Competent Representation:
Ethics and Technology in the Practice of Law

Cara E. Greene, Esq.
Outten & Golden LLP
www.outrnengolden.com
3 Park Avenue, 29th Floor
New York, NY 100 16
T: (212) 245-1000 F: (212) 977-4005
ceg@outrngolden.com

“Do Lawyers Have An Ethical Duty To Understand Technology?”

American Bar Association Section of Labor & Employment Law
National Symposium on Technology and Labor and Employment Law
Co-sponsored by the UC Berkeley Center for Labor Research and Education and the
Berkeley Center for Law and Technology
April 21-23, 2013
Bancroft Hotel - Berkeley, CA
INTRODUCTION

The days are gone when all an attorney needed to practice law was a typewriter and a telephone. Technology has transformed the legal practice and attorneys must stay abreast of technological developments if they are to satisfy their ethical obligation to provide competent representation. In fact, the American Bar Association recently amended the Model Rules of Professional Conduct (“Model Rules”) to account for changes in technology, concluding that “competent lawyers must have some awareness of basic features of technology” and amending Comment 6 of Model Rule 1.1 to clarify that minimum competence requires that attorneys keep abreast of changes in the law and practice, including “the benefits and risks associated with technology.”

Preserving Confidentiality of Communications

Client confidentiality is one of the bedrock principles of the Model Rules of Professional Conduct. Rule 1.6 of the Model Rules provides that: “a lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).” This holds true whether a lawyer is communicating with opposing counsel,

---

1 This paper was compiled from earlier papers written by the author, including those written for the National Symposium on Technology in Labor and Employment Law (2011), the American Bar Association Section of Labor and Employment Law Annual CLE Conference (2011), and the Ethics Corner for the American Bar Association Section of Labor and Employment Law Flash.
3 For an alphabetical list of jurisdictions that have adopted a variation of the Model Rules, see http://www.americanbar.org/content/dam/aba/migrated/cpr/pic/ethics_2000_status_chart.authcheckdam.pdf.
talking to his neighbor on the train, or posting a status update on Facebook. Information relating to the representation is not to be disclosed.\(^4\)

Failing to take steps to preserve the confidentiality of client communications, whether by email, text, or other means, may land an attorney in ethical hot water. In the employment context, according to a recent ethics opinion, attorneys must take precautions when they know or have reason to believe that a client is using his or her employer’s devices to send or access privileged client-attorney communications.\(^5\)

As ABA Opinion 11-459 recognizes, attorneys and clients often communicate with each other through email or other electronic means, and clients may use their employers’ computers, smartphones, or other electronic devices to facilitate those communications. However, employers may be able to access employee emails, thus jeopardizing the confidentiality of these client-attorney communications.

Courts are split as to whether employees have a reasonable expectation of privacy for emails sent from company computers. For instance, some courts have found that under certain circumstances, employees do have an expectation of privacy.\(^6\) ABA Opinion 11-459 refuses to

\(^{4}\) Some variations of the rule, such as Rule 1.6 of the New York Rules of Professional Conduct, limit the obligation not to disclose client information to information that is confidential.


weigh in on the substantive question of whether an expectation of privacy exists in communications sent from work computers. However, as the ABA Opinion highlights, the ethics rules require that attorneys take reasonable care to protect the confidentiality of information relating to the client-attorney relationship. This is true whether the communication is by letter, phone call, or electronic means. Specifically, Rule 1.6(a) of the Model Rules requires that a lawyer refrain from revealing, “information relating to the representation of a client unless the client gives informed consent” and a lawyer has a duty to protect the confidentiality of the information.7

In light of the unsettled state of law, ABA Formal Opinion 11-459 suggests that attorneys take steps to explain to their clients the dangers associated with communicating via email or other electronic means. This is especially true in the employment context, where:

