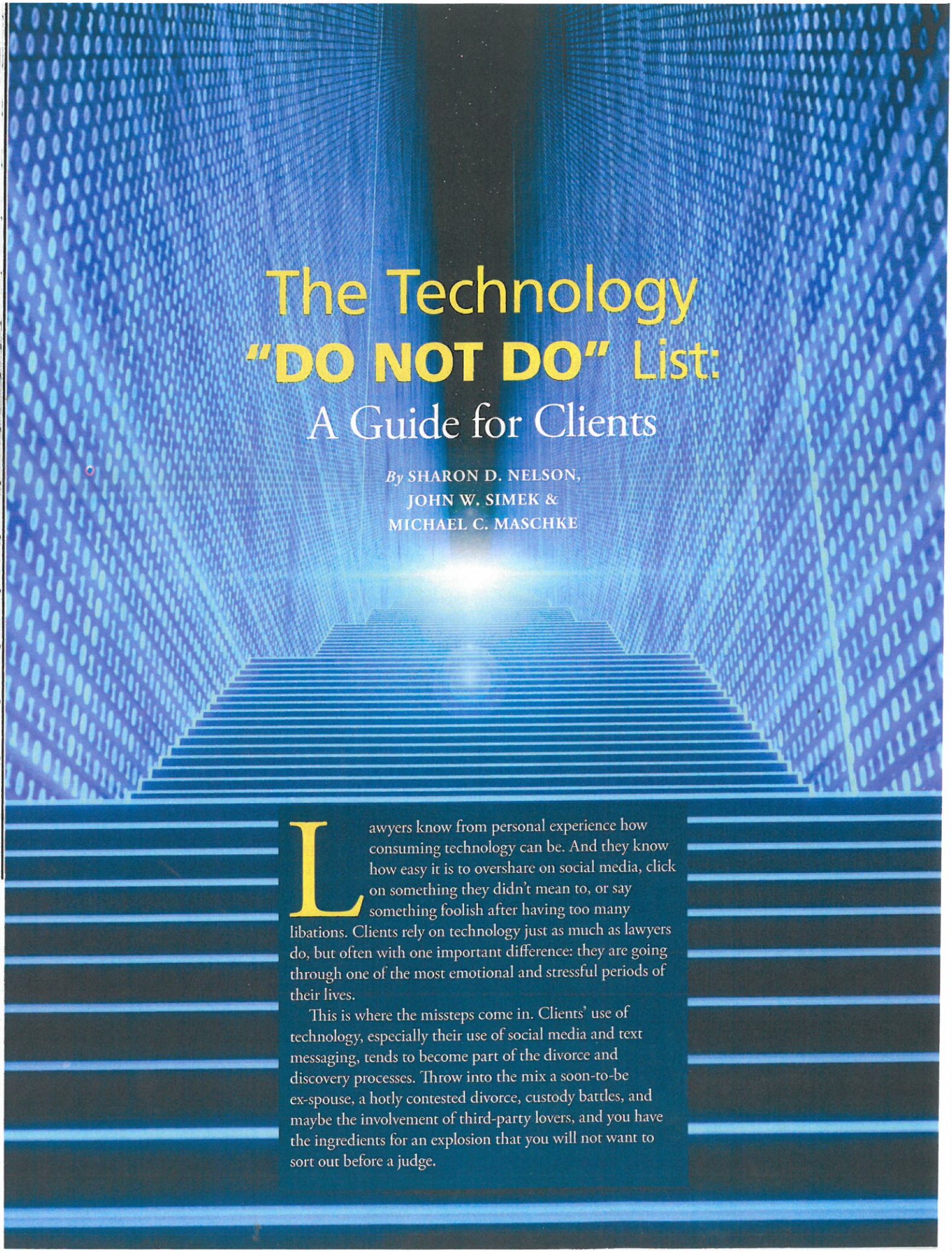

The Technology "DO NOT DO" List: A Guide for Clients

By SHARON D. NELSON, JOHN W. SIMEK & MICHAEL C. MASCHKE

Lawyers know from personal experience how consuming technology can be. And they know how easy it is to overshare on social media, click on something they didn't mean to, or say something foolish after having too many libations. Clients rely on technology just as much as lawyers do, but often with one important difference: they are going through one of the most emotional and stressful periods of their lives.

