



THE FLORIDA BAR

Best Practices for Professional Electronic Communication



UPDATED NOVEMBER 2019

Table of Contents

- I. Communication..... 3
- II. Texting..... 3
 - Technology Considerations of Texting..... 4
- III. Email..... 4
 - A. Replying to Email 7
 - B. Rules for Email Discussion Groups..... 8
 - C. Responding to an Angry Email 8
 - Technology Considerations of Email..... 9
- IV. Social Media..... 9
- V. Telephone/Cell Phone 11
 - A. Telephone 11
 - B. Cell Phone 12
 - C. Hostility via the Telephone/Cell Phone 12
 - D. Setting Voicemail 13
 - E. Leaving a Voicemail..... 13
- VI. Laptop/Tablet Usage in Public and Cybersecurity 14
- VII. Records Management..... 15
- VIII. Expectations..... 15
- IX. A discussion of Ethics Issues in Electronic Communication..... 16
 - A. Creating Inadvertent Relationships 16
 - B. Electronic Practice 16
 - C. Confidentiality..... 16
 - D. Inadvertent Disclosure via Metadata..... 17
 - E. Impugning Integrity of Judges..... 18
 - F. Communication with/Investigating Witnesses..... 18
 - G. Communicating with Represented Persons via Social Networking Sites or Other Electronic Means
19
 - H. Social Networking, Electronic Communication and Judges 19
 - I. Social Networking and Mediators..... 20
 - J. Social Networking and Jurors 20

Cover art: jbrouckaert / www.fotosearch.com

I. Communication

The Oxford Dictionary defines communication as: “The imparting or exchanging of information or news” or, alternatively, “The successful conveying or sharing of ideas and feelings.”

Lawyers use multiple forms of communication on a daily basis to diligently advocate and are in a constant state of communication with clients, opposing counsel, the court and colleagues. This guide provides best practices for the most popularly used forms of electronic communication.

The Oath of Admission to The Florida Bar includes a pledge of “fairness, integrity and civility, not only in court, but also in all written and oral communications.”

II. Texting

Texting is a common form of communication that requires a basic level of etiquette. It is best practice to:

- Keep texts short. More than 160 characters means that a telephone call or email is the better way to deliver your message. Think of texts as preludes or follow-ups to conversation, not the conversation itself.
- Because of the brevity of most texts, your tone can be misunderstood by the recipient. Texts are best left for general messages such as, “I will be arriving at mediation in less than five minutes” or “Our conference call will start at 2 p.m.”
- Texting is the most informal form of communication. If the message is important, deliver it in person, by telephone or via email.
- Try to spell out all words to eliminate confusion. Never use ALL CAPS; which is the digital equivalent of yelling. Check your spelling; autocorrect will often change words you intended to use into words you did not intend to use.
- If your conversation requires the exchange of more than three texts, it is probably better to communicate face-to-face or by email or telephone.
- Be sure you have permission to text the person. Just because the person provided a cell phone number does not mean you have permission to text. If you are texting someone for the first time, identify yourself.
- Do not text while in business meetings or court proceedings (be aware of Rule 4-1.6 Confidentiality). Do not text while driving or send a text to someone who you know is driving.



- Respect the time of others. Do not send text messages to clients, opposing counsel or others involved with legal matters outside of normal business hours (8 a.m.-5 p.m.) unless you have permission. Be mindful of time zones.
- Pursuant to a decision of the Board of Governors, an advertising lawyer may send advertisements via text only if (1) the advertising lawyer complies with all requirements for written communications sent to specific recipients under Rule 4-7.18(b), (2) provides an “opt-out” for recipients, (3) the recipients are not required to pay for receipt of the text messages, and (4) the lawyer complies with all state and federal laws, rules and regulations regarding unsolicited text messages. The advertising lawyer is responsible for determining compliance with all applicable laws, rules and regulations, including the federal Telephone Consumer Protection Act, 47 U.S.C. §227. This advisory advertising opinion only addresses compliance with the Rules Regulating The Florida Bar related to attorney advertising and does not address whether the advertising lawyer is in compliance with applicable laws, rules and regulations regarding unsolicited text messages.

