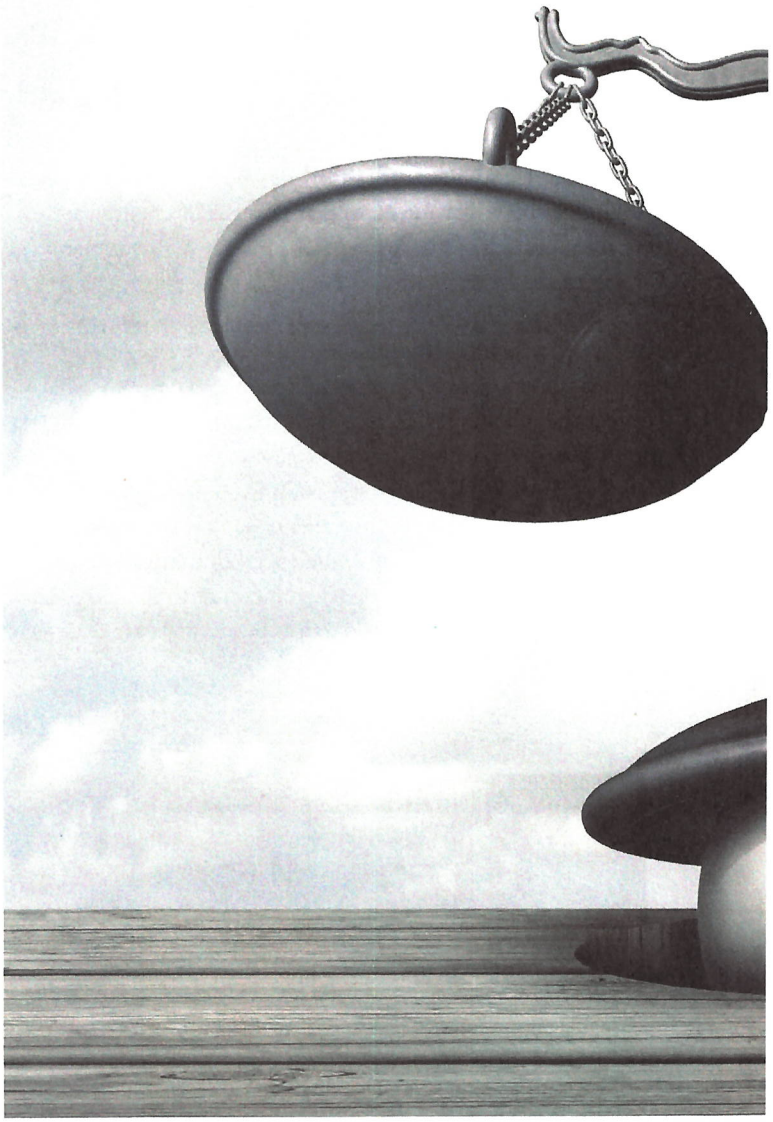
Tech Ethics Challenges for Family Lawyers Abound

By DANIEL J. SIEGEL & THOMAS G. WILKINSON



Technology is a part of every aspect of every lawyer's practice. From smartphones to email to social media, technology issues abound.

Family Lawyers Face Special Tech Challenges

Family lawyers face some special challenges, however, because they must deal not only with office technology but also the ethical concerns created by clients who neither know nor care about the rules governing their lawyers' conduct. Family law clients typically want to win at any cost because their objectives include punishing their spouse. And not surprisingly, they often expect their lawyers to share that goal and a willingness to engage in ethically questionable tactics to achieve the desired outcome. This article will highlight some of the ethical/technological issues facing family lawyers and review some best practices for dealing with them.

One example of those issues occurs when a client reveals he or she is using an app that spies on and tracks a spouse or other person. A family lawyer should be familiar with state and federal wiretap laws and pertinent ethics guidance and be prepared to offer sound advice. If you don't believe how prevalent these apps are, just perform an Internet search for "app for spying on spouse." There were 836,000 results in July 2018 for this topic, and these included numerous sites that test and evaluate the efficacy of these apps.