Given the nature of the representation—an employment dispute—the lawyer is on notice that the employer may search the client’s electronic correspondence. Therefore, the lawyer must ascertain, unless the answer is already obvious, whether there is a significant risk that the client will use a business e-mail address for personal communications or whether the employee’s position entails using an employer’s device. Protective measures would include the lawyer refraining from sending e-mails to the client’s workplace, as distinct from personal, e-mail address, and cautioning the client against using a business e-mail account or using a personal e-mail account on a workplace computer or device at least for substantive e-mails with counsel. . . . if the lawyer becomes aware that a client is receiving personal e-mail on a workplace computer or other device owned or controlled by the employer, then a duty arises to caution the client not to do so, and if that caution is not heeded, to cease sending messages even to personal e-mail addresses.

While it is not always the case that sending client-attorney communications via a work computer will breach confidentiality, best practices dictate that attorneys advise their clients

---

7 See Model Rule 1.1; Model Rule 1.6, Comments 16, 17.
early, and repeatedly if necessary, that they should not use employer computers, cell phones, iPads, etc. to communicate about their matters.

The Comments to Model Rule 1.6 further clarify what diligence an attorney must exercise to preserve confidentiality. Comment 18 states that a lawyer must “act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer’s supervision,” and Comment 19 explains: “When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients . . .”

In addition, as part of the ABA’s recent amendments to the Model Rules⁸, the ABA adopted Model Rule 1.6(c), which requires that, “A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.”⁹ Comment 18 also clarifies subdivision (c) by outlining factors to determine reasonable measures, including “sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer’s ability to represent clients (e.g., by making a device or

---

⁸ The American Bar Association’s Commission on Ethics 20/20 (the “ABA 20/20 Commission”) recently concluded its task of updating the Model Rules of Professional Conduct (“Model Rules”) to reflect technological changes in the way law is practiced, with the ABA adopting amendments to the Model Rules in August 2012 and February 2013. See http://www.americanbar.org/groups/professional_responsibility/aba_commission_on_ethics_20_20.html
⁹ Model Rule 1.6(c).
important piece of software excessively difficult to use).”\textsuperscript{10} Further, a client may require the lawyer to implement special security measures not required by the Model Rules or may agree (after being apprised of the risks in doing so) to forego security measures otherwise required by Model Rule 1.6.\textsuperscript{11}

Amendments to Model Rule 4.4 (Respect for Rights of Third Persons) and its commentary highlights that confidential information may be stored electronically and may exist within the metadata of electronic documents.\textsuperscript{12} The Model Rule requires that when such information is inadvertently disclosed, the recipient must promptly notify the sender.\textsuperscript{13} Several states have issued ethics opinions addressing the inadvertent disclosure of metadata\textsuperscript{14} and most opinions reach the same conclusion as the Model Rule: that a recipient of a document that includes inadvertently disclosed metadata must notify the sender.\textsuperscript{15} The opinions differ as to whether a recipient may “mine” the metadata after notifying the sender.\textsuperscript{16}

\textbf{Preserving Confidentiality on the Cloud}

Cloud computing allows individuals to access applications and store information remotely, without physically buying and installing software or saving to a local storage device (think “Gmail” for email or “DropBox” for online storage). This technology undoubtedly offers a number of benefits to law practices of all sizes, the two primary advantages being reduced cost and increased accessibility. For example, with cloud computing a law firm can greatly reduce its

\textsuperscript{10} Model Rule 1.6, Comment 18.

\textsuperscript{11} Id.

\textsuperscript{12} Model Rule 4.4, Comment 2.

\textsuperscript{13} Model Rule 4.4.

\textsuperscript{14} See http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/metadatashart.html for a chart of ethics opinions addressing inadvertent disclosure of metadata.

\textsuperscript{15} Id.

\textsuperscript{16} Id.
need for a large internal IT infrastructure (servers, back-up storage, on-site Tech support, etc.) by utilizing online storage systems. This could be particularly useful for budding firms that may not have the capital to establish an adequate on-site IT infrastructure. In terms of accessibility, cloud computing allows attorneys to access practice management software and client files from anywhere with an internet connection.