This is where the missteps come in. Clients' use of technology, especially their use of social media and text messaging, tends to become part of the divorce and discovery processes. Throw into the mix a soon-to-be ex-spouse, a hotly contested divorce, custody battles, and maybe the involvement of third-party lovers, and you have the ingredients for an explosion that you will not want to sort out before a judge.

The "Do Not Do" List

Happily, at the onset of the engagement, you can help clients protect themselves from technology missteps. Advise them to follow the technology "do not do" list.

We live in an extremely over-shared world. People often feel compelled to post videos and pictures of everything they do, believe in, or feel at any given moment. Opposing attorneys know this better than anyone. They regularly use the goldmine of information found on social media to bolster their cases. Too often clients post information that may be harmful to their cases, such as photos of their most recent blind date at a local winery or their spur-of-the-moment extravagant trip to Bali for a little "R & R." Surely your client will be asked about these activities should opposing counsel get hold of the posts, and instead of just being innocent, shared posts, they are now evidence that your client is an adulterer, a drunk, and a hider of assets. After all, how could your client afford that luxurious trip? Who was your client's companion?

Do Not Stay on Social Media

The best technological advice you can give your clients is to stop using social media accounts entirely. It might be hard, but quitting cold turkey could be the best thing they do to help their cases. Many social media providers such as Facebook and Instagram allow users to disable, rather than delete, accounts, so that after the divorce is finalized or the ink has dried on the settlement papers, your client will be free to post again, however unwise their posts. And clients who disable or deactivate their accounts rather than deleting them will not face accusations of spoliation.

Do Not Access

Switching gears for a moment, we want to discuss something that most clients lose during the divorce process—common sense. Clients are often willing to go to immeasurable lengths to get information on their soon-to-be ex-spouses to help strengthen their negotiating positions or to gain any perceived upper hand in the process. These efforts may include breaking the law. Accessing a password-protected account belonging to the other party, especially when there is an expectation of privacy, should be discouraged at all costs. There are legal routes to obtaining the same information, and these should always be the paths taken. Some examples of accounts that should never be accessed include the other party's:

- new (nonmarital) bank account, credit card account, loan records, or stock trading account;
- personal or business email accounts;
- social media accounts, such as Facebook, Instagram, and Snapchat; and
- Apple iCloud accounts (www.icloud.com).

It is always important to obtain information legally to keep your client out of hot water with the judge and the law. And no, the "accounts are shared" excuse is not a get-out-of-jail-free-card. Your client better have a good criminal defense attorney on speed-dial if he or she ignores these warnings.

Do Not Borrow or Steal

While we are on the topic of "doing things the right way," your clients should never steal or "borrow" the other parties' personal devices to have them analyzed by digital forensics companies or private investigators. Again, there is a right way and wrong way to do this. As their attorney, you can request the devices and information contained on them through the discovery process via a subpoena or court motion. Having your client steal the devices in the dead of night to have them covertly inspected (or worse, to install spyware) is not the best course of action. More on spyware in just a bit. Having said that, there is no blanket restriction on making a forensic copy for preservation purposes. You just can't go snooping around before getting court approval or agreement of the device owner.

Do Not Remain Ignorant of the Law

While any respectable digital forensics company would immediately inform your client of the limitations of the work it can legally perform, your client is better off being educated beforehand. Generally, a marital device can be forensically (and legally) copied or preserved, and that may be all that can be done at that moment without further authorization from a court to access "password-protected" materials. The marital device can be forensically imaged in the same way that either party could legally make a backup of the device or its data. But if one party has a password-protected email or any other sort of account on the marital computer, the laws protect the privacy of that data. Installing spyware, cracking or guessing passwords—all of that is not permitted.

Shopping around for someone to get you "all of the data" from a device regardless of its legal protections will only lead to more problems, including inadmissibility problems, and yes, possible criminal charges. While attorneys can explain any state-specific "gray areas" to their clients, the best advice is to respect the privacy of password-protected data unless there is an agreement with the other party to grant access or a court order authorizing access.

