trapped in an endless barrage of pop-up porn which refused to go away. Understandably, he was somewhat reluctant to call the courthouse IT staff. Enough said? ☺
12. **Use the Auto-Complete function with abandon.** This feature is so helpful and so potentially deadly. It is incredibly easy to let this function go and send an e-mail to someone other than the intended recipient. At best, the result is embarrassing. At worst, it is a genuine problem where you have perhaps sent confidential data to an unrelated third party or, the nightmare of nightmares, to opposing counsel.
13. **Use weak or non-existent passwords.** Passwords are critical defenses, so do not use your pet's name, your child's name or the name of your favorite sports team. Make your password complex, including numeric characters. A good tip is to do a short sentence that you won't forget.
14. **Write in anger.** An old chestnut, and still one to bear in mind. The unfortunate part of electronic communications is that when someone writes us something idiotic, we can immediately reply and point out the complete lunacy of what has just been transmitted. This is particularly tempting when a lawyer is under attack. Don't do it! Cool off. Go take a walk. Do anything other than reply immediately with words that cannot be recalled and may live forever and come back to haunt you! Remember, there is no “do over” key for e-mail.
15. **Hit the “Send” button quickly.** We're all so busy that hitting the send button promptly after composing an e-mail seems so natural. Done with this . . . on to the next thing. There is an inherent danger here. Look at the message one more

time – is it going to the right people? Have you proofread? Is there anything wrong with the tone or substance? Just pause a minute. Remember – each time you send an e-mail, you must see it on the front page of the Washington Post, on a billboard on Route 95, and in front of your mom’s face. If it can be in all three places without causing embarrassment or a problem, you’re probably ready to hit “Send.” Did we mention a warning about the lack of a “do over” key?

16. **Make it impossible to find your own files.** Files should be named appropriately, including the client name and the kind of document, perhaps the date. Having a good, descriptive name, you must now create a structure (one of your own or through a case management system) that makes it easy to find what you are looking for. If you do not have a case management or document management system, make sure that you have electronic files named by client, with descriptive titles for each file, including the client name in case you mistakenly move the file to another folder.
17. **Rely completely on your computer calendar.** So what happens when your Internet goes down? Or your server crashes? The authors are devoted adherents of the tech world, but it is always prudent to have a secondary calendar that can provide a fallback measure.
18. **Leave your computers on at night.** Are you nuts? Do you personally know each member of the cleaning crew? Can you vouch for each of them? Robbers who broke into an entertainment complex in Colorado recently found themselves unable to open the safe even though they had the code. Perplexed, they looked around and found a computer that was on and Googled information about the safe. Moments later, the safe was open and they left with \$12,000 – so you see, it is very helpful to have computers on at night – helpful for all the wrong sort of people.
19. **Don’t change the defaults.** Every script kiddy and macho hacker knows the defaults of all common computer-related devices. In fact, they are posted on the Internet. If you don’t want a burglar in your house, you always, at a minimum, lock the door. Changing the defaults is locking the door.
20. **Don’t secure your wireless network** – at home or at work. Wherever you work, your wireless network should be secure. This means that you must change such things as the SSID and the default admin password. Disable the advertisement of the wireless network and enable some sort of encryption for the cloud. Create MAC filtering rules to limit connections to those that are predefined. After all, you shouldn’t be in the business of creating the neighborhood hotspot.
21. **Don’t have adequate anti-virus and anti-spyware software.** This is “bare bones” protection these days. You should have one good anti-virus solution and preferably two anti-spyware solutions these days. If you have a subscription, don’t let it lapse.