However, while the potential benefits do indeed seem promising, attorneys should remember that the same ethical rules apply in the cloud as on Earth and that the benefits of cloud computing do not come without potential ethical pitfalls. The ABA 20/20 Commission identified the following potential risks associated with cloud computing:

- unauthorized access to confidential client information by a vendor’s employees (or sub-contractors) or by outside parties (e.g., hackers) via the Internet
- the storage of information on servers in countries with fewer legal protections for electronically stored information
- a vendor’s failure to back up data adequately
- unclear policies regarding ownership of stored data
- the ability to access the data using easily accessible software in the event that the lawyer terminates the relationship with the cloud computing provider or the provider changes businesses or goes out of business
- the provider’s procedures for responding to (or when appropriate, resisting) government requests for access to information
- policies for notifying customers of security breaches
- policies for data destruction when a lawyer no longer wants the relevant data available or transferring the data if a client switches law firms
- insufficient data encryption
• the extent to which lawyers need to obtain client consent before using cloud computing services to store or transmit the client’s confidential information.17

At least five states have addressed cloud computing, and all five have approved of the use of this technology in the practice of law.18 The general gist of all five opinions is that while the technology may be different, an attorney’s ethical obligations remain the same, however. The NYSBA Committee concluded that just as an attorney may hire a third party to store hard-copies of client files, so too may an attorney use an online storage system, provided the attorney exercises reasonable care to ensure that the information will remain secure.19 This is consistent with New York Rules of Professional Conduct Rule 1.6(a), which requires that, subject to certain exceptions, “a lawyer shall not knowingly reveal confidential information . . . or use such information to the disadvantage of a client or for the advantage of a lawyer or third person.”20 Rule 1.6(c) requires that an attorney exercise “reasonable care” to ensure that third-parties who provide services for the attorney do not divulge or use confidential information.21

While it may be relatively clear what “reasonable care” entails in the context of traditional third party storage, those same practices do not seamlessly transfer to online storage. Thankfully, the ethical opinions that have addressed this issue have provided some basic guidance. The NYSBA Committee opinion offers a non-exhaustive list of four steps an attorney

20 N.Y. Model R. Prof. Conduct 1.6(a).
21 N.Y. Model R. Prof. Conduct 1.6(c).
may wish to take in her effort to exercise reasonable care. First, ensure that the storage provider has “an enforceable obligation to preserve confidentiality and security, and that the provider will notify the lawyer if served with process requiring the production of client information.” Second, attorneys should investigate the storage provider’s “security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances.” While the opinion does not directly address what constitutes “adequate under the circumstances” one can imagine that this might depend on the nature of the client. For example, different security measures might be required for a large corporate or government client who has been the target of “hacking.” A firm may even want to consider whether cloud storage should be avoided entirely for such a client. Conversely, less stringent security measures might be required for a smaller client where this risk is minimal. These same considerations would be present in more traditional storage. Third, the NYSBA Committee’s opinion suggests that lawyers utilize “available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored.” Finally, attorneys should investigate the provider’s ability to “purge,” “wipe,” and “transfer” the data if the attorney decides to use another provider.

While the NYSBA Committee opinion provides general guidelines on how to avoid ethical problems, the opinion does not provide much in terms of specifics or best practices. Unfortunately, the other ethics opinions to address this issue are similarly vague. What is clear from the opinions is that attorneys have an affirmative obligation to keep abreast of technological

---

23 Id.
24 Id.
developments and ensure that the security measures remain current.\textsuperscript{25} As the ABA 20/20 Commission has explained,

Technology can increase the quality of legal services, reduce the cost of legal services to existing clients, and enable lawyers to represent clients who might not otherwise have been able to afford those services. Lawyers, however, need to understand that technology can pose certain risks to clients’ confidential information and that reasonable safeguards are ethically required.\textsuperscript{26}

Other industry groups also are tackling the issue. In December 2010, a group of cloud computing providers organized as the Legal Cloud Computing Association (LCCA). The LCCA published a letter to the ABA 20/20 Commission requesting, among other things, that the ABA publish minimum technology standards as well as model terms of service for cloud computing providers.\textsuperscript{27} While the ABA has not yet responded to this request, should they choose to do so, practitioners would have much needed guidance when seeking out a provider and evaluating whether their security measures are adequate. Until then, practitioners should be aware that they have a continuing obligation to monitor the technology they are using to make sure it remains adequate to protect confidential information.