Do Not Spy or Hack

In the realm of divorce, clients often resort to spyware, hacking, interception of communications, and electronic monitoring. These should always be avoided. Your client should never install software on a computer system or mobile device to monitor a former (or soon-to-be former) spouse's activity. He or she should never modify the settings of an email account to auto-forward messages. The list of things clients should not do to monitor a former partner is a mile long.

One of the more popular mechanisms these days is the

Find My iPhone feature of a jointly used Apple iCloud account, which tracks the other party's movements and location. This usually works when one party isn't aware of what an iCloud account even is or which device is set up to use it! Sharing iCloud accounts is a big no-no in our book. Not only can a spouse track his or her partner's location within a few feet, but any messages, emails, photographs, videos, and other application data may be accessible as well, especially if the iCloud account is being used on multiple devices. If your clients use an Apple iPhone, iPad, or Mac computer system, we recommend that you instruct them to disconnect any previously configured iCloud account and create new ones for their new life. They can accomplish that through device settings or www.icloud.com.

One of the more interesting scenarios we have encountered involved a client who used a Google Nesr security camera installed at a jointly owned rental property to monitor the soon-to-be ex-spouse. The spouse was allegedly dating the renter. The monitoring enabled the client to catch his spouse committing adultery, which he thought would lead to a quick resolution and settlement of the divorce. Instead, there were more headaches for the client, including another civil suit and a pending criminal investigation. Was it worth it? The client probably doesn't think so now. If you don't know the legality of your client's actions, it certainly wouldn't hurt to err on the side of caution and save the client future self-inflicted heartburn.

Do Not Post Revenge Porn

Not every divorce is desired by both parties. Sometimes your client's hand is forced by the actions of the other party. One thing that your spurned client should not do is take revenge— either physically or online. Sadly, we have seen a significant rise in revenge porn cases.

More and more spurned partners have turned to the idea of "getting back" at their former spouse by posting on the Internet private photographs and videos taken or received through the previous relationship. There are now many websites dedicated to revenge porn, so this trend should not come as a surprise. As more victims have sought legal recourse for these actions, forty states currently have laws banning revenge porn, while other states have harassment laws that may be applied to seek justice for the victims in these criminal matters.

Some people believe they can get away with this type of conduct without having the evidence traced back to them, but in reality, they are setting themselves up for criminal charges. The websites used to upload and post these types of photos maintain logs that can help to identify where the activity originated from and, ultimately, who uploaded the photos or videos. Internet service providers, including mobile carriers, also maintain logs. These logs cannot simply be deleted by your client, so it would be best to advise them against any type of revenge activity from the onset of the engagement.

Do Not Delete

Another potentially criminal action that we often consult on is spoliation. The intentional deletion of potentially relevant data can derail your client's divorce case. It's far better for data to be properly preserved, searched, and produced than to have to explain to a judge why your client was deleting emails or text messages in violation of a discovery order, subpoena, or document request. The problem for clients is that there are digital forensic companies that can recover deleted information and produce it in court. There may even be evidence to recover that shows who deleted the information and exactly when it was deleted.

We've been involved with many matters in which evidence has shown mass purging right before the date a party was required to produce evidence in response to a subpoena or court order. We have also seen Internet searches for how to successfully delete text messages or emails. Boy, do the judges love to see those searches! They are equally incensed to hear how a phone mysteriously was stolen or lost right before being requested for analysis. We've received countless phones that have been water damaged, factory reset, or just plain lost, immediately prior to a court deadline to produce them. Needless to say, this practice is frowned upon and may lead to some serious legal consequences for your client. Oh, and don't think that replacement of the phone with another model or an identical model can't be determined through analysis. No matter what, hiding, destroying, or otherwise obstructing the discovery of evidence will not result in a good outcome in court.

Do Not Romance on Secured Apps

Protecting privacy and personal communications is important to most people. However, installing an application on your phone or computer that offers secure encrypted communication may not be a good thing, especially if the intent was to securely communicate with a paramour. Signal, WhatsApp, and Telegram are several apps used for secure communications. Even though you won't be able to obtain the content of the communications, you may be able to retrieve contacts, dates, and times of the communications. Technically, there is nothing wrong with using these secure communications apps. However, if the paramour's ID is found on your spouse's phone and the paramour has also installed the same app with your spouse's ID, the inference may be all it takes to sway the court.