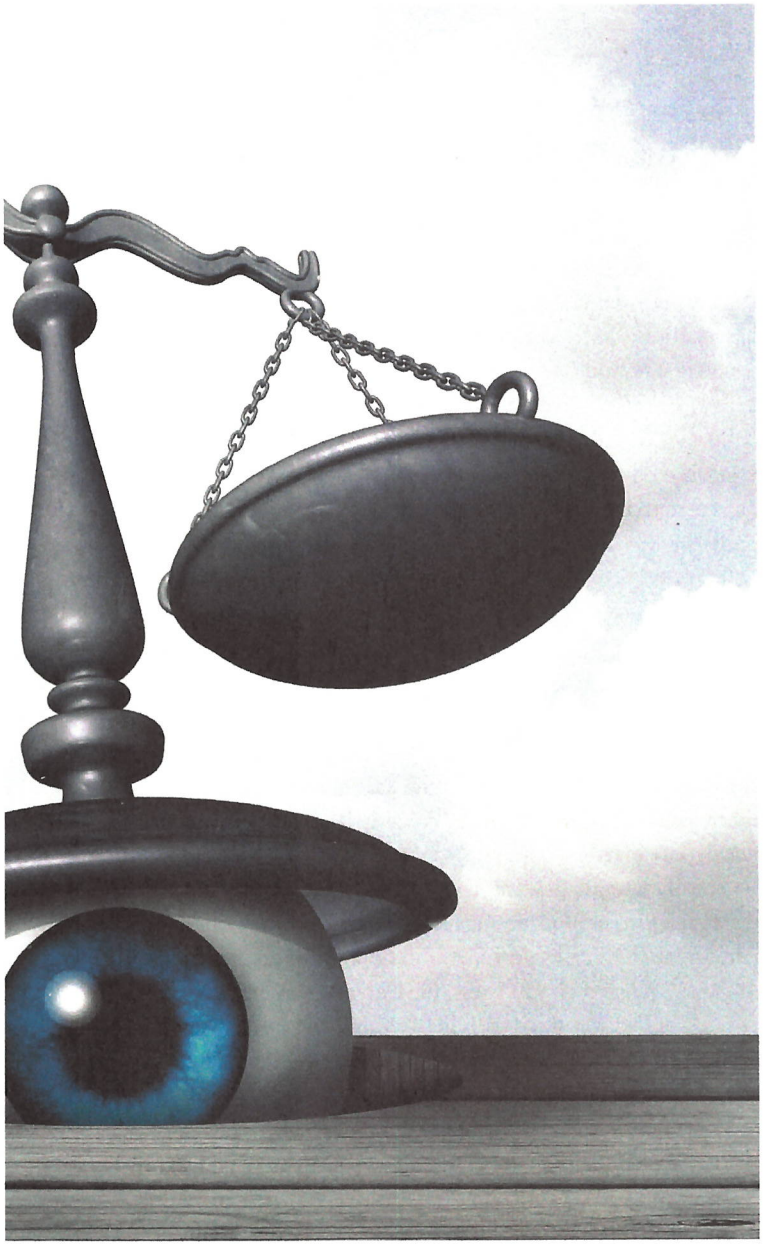
Knowing about these programs and apps means that you will be prepared when a client explains that she uses software to monitor her estranged spouse's calls, text messages, email, Internet history, and GPS location and declares that "he'll never find out about it, and don't you say anything or you're fired." Or, when a client separated from his spouse explains that he still logs into his wife's email and Facebook accounts because "hey, she was dumb enough not to change the passwords," you cannot shrug your shoulders and remain silent. Nor can you simply send an email to a client containing confidential communications without assuring the client that only he or she can view the contents, including the attachments, and explaining that a spouse cannot just walk up to the computer and access every communication. These situations happen all too often.

With technology evolving, you cannot plead ignorance or look the other way after discovering that a client is engaging in conduct that may place you in ethical hot water or be illegal in many states.

While you cannot ignore your clients' wishes, you must balance them with your ethical obligations under the Model Rules of Professional Conduct. *The Rules mandate that lawyers recognize the risks and benefits of technology and take appropriate steps to prevent unauthorized disclosure of confidential information.*

Rule 1.1: Competency

Any analysis of a lawyer's obligations begins with the Model Rules of Professional Conduct. As of November 1, 2018, which is when they went into effect in California, they have



been adopted in some form in every state. (Because this article addresses these issues generally, it will focus on the Model Rules rather than state-specific variations of the Rules.) At the center of these technology-focused obligations are Rules 1.1: Competence and 1.6: Confidentiality of Information. In addition, Rules 5.1: Responsibilities of a Partner or Supervisory Lawyer; 5.2: Responsibilities of a Subordinate Lawyer; and 5.3: Responsibilities Regarding Nonlawyer Assistance require attorneys to ensure that staff and the outside firms they work with also understand the need to preserve client confidentiality.

While many aspects of the Rules address or touch upon technology, the 2013 amendment to the Comment to Rule 1.1 is generally considered the most significant because it explains that "[t]o maintain the requisite knowledge and skill [necessary to be competent], a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology." This Comment codified the underlying assumption that to be competent, lawyers must understand and address the technological issues arising in their practices. These issues could range from confidentiality of communications to utilizing technology at hearings to effectively presenting a client's case to a judge or other fact finder.