Like cloud computing, “local” technology, like the use of laptops and Wi-Fi, also raises ethical concerns. The ABA 20/20 Commission proposed certain precautions that lawyers may wish to take to preserve confidentiality in this context. While not adopted, they remain informative, and include:

\begin{itemize}
\item \textsuperscript{25} N.Y. State Bar Assoc. Comm. on Prof’l Ethics, Op. 842, at *3; See also AZ Eth. Op. 09-04 (2009) (“because technology is constantly evolving, the lawyer will have a continuing duty to stay abreast of appropriate safeguards that should be employed by the lawyer and the third-party provider.”).
\item \textsuperscript{26} ABA 20/20 Comm’n Initial Draft Proposals – Technology and Confidentiality.
\end{itemize}
• providing adequate physical protection for devices (e.g., laptops) or having methods for deleting data remotely in the event that a device is lost or stolen

• encouraging the use of strong passwords

• purging data from devices before they are replaced (e.g., computers, smart phones, and copiers with scanners)

• installing appropriate safeguards against malware (e.g., virus protection, spyware protection)

• installing adequate firewalls to prevent unauthorized access to locally stored data

• ensuring frequent backups of data

• updating computer operating systems to ensure that they contain the latest security protections

• configuring software and network settings to minimize security risks

• encrypting sensitive information, and identifying (and, when appropriate, eliminating) metadata from electronic documents before sending them

• avoiding “wifi hotspots” in public places as a means of transmitting confidential information (e.g., sending an email to a client)²⁸

Preserving Confidentiality on the Web

While most attorneys understand their confidentiality obligations in respect to oral communications and traditional written correspondence, recent disciplinary proceedings evidence that attorneys may be more likely to disregard Rule 1.6 when it comes to online communications. The case of In re Peshek²⁹ provides one such example. In that matter, Respondent, an assistant public defender, maintained a blog entitled, “The Bardd (sic) Before the Bar – Irreverant (sic) Adventures in Life, Law, and Indigent Defense.” On a regular basis, Respondent blogged about her criminal defense work, referring to clients by their first names, a derivative of their first names, or their jail identification numbers. Included in her posts were

²⁸ Id.
her clients’ jailhouse confessions, commentary on her clients’ truthfulness and behavior, and derogatory statements about the court. When the blogs were discovered, Respondent was fired from her job and the Commission found that she had violated Rule 1.6, among other rules.\textsuperscript{30}

As with blogging, social media sites like Facebook and Twitter present opportunities to disregard the obligation to preserve client confidentiality. The attorney who posts a status update, “Spent the day in a deposition with a client who conveniently ‘forgot’ the truth,” may very well run afoul of the rules, especially if by the facts and circumstances the identity of the client may be ascertained.

But attorneys are not the only ones who may be more reckless in online communications. Clients too may be more likely to share confidential, attorney-client privileged information in a social media forum, as one recent case demonstrates. In \textit{Lenz v. Universal Music Corp.}\textsuperscript{31}, the district court upheld the magistrate’s decision to compel attorney-client communications because the client had discussed the communications in emails and instant chats with family and friends, in blog postings, and with the media.