Do Not Jeopardize Your Case: Use the "Do Not Do" List

Now that we have spent some time reviewing technology missteps—why should your clients listen to our advice?

Roughly twenty-five percent of our digital forensics cases are family law matters. We've seen firsthand the trouble clients get into when they access accounts without authorization. We've seen lawsuits filed in response to the

installation of spyware or use of a security camera to remotely and surreptitiously monitor a former spouse. We've seen the weight of evidence lessened due to the manner in which it was obtained. There have even been occasions where a party has been jailed due to the spoliation of evidence. These things are rare, but we've seen them happen.

Judges have little or no tolerance for your client's foolish or illegal actions. They have zero tolerance for your client lying to the court. A little stern guidance at the outset of an engagement can benefit clients greatly—if you can get them to listen, which is sometimes challenging. It is certainly worth the effort to try. You would hate to have a misstep affect the outcome of a custody or spousal support battle.

We have all become too reliant on technology in our day-to-day work and personal lives. Even during some of the most stressful situations your clients will ever face as they go through the divorce process, they need to maintain (instead of lose) their common sense when it comes to the usage of technology. The legal consequences of missteps are real—and often devastating. FA

SHARON D. NELSON (snelson@senseient.com), JD, is president of Sensei Enterprises, Inc., www.senseient.com, a cybersecurity, information technology, and digital forensic firm based in Fairfax, Virginia. She concentrates her practice on electronic evidence law and is the coauthor of numerous books on cybersecurity, including *Locked Down: Practical Information Security for Lawyers* (ABA, 2016) and *Encryption Made Simple for Lawyers* (ABA, 2015). She has long been an active leader of the technology-related committees of the ABA and other bar associations.

JOHN W. SIMEK (jsimek@senseient.com), who holds engineering and MBA degrees, is the vice president of Sensei Enterprises. He is a digital forensics technologist who holds the Certified Information Systems Security Professional (CISSP) and EnCase Certified Examiner (EnCE) designations, as well as others. He testifies as an expert witness throughout the United States, has coauthored books with Sharon Nelson and others, and frequently speaks nationwide on information security, legal technology, and electronic evidence.

MICHAEL C. MASCHKE (mmaschke@senseient.com) is CEO of Sensei Enterprises. He holds the EnCE and other certifications and is experienced in network troubleshooting, design, and implementation, security systems integration, and computer engineering. Before assuming his current role, he oversaw Sensei's digital forensics and IT departments, which provide support to more than 200 area law firms, corporations, and other organizations. He, too, is a coauthor and speaker on cybersecurity topics.

Expectations of Privacy

continued from page 13

what is a relatively common behavior. The question that you have to ask is less about whether you will be criminally prosecuted and more about the goal of the recording. If your client is being threatened, a recording of the threat, particularly when there is more than just the bare bones of a threat, can support a criminal action or an abuse restraining order.

There are also times when your client's child is telling him or her about something such as physical abuse that happened, and your client wants to record what the child is saying in order to report it to the police. This is an appropriate use of recording, assuming that you are not asking leading questions, thereby contaminating the reporting. However, if your client engages in a pattern of recording the child's statements, a judge might view the pattern as being psychologically damaging to the child because it puts the child in the middle of a parental conflict. Moreover, if there is a pattern of recording the child's statements or a habit of recording openly every transition between parents, a judge might admit recordings because the potential for harm in requiring a parent to wait to capture that one bad act would outweigh the risk of psychological harm to the child from being recorded. The reality of video and audio recordings is here to stay. It is an everyday reality, and every parent has to evaluate whether recording would be intrusive in a way that affects the psychological well-being of his or her child and to decide, therefore, whether it should or shouldn't be used.

Be Aware—Be Very Aware

You wouldn't want to induce fear of using technology to record, but recording should be done with an awareness of its risks and goals. Be very aware, also, of what the laws are, what the pitfalls are, and what the benefits of audio and video recording are. After all—paranoia is a heightened sense of awareness, and just because someone's paranoid doesn't mean they're wrong. FA