A total of thirty-four states now impose an ethical duty of technology competence. Some states are going further than incorporating the recent Comment to the Rule 1.1 definition of competence. For example, Florida now requires attorneys to take three hours of technology-based continuing legal education courses every three-year reporting period. In addition, the Pennsylvania Bar Association has requested that the state supreme court require attorneys to take one hour of technology-based CLE every two years. The North Carolina State Bar has also requested that its state CLE requirements be modified to require one hour per year of technology training.

For family lawyers, such mandatory CLE could focus, for example, on teaching attorneys how to educate clients about the risks and dangers of posting personal information on social media websites, or on why and how cellphone communications and text messages are not necessarily confidential. Alternatively, they could focus on topics ranging from cybersecurity to email encryption to digital signatures. In practice, numerous possible courses could fit the definition of a technology-based CLE, and many would also qualify for ethics CLE credit.

Rule 1.6: Confidentiality of Information

Hacking, ransomware, email snooping, and old-fashioned carelessness are among the ways that attorneys negligently or inadvertently disclose sensitive or confidential client information, not only about their clients but also about other parties and witnesses in each matter. For example, in Pennsylvania, family law case records were available online and unredacted in some counties. This meant that sensitive information such as children's medical records, credit card numbers, drug testing results, and other data were publicly available via some court websites. The Pennsylvania Supreme Court adopted a study committee's recommendations and precluded public disclosure of family law–specific documents. Now, Pennsylvania lawyers must separate confidential documents in their court filings and redact precluded information, and the failure to do so could result in lawyer discipline.

Lawyers have always had an obligation to "not reveal information relating to the representation of a client" and to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to a client" under Rule 1.6. With more courts adopting policies such as Pennsylvania's and many jurisdictions adopting data privacy laws, family lawyers must now take additional care to make sure that neither confidential client information nor sensitive information about others is ever publicly disclosed.

Tech Security Measures for the Modern Family Lawyer

Do you leave client files in your reception area where anyone can look at them? Of course not. You store them in file cabinets where only attorneys and staff can view them. The same applies for electronically stored (also called "digital") records.

This means that law firms need to store all data on secure servers or computers where only the people who need to view the information can access it. They should also install appropriate security, including encryption, which is a process that converts data into a form that prevents unauthorized persons (hackers) from viewing the information. When the information is particularly sensitive, firms should take additional steps to assure the information's security by first asking:

- How sensitive is the information?
- What is the likelihood of disclosure if additional safeguards are not used?
- Does the client require that the firm employ additional safeguards?
- What is the cost of employing additional safeguards?
- How difficult will it be to implement the safeguards?

In many cases, the software on your server may have encryption capability. For example, Windows Server 2016 software includes encryption technology that protects data at rest, such as BitLocker full-volume encryption and Encrypting File System (EFS) file-level encryption.

If this sounds like techno speak, then you might need the guidance of a consultant to handle your data security. After all, you went to law school to learn how to practice law, not to know which encryption method works best or why you should or should not employ a specific type of technology.

Social Media: The Bane of Every Family Lawyer's Existence

In the now-infamous divorce case of *B.M. v. D.M.*, 927 N.Y.S.2d 814 (Sup. Ct. 2011), the wife sought maintenance from her former husband, claiming that she was disabled because of chronic back pain. Among the evidence presented to the court were the wife's social media "blogs," that is, posts on Myspace, Facebook, and other websites, which the court summarized as follows.

> According to Wife, belly dancing strengthens and stretches her muscles. At trial, Wife claimed that she was prescribed belly dancing as "a form of physical therapy." However, her claim in that regard was controverted by her own expert witness. When Dr. Maloney was asked if he recommended belly dancing to Wife, he stated: "I don't know anything about it."
>
> Wife admits that from April 2006 through January 2008 she used a home computer to blog about her belly dancing activities. The Court finds not credible Wife's claims that she stopped belly dancing a year and a half ago. On cross examination, Wife admitted that she belly danced as recently as May 20, 2010. In addition, Wife admittedly participated in a two hour belly dancing production in June 2010 in Manhattan but claims that she only had a speaking role. Wife denies that she participated in any of the dancing and claims she only did "ring around the rosy." Wife admitted at trial that she participated in several rehearsals before performing in the show. Wife also posted comments on Facebook about her performance. When asked why she didn't post online any pictures of herself dancing, Wife replied: "Gotta be careful what goes on line pookies. The ex would love to fry me with that."

That's right, her ex-husband would love to "fry" her with the information she posted online, and he did—as have many other parties in divorce, custody, alimony, and other family law matters.