In true 21\textsuperscript{st} Century fashion, the underlying controversy also stemmed from the use of social media. The plaintiff had posted a 29-second video of her toddler dancing to the song “Let’s Go Crazy” (by the artist Prince) on YouTube. Universal Music Corp., the copyright owner for the song, sent YouTube a take-down notice alleging that the video infringed on its copyright. After YouTube complied with the request, the plaintiff, who is represented by the Electronic Frontier Foundation (“EFF”), sued Universal, alleging that Universal knowingly and

\textsuperscript{30} Respondent also violated Rules 1.2, 3.3, and 8.4 of the Illinois Rules of Professional Conduct by failing to bring to the Court’s attention the fact that one of her clients had committed perjury, a fact she included in her blog posts.

\textsuperscript{31} No. 07 Civ. 03783, 2010 WL 4789099 (N.D. Cal. Nov. 17, 2010).
materially misrepresented in its takedown notice that the video infringed on its copyright, a violation of the Digital Millennium Copyright Act.

Prior to retaining counsel, as well as during the litigation, the plaintiff discussed her conversations with counsel in emails, electronic chats, blog posts, and media interviews. For example, in emails, the plaintiff stated that EFF was “very, very interested in the case,” and that “EFF is pretty well salivating over getting their teeth into [Universal Music Group] yet again.” In others, she stated that EFF was planning a “publicity blitz and/or a lawsuit against Universal.” In electronic chats, she discussed the legal strategy in dropping her state law claims, as well as her attorneys’ opinions about why Universal had sent the notice. In speaking with a reporter, the plaintiff stated that “[i]n discussing the situation with one of the EFF lawyers, we came to the conclusion that I did not infringe the copyright and eventually we decided to file this lawsuit.”

On the basis of these statements and others like them, the Court found that the plaintiff had waived the attorney-client privilege and that Universal was entitled to discovery of attorney-client communications related to the plaintiff’s motivations for pursuing litigation, the legal strategy, and certain factual issues.

Both In re Peshek and Lenz should serve as cautionary tales for attorneys practicing in the era of social media. Attorneys must remember that their obligation to preserve client confidentiality does not end when they log on to Facebook, Twitter, or blog spaces. If anything, attorneys should have heightened sensitivity to confidentiality when dealing with social media, given its lack of privacy and its ability to expand beyond the initial audience.

Ethically Using Social Media in Discovery

Social media serves as a new repository of potentially relevant information. Conversations that would have taken place by email ten years ago, and around the water cooler
twenty years ago, now happen via Facebook and Twitter. Photos, which may contain incriminating images, are memorialized and conveniently “tagged.”

Social media not only contains potentially relevant information, it also provides the means for discovering the information. By simply “Friending” a potential witness or following a Twitter feed, an attorney can gain access to the information contained on those social media sites. Informal discovery has long been an accepted, and even an encouraged, means of gathering evidence and information. As the New York Court of Appeals explained in *Niesig v. Team I*[^32^], “avenues of informal discovery of information [] may serve both the litigants and the entire justice system by uncovering relevant facts, thus promoting the expeditious resolution of disputes.”

Informal discovery is not without limits, however. Model Rules 4.1, 4.2, and 4.3 all set forth guidelines for engaging in informal discovery. Model Rule 4.1 prohibits an attorney from making a false statement or material misrepresentation in the course of representing a client.[^33^] Model Rule 4.2 prohibits *ex parte* communications with a represented party, unless the represented party’s attorney has given consent or the communication is authorized by law or court order.[^34^] Model Rule 4.3 prohibits an attorney from stating or implying that he or she is disinterested when communicating with an unrepresented person.[^35^]