22. **Don't backup – and almost as bad – don't do “test restores” of the backups.**
Most lawyers should be doing incremental (or differential) backups daily and full backups at least weekly. If you're doing less, think again about the potential danger. Also, backup media fails over time, so don't assume that you have a good backup without doing periodic test restores. In case after case, we've seen lawyers rely on backup tapes only to find that they were corrupted when disaster struck and those tapes held the only backup of the law firm data. External hard drives increase reliability, but should also be changed in rotation just like tapes.
23. **Use an online backup system.** This one is controversial. There is nothing inherently wrong with an online backup system from a technical standpoint. WE hasten to add that we have seen several total failures when it comes to restoring backup from online backup providers. Even in the best scenario, someone else is holding your data. What will you do if they belly up? What if they have a disgruntled employee who sells your data? What kind of REAL recourse is there in a situation like that? At the very least, encrypt the data before you send it offsite!
24. **Don't have a disaster recovery plan.** Do you think the lawyers caught in Katrina ever imagined that they would face a disaster that was so large it would involve both their home and office? Many of them had backup media at home and lost that media as well as the computers/server at work. This was compounded by not having power or cell phone towers. The communication breakdown was further aggravated by food and water shortages, office buildings being declared closed by authorities, etc., etc. In our world, where natural disasters present plenty of hazards, the ante has been upped by our realization that no one – anywhere – is safe from acts of terrorism as well. Many of the Katrina lawyers lost their practices forever because they were not sufficiently prepared. When it comes to disasters, an ounce of prevention is indeed worth a pound of cure.
25. **Fail to have an employee termination policy or fail to follow it.** We sometimes chuckle that the only way to have a safe employee termination is to issue a blindfold and cigarette and execute the employee. Our cynicism comes from the number of ex-employees who have caused technological havoc by accessing the law firm network once their authority to do so has expired. When you are ready to terminate someone, never let them have access to their computer post-termination. Immediately cut all access to your systems from the outside and forward all of their business e-mail to someone else. Collect all their keys. Change the security codes if necessary.
26. **Have a laptop without a power-on password, encryption, or biometric access.**
In a world where laptops are the #1 stolen item at airports (and they rank in the top five at hotels, from cars, etc.), you must take precautions. The new “finger-swipe” biometrically accessed laptops are no longer out of anyone's price range. Encryption of the data is no longer difficult. At the very, very least, make sure no

one can get on your laptop at all without that power-on password. It is surely malpractice not to take this most elementary of precautions.

27. **Put client data on an unencrypted thumb drive.** Look at the size of a thumb drive. Smaller even than our now very small cell phones. How often do we lose cell phones? About 50% of us have lost one at one time or another. Here we have an even smaller device. It is critical that data on a thumb drive be protected either by requiring a password or by encrypting a portion of the drive which carries client data.
28. **Have client data on a cell phone that doesn't require a password.** As our business frequently forensically images cell phones, it always strikes us as remarkable how few cell phones we see that require a password. It may well be that we are simply the "hurry up" generation that doesn't have time for that extra step, but if there is client data on the phone, it certainly seems like we **MUST** take the time to ensure that client data cannot be accessed if we accidentally lose our phones in a cab!
29. **Don't scrub the metadata.** It is impossible to overstate the importance of this. Court briefs have actually been filed with metadata intact. In one memorable comment, an attorney asked if anyone thought that the "yo-yo brain judge" would understand what was being argued. As you can imagine, the judge was not amused as he viewed the comment in the electronic document. Our favorite metadata scrubber is Metadata Assistant, by Payne Consulting (about \$80 per seat). www.payneconsulting.com. Already own Adobe Acrobat? Convert your document to PDF and that will strip out almost all the metadata, usually everything you'd care about. Can you look at the metadata in opposing counsel's documents? The ABA says yes, New York says yes, Florida says no, and Virginia hasn't spoken. We agree with the ABA opinion (Formal Opinion 06-442).
30. **Redact PDF with black boxes.** Even the federal government has pulled this gaffe, thus exposing the placement of troops in Iraq. More notable to the legal community, a law firm involved in the infamous suit against AT&T for intercepting citizen e-mails and sharing them with the government made the same error in one of its briefs. Ordered by the court to release some documents but with certain sensitive information redacted, the firm clumsily used black bars to do so. Journalists promptly pounced on the black boxes and stripped them out, revealing incredibly sensitive data which seemed to confirm the allegations of the Electronic Freedom Foundation. If you are going to redact information, use professional software such Redax or upgrade to Acrobat 8.0, which includes redaction and Bates stamping ability.
31. **Donate your old computers to charity (or otherwise dispose of them) without wiping the hard drives.** As much as you'd think this was obvious, every time a college student does a new study with hard drives purchased on eBay, they find law firm data. If you have someone who is IT competent, it is a simple matter to

wipe the drives effectively. If you do not, it might cost you \$100 per drive to have it professionally wiped. A small price to avoid a big security hole.