Family lawyers beware. Clients post all the time, they disregard instructions about not posting, and they often jeopardize their cases, as D.M. did here. Lawyers, regardless of their level of tech savviness, have an affirmative, indeed an ethical, obligation to advise clients about the impact social media postings can have on their cases. These duties include advising clients that:

- the content of their social media accounts may be used in legal proceedings and that they should not post anything related, or potentially relevant to, their claims on any social media websites;
- they are prohibited from deleting or otherwise destroying content on social media websites; and
- they must preserve social media information relevant to their cases.

Similarly, attorneys may not delete or destroy client social media content, and they may have an affirmative obligation to obtain and preserve social media data they believe are or may be relevant to the clients' claims.

Speaking of ethical concerns arising from posting on social media, the ABA recently issued ethical guidance for lawyers engaging in blogging or other public commentary. In Formal Opinion 480 of March 6, 2018, the Standing Committee on Ethics and Professional Responsibility reminded lawyers of their duty to protect the confidentiality of client information, explaining that a lawyer is prohibited from commenting publicly about any information relating to a representation, even client identity. *See also* Pa. Bar Ass'n Formal Op. 2014-300 (2014); D.C. Bar Ethics Op. 370 (2016) (lawyer who chooses to use social media must comply

with ethics rules to the same extent as one communicating through more traditional forms of communication). Absent client consent, a lawyer cannot participate in public commentary that includes client information, even if couched as a "hypothetical," if there is a reasonable likelihood that a third party might discover the identity or situation of the client from the facts in the hypothetical.

Online public commentary provides a vehicle for lawyers to share knowledge, opinions, experiences, and case law developments of interest to practitioners. Many lawyers now view social media as an integral, if not primary, component of their marketing strategy. However, the ethical constraints on client confidentiality, as well as on trial publicity and other public statements, must be borne in mind. As ABA Formal Opinion 480 explains, "[w]hile technological advances have altered how lawyers communicate, and therefore may raise unexpected practical questions, they do not alter lawyers' fundamental ethical obligations when engaging in public commentary."

Email: Special Precautions Needed

In 1999, the ABA Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 99-413, concluding that because "[l]awyers have a reasonable expectation of privacy in communications made by all forms of e-mail, including unencrypted e-mail sent on the Internet, despite some risk of interception and disclosure . . . its use is consistent with the duty under Rule 1.6 to use reasonable means to maintain the confidentiality of information relating to a client's representation."

In 2017, the Committee reversed course, issuing Formal Opinion 477R, which reconsidered and limited the application of Formal Opinion 99-413. It concluded that

> [a] lawyer generally may transmit information relating to the representation of a client over the internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.

In short, the Committee concluded that lawyers and law firms may no longer rely upon email as a per se secure method of communications and that they must, when necessary, utilize appropriate security measures, including requiring encrypting email and also encrypting attachments (by, for example, requiring the use of passwords to prevent unauthorized persons from accessing attachments). The opinion explained the Committee's analysis:

> Different communications require different levels of protection. At the beginning of the client-lawyer relationship, the lawyer and client should discuss what levels of security will be necessary for each electronic communication about client matters. Communications to third parties containing protected client information requires analysis to determine what degree of protection is appropriate. In situations where the communication (and any attachments) are sensitive or warrant extra security, additional electronic protection may be required. For example, if client information is of sufficient sensitivity, a lawyer should encrypt the transmission and determine how to do so to sufficiently protect it, and consider the use of password protection for any attachments. Alternatively, lawyers can consider the use of a well vetted and secure third-party cloud based file storage system to exchange documents normally attached to emails.

Thus, it may amount to a violation of the Model Rules for lawyers to include information in the body of an email or in the attachments that contains confidential or sensitive information. In those circumstances, the best practices are to password-protect all attachments and to assure that only intended recipients can view the information.

Conclusion: Only the Most Responsive to Change Survive

Charles Darwin said that, "It is not the strongest species that survive, nor the most intelligent, but the ones most responsive to change." Lawyers and law firms that do not adapt to technological advances or address the potential for client mishandling of privileged or confidential information place themselves in jeopardy. Technology is only moving forward, and family lawyers must adapt to serve their clients effectively. FA

DANIEL J. SIEGEL (dan@danieljsiegel.com), principal of the Law Offices of Daniel J. Siegel, provides ethical guidance and disciplinary representation for attorneys and law firms. He is the editor of *Fee Agreements in Pennsylvania* (6th ed.) and author of *Leaving a Law Practice: Practical and Ethical Issues for Lawyers and Law Firms* (2d ed.), published by the Pennsylvania Bar Institute.

THOMAS G. WILKINSON (twilkinson@cozen.com) is a member of Cozen O'Connor, where he handles commercial litigation and lawyer professional responsibility and liability matters. He serves on the ABA Standing Committee on Professionalism and is a member of the Association of Professional Responsibility Lawyers. He is a past president of the Pennsylvania Bar Association and Pennsylvania Bar Institute.