[^33^]: Model Rule 4.1 provides in relevant part: “In the course of representing a client a lawyer shall not knowingly: (a) make a false statement of material fact or law to a third person.”
[^34^]: Model Rule 4.2 provides: “In representing a client, a lawyer shall not communicate about the subject of the representation with a person the lawyer knows to be represented by another lawyer in the matter, unless the lawyer has the consent of the other lawyer or is authorized to do so by law or a court order.”
[^35^]: Model Rule 4.3 provides: “In dealing on behalf of a client with a person who is not represented by counsel, a lawyer shall not state or imply that the lawyer is disinterested. When the lawyer knows or reasonably should know that the unrepresented person misunderstands
Several ethics opinions have considered the application of these rules to discovery via social media. The New York State Bar Association’s Committee on Professional Ethics (“NYSBA Committee”) affirmed that an attorney may view and access publicly available social media pages, such as Facebook and MySpace profiles, without running afoul of the ethics rules.\(^{36}\) In the NYSBA Committee’s opinion, Rule 8.4(c) – misconduct by “engaging in conduct involving dishonest, fraud, deceit or misrepresentation”\(^{37}\) – is not implicated because the information is available to the public at large and the lawyer is not engaging in deceit to obtain the information.

A March 2009 advisory opinion from the Philadelphia Bar Association Professional Guidance Committee (“Advisory Committee”) addressed an inquiry by an attorney who wished to dig for relevant evidence in a witness’s on-line Facebook and MySpace accounts.\(^{38}\) The attorney hoped to engage the services of a third party who would attempt to gain access to the witness’s friendship networks by “Friending” the witness. The attorney stated that the third party would do so without revealing that the third party would be mining for information to give to the attorney.

In response to the attorney’s inquiring about whether this proposed course of conduct was ethically permissible, the Advisory Committee was unequivocal: “deception is deception” and that includes “Friending” under false pretenses. First, the Advisory Committee noted that the

---

37 New York Rules of Professional Conduct Rule 8.4 provides in relevant part: “A lawyer or law firm shall not . . . engage in conduct involving dishonesty, fraud, deceit or misrepresentation.”
attorney is responsible under the professional rules for the conduct of the third person, pursuant to Rule 5.3.\textsuperscript{39} In short, the Advisory Committee affirmed that attorneys are responsible for the misdeeds of the third parties they employ when it comes to covert operations.

Importantly, the Advisory Committee also determined that such conduct would violate Rule 8.4(c). Because the planned communication by the third party omits a highly material fact, “namely, that the third party who asks to be allowed access to the witness’s pages is doing so only because he or she is intent on obtaining information and sharing with a lawyer for use in a lawsuit to impeach the testimony of the witness,” and the omission would purposefully conceal that fact from the witness, the proposed conduct rises to the level of misconduct. In finding the proposed acts deceitful, the Advisory Committee likened the internet networks as “private areas” closed to the general public, as opposed to public areas, such as outside surveillance videos of plaintiffs in a tort action.

The New York City Bar Association’s Committee on Professional Ethics (“NYCBA Committee”) reached a somewhat different conclusion when considering the issue of whether an attorney “may resort to trickery via the internet to gain access to an otherwise secure social networking page and the potentially helpful information it holds.”\textsuperscript{40} Ultimately, the NYCBA Committee concluded that if an attorney or investigator “Friends” a witness using only truthful

\textsuperscript{39} Pennsylvania Rules of Professional Conduct Rule 5.3 provides in relevant part: “With respect to a nonlawyer employed or retained by or associated with a lawyer . . . a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if: (1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or (2) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and in either case knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

information (i.e. the attorney or investigator’s real name and profile), and subject to compliance with all other ethics rules, the attorney or investigator is not obligated to disclose the reasons for making the “Friend” request.

May attorneys investigate jurors and potential jurors using the internet and social networking sites like Facebook and Twitter without running afoul of ethics rules? Several recent decisions answer the question in the affirmative. In a recent ethics opinion, the New York County Lawyers Association Committee on Professional Ethics considered whether, after jury selection is complete, an attorney may conduct ongoing research on a juror via Twitter, Facebook, and other social networking sites. N.Y. Cnty. Lawyers Ass’n Comm. On Prof’l Ethics Op. 743 (May 18, 2011). The Committee concluded that while an attorney may not contact a juror or potential juror under Rule 3.5 of the New York Rules of Professional Conduct, an attorney may access publicly available social networking sites if the juror is unaware that the attorney is doing so. Rule 3.5(a)(4) prohibits an attorney from communicating with or causing another person to communicate with the jury pool or members of the jury during the course of a trial.