32. **Be a “chatty Kathy” online.** We have become a society of online chipmunks, happily chattering away in chat rooms, in blogs, on listserves, and via IMs and e-mails. You should assume, at all times, that whatever you transmit electronically will live forever. Remember, deleted isn’t deleted and the power of computer forensics to recover deleted data is fearsome. If you don’t want to answer for what you’ve written three years later, don’t send it!
33. **Don’t have an Internet and e-mail usage policy for your office.** Are you daft? Do you know what these people do, especially when you are not in the office? All of the things we tell you not to do in these tips is exactly what they will do. They will check what’s going on in their soap operas, visit the celebrity gossip columns, etc. Not to mention the temptation to post things on a listserv (with your law firm signature attached of course) that may not be precisely the representation of your firm that you would choose. Make a policy and then enforce it.
34. **Don’t have a policy about what data may and may not leave on removable media (thumb drives, iPods, phones, PDAs, etc.** This is precisely how much of your confidential data leaves the office. If they don’t e-mail it, they download it. So have a policy – there are even utilities to help you monitor anything being downloaded via USB drives.
35. **Don’t train your employees about computer security.** There are few ways to get more “bang for the buck” than by training those who work for you. Most of them don’t know how to spot a phishing attack – or how to recognize social engineering over the phone that might persuade them to give up a password. Give them the benefit of safe computing training and policy training and you have built a worthy moat around the castle which contains your client information.
36. **If you have a disgruntled employee you’re thinking about firing, don’t think too long.** This is a common scenario – you know you have someone who is angry or disgruntled. Perhaps you didn’t give them a raise, perhaps they don’t like your demeanor – the reason doesn’t matter. Once you are aware of a potential problem, the likelihood of misconduct increases exponentially. As soon as you have your “employment law ducks” in order, let them go. If they do any work on your network whatsoever, this is an especially firm rule. As one law firm system administrator boasted, “I can bring this firm to its knees anytime I want.” Believe him, for he speaks the truth!
37. **Fail to encrypt your e-mail.** OK, this is a red herring. No one requires encryption. Very few lawyers use it. It isn’t hard, but it takes a little extra time. Still . . . the real message here is that important things (such as proprietary data)

should not be transmitted electronically without being encrypted. Think before you use e-mail!

38. **Converse via e-mail with your client using the client's work e-mail.** This is always a troublesome area, since it is not yet fully clear whether the attorney-client privilege will apply to e-mail sent from a work machine, whether via a work e-mail address or a personal e-mail address. In at least one case in Virginia, the judge found that there was no privilege between attorney and client for anything sent from a work computer. Period. As experts, we believe that decision was wrong, but that doesn't change the current practical implications for lawyers. Better reasoned decisions from other states have indicated that the privilege would not be lost if the client took reasonable measures to protect the privilege (e.g., not using the work e-mail address, keeping attorney-client e-mails segregated on the hard drive in an appropriately named folder).
39. **Fail to address e-mail correspondence in your retainer.** Given the paragraph above, the perils of e-mail correspondence should be evident. Many lawyers believe, and we agree, that there should be a separate paragraph in your retainer pertaining to e-mail, in which the client specifically agrees that e-mail communication is acceptable or not acceptable. It should discourage the client from communicating from work and also stress the importance of not divulging sensitive data in e-mail. A number of lawyers, including one of the authors, makes sure that this paragraph is separately initialed so that it is abundantly clear that the client understood potential risks before using e-mail as a vehicle of communication.
40. **Have a file sharing program on your computer or network.** C'mon, fork over the money for the new Elton John CD. Or for the new "Harry Potter" movie. File sharing of protected works not only constitutes copyright infringement, but it leaves your computer/network wide open to the Internet. If you have kids at home, and work from home, you may not even be aware that your kids have installed file sharing programs. We have six kids, and yes, it happened to us. Forewarned is forearmed!
41. **Enable file sharing between the workstations at your office.** This is a tough one. Microsoft allowed peer-to-peer file sharing among Windows computers. Disable this feature if you have a server. Small offices will use file sharing to keep costs down and still allow access to client data from multiple computers. If you must use file sharing, limit and restrict the access. Require user IDs and passwords to get to the data. Don't configure unrestricted access to your data since that's what the hackers love.
42. **Use copyrighted images on your website without a license.** This is done all the time. It is incredibly simple to get royalty-free clip art or photos on the Internet. If you want something classier, the prices to get a license are generally quite modest. Folks are searching for infringing materials on the Net all the time these