The Committee opined that while an attorney may access publicly available social networking sites, sending a friend request via Facebook, connecting with a juror via LinkedIn, signing up for a RSS feed of a juror’s blog, or following a Twitter account would entail impermissible contact with a juror. Furthermore, if the juror becomes aware that an attorney is monitoring social networking sites, “the contact may well consist of an impermissible communication, as it might tend to influence the juror’s conduct with respect to the trial.” As the Committee noted, recent ethics opinions have outlined other considerations for accessing social networking sites ethically. See N.Y. State Bar Ass’n. Comm. on Prof’l Ethics, Op. 843 (2010);
see also Phila. Bar Ass’n. Prof’l Guidance Comm., Op. 2009-02 (March 2009). The Committee also noted that under Rule 8.4, attorneys may not direct others to do what they themselves cannot.

Addressing a related issue, the New Jersey Appellate Division held that, under New Jersey law, attorneys are permitted to research potential jurors via the internet as part of jury selection. Carino v. Muenzen, No. A-5491-08T1, 2010 WL 3448071 (N.J. App. Div. Aug. 30, 2010), cert. denied, 205 N.J. 96 (Feb. 3, 2011). In Carino, a medical malpractice case, plaintiff’s counsel used a laptop computer in the courtroom to Google potential jurors. When the trial judge became aware of the attorney’s actions, the judge prohibited further internet research in the courtroom on the basis that because the plaintiff’s attorney had not provided advance notice of his intention to research potential jurors on the internet, defense counsel (who did not have a laptop computer in the courtroom) was disadvantaged.

Plaintiff appealed on the basis, among others, that the trial court abused its discretion by precluding his attorney from conducting internet research on prospective jurors, thereby depriving him “of the opportunity to learn about potential jurors . . . one of the most fundamental rights of litigation.” The Appellate Division agreed and found that the trial court acted unreasonably in denying plaintiff’s counsel use of the internet. The Appellate Division explained that, “There was no suggestion that counsel’s use of the computer was in any way disruptive. That he had the foresight to bring his laptop computer to court, and defense counsel did not, simply cannot serve as a basis for judicial intervention in the name of ‘fairness’ or maintaining ‘a level playing field.’ The ‘playing field’ was, in fact, already ‘level’ because internet access was open to both counsel, even if only one of them chose to utilize it.” The Appellate Division found that plaintiff’s counsel was not prejudice as a result of the trial court’s
decision, however, because plaintiff’s counsel could not point to one juror who would have been struck as a result of information discovered via an internet search.

In another case touching on internet investigation of jurors, the Supreme Court of Missouri held that attorneys have an obligation to investigate the background of jurors and ordered that going forward, “a party must use reasonable efforts to examine the litigation history on Case.net of those jurors selected but not empanelled and present to the trial court any relevant information prior to trial.” *Johnson v. McCullough*, 306 S.W. 3d 551 (Mo. 2010). In that case, plaintiff’s counsel sought a new trial after discovering that one of the jurors had lied during *voir dire* about previous litigation experience.

As technology develops, attorneys will have at their disposal additional means of conducting research on potential and sitting jurors. But attorneys must remember that while the technology has changed, the ethics rules still apply.

**CONCLUSION**

While advances in technology and communications may leave an attorney scratching his or her head as to the application of the ethics rules, this need not be the case. The essence of the ethics rules remains unchanged. By applying common sense and remembering that the rules do not cease to apply simply because technology is involved, an attorney can tackle the challenges of practicing law in the 21st Century with confidence.

----------------------------------

*Cara E. Greene* is a partner at Outten & Golden LLP in New York City, where she represents partners and employees in all aspects of employment law. She regularly writes and speaks on ethics issues in the employment law practice.