days and there are sophisticated tools to help them. Don't help the infringement bounty hunters!

43. **Call yourself a specialist or an expert on your website.** Come on, we know you've read Virginia's advertising rules. You know better.
44. **Appear to promise results on your website.** See number 43 above. If you even describe results of cases, you must explain that results are dependent on individual fact scenarios and state that case results do not guarantee or offer a prediction of the same result in another case. It must do this in bold type, in caps, and in a font size as large as the largest size font used to describe the case results. See Rule 7.2(a)(3).
45. **Don't have a disclaimer statement in your e-mail.** This entry is here under protest. It is probably a good idea to have one, but most experts agree that disclaimers are pretty worthless and provide almost no protection. However, it is nice to put in the tagline that tells people what to do if they receive an e-mail message in error. Remarkably enough, most folks actually want to do the right thing and will tell you that they received your message in error. All things considered, it is better to know than not to know!
46. **Decide you don't need to know about electronic evidence.** Sorry, but this is no longer possible. You can no longer make a deal with the opposing counsel that "I won't go there if you won't." In a world where 95% of the data is created electronically and only a fraction of it is ever reduced to paper, you have no choice but to consider whether ESI (electronically stored information) may be a part of your case.
47. **Mishandle or spoliage ESI.** Until recently, lawyers were getting away with this on a regular basis, but no longer. Judges have had enough, and are beginning to hand out sanctions like penny candy, mostly against clients, but now and again against the law firm as well. You must understand your client's technology well enough to avoid spoliation and to determine where relevant evidence may be in order to preserve or produce it. If you are not up to speed, it is time to get there.
48. **Violate password protected data.** Outside of the workplace (where employers have the right to monitor what transpires on their networks), passwords create a right of privacy. It doesn't matter who owns the computer. The right of privacy applies between spouses as well. Why? Because the law says so. If we had a \$1.00 for every time a spouse argued that they had the right to search their partner's e-mails, we would be rich. If you, as an attorney, violate this right, you too are guilty of a crime. Interception is prohibited under the federal and state wiretap act – any other form of accessing private data is prohibited under the Virginia "unauthorized access" statute. You may "freeze" the data (either party in a marriage can make a backup, after all) but you may not access it without consent of the party or a court order.

49. **Accept or use telephone records obtained by pretexting.** This is against the law in Virginia. If you know the records have been obtained by pretexting when they slide those records across the desk and you nonetheless take them, you have violated the law.

50. **Counsel your client to put a GPS tracking device on someone's car without fully knowing the facts.** These gadgets provide great evidence, but in the state of Virginia, it is illegal to put a GPS tracker on a vehicle unless you are that vehicle's owner. There are no reported cases thus far, so we cannot tell you whether it is ok to put a GPS tracker on a car which both parties have purchased but which is still owned by the bank because there is a car loan. These are not dice we wish to roll.

This list could go on and on and on . . . but hopefully, it is clear that there are significant dangers in the electronic world, waiting to trap the unwary lawyer. Here, at least, is a good starting point for making sure you've covered as many ethical bases as you can.

Want some extra help? Go to www.legalethics.com, www.abanet.org/cpr or www.findlaw.com/01topics/14ethics/index.html

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