Technology Considerations of Texting

- Texts are not temporary. Text messages can be saved on a cell phone within the actual conversation or on a smartphone by simply taking a screenshot of the conversation. These captured text messages can be forwarded to other recipients or exported off the device.
- Text threads can be altered. Most smartphones allow users to delete individual text messages in a thread/conversation. Do not assume the thread you are seeing, reading or sending will remain intact.
- When dealing with text messages related to a client, you should be familiar with the backup policies, methods, retrieval, metadata, etc. that texting service providers and devices employ for retaining and destroying sent and received text messages.
- Use sound judgment when texting. Although texting is an easy and quick form of communication, lawyers should consider whom they text and whom they receive texts from. Responding to clients via text could consume a large part of your day if you do not control communication.

III. Email

Email is a quick and convenient way to connect with clients, colleagues, the court system and opposing counsel. It is not a good substitute for face-to-face contact and telephone calls for interpersonal communication. Email messages may become part of a court record and may be subject to disclosure to third parties. Compose email messages in the same manner and with the same good judgment that you would employ for any other communication. When a topic needs

to be explained or negotiated and will generate too many questions and confusion, don't handle it via email. Also, email should not be used for last minute cancellations of meetings, lunches or interviews, and never for devastating news. If you need to deliver bad news, a phone call or meeting is preferable.

It is best practice to:

- Use a descriptive subject line; never leave the subject line blank. It should pinpoint for the recipient exactly why you are emailing. Also, a clear subject line allows for easy searches later. Don't hit "Reply" to an old message and send an email that has nothing to do with the previous one. Change the subject line when the content of the email chain changes.
- Use a salutation. Make no assumptions about the receiving party's gender. Your email greeting and signoff should be consistent with the level of respect and formality of the person you're communicating with. Write for the person who will be reading it: If the recipient is very polite and formal, write in that language. The same goes for a recipient who tends to be more informal and relaxed. If you are uncertain about whether the recipient remembers you, or will recognize your name and email address, include a simple reminder of who you are. Example: "I am emailing about the Smith case that we discussed at the CLE event on xx/yy/zzzz in Tampa."
- Be courteous. As with any other form of business correspondence, email messages should be written with courtesy and respect – two hallmarks of professionalism. Do not employ rude or facetious remarks that could be deemed unethical, unprofessional, defamatory or prejudicial (Rule 4-8.4(d)).
- Don't use ALL CAPS. It can be read as shouting and makes your email difficult to read. Exclamation points and other indications of excitement such as emojis, abbreviations such as LOL, and ALL CAPS do not translate well in business communications. Leave them off unless you know the recipient extremely well. Humor can easily get lost in translation without tone or facial expressions. In a professional exchange, it's better to leave humor out of emails unless you know the recipient well. Just as jokes get lost in translation, tone is easy to misconstrue without the context you'd get from vocal cues and facial expressions. Avoid using negative words such as "failure," "wrong," or "neglected," and always say "please" and "thank you." Miscommunication can easily occur because of cultural differences, especially in writing where we can't see body language. Tailor your message to the receiver's background or how well you know them.
- Check, revise and edit your email. Do not ignore the basics of writing, punctuation and spelling. Watch your tone. Avoid slang, jargon and abbreviations. Be succinct without coming across as rude. Create your message as a concise, stand-alone note, even if it is in response to a chain of emails. It is frustrating for recipients to scroll back through

multiple emails to understand the issues. Be clear. Make sure it's not a burden to read. Consider using bullet points or numbering. The person reading your email should not have to dig through several paragraphs to figure out what you're saying. State the purpose of your email within the first two sentences.

- Sign your email. Include information such as your telephone number, position, location and email address. Different signatures for different recipients may be appropriate. For example, shorter signatures may suffice for email to internal colleagues. This provides the recipient, particularly external recipients, with some information about you. The recipient should not have to look up how to get in touch with you.
- Appropriately use "cc." A "cc" (carbon copy) suggests that the message is for information only; no action is necessary on the part of the "cc" recipients. Send carbon copies only to those who need a copy. Before you click "Reply All" or put names on the "cc" or "bcc" (blind carbon copy) lines, ask yourself if the recipients really need the information in your email; if they don't, why send it? Take time to send your messages to the right people.
- If you're sending a message to a group of people and you need to protect the privacy of your list, use "Bcc," otherwise, use bcc with caution.
- Use attachments for long text or reports, or when special formatting is necessary. To keep the file size small, avoid unnecessary graphics (pictures and logos) and/or embedded multimedia. Most email servers accept attachments up to 10 MB, the general standard. Your email system may let you attach a document as large 25 MB, but that doesn't mean the recipient can or will receive it, as large attachments can clog the recipient's inbox and cause other emails to be returned to the sender. There are other ways to reduce a document's file size, such as compressing images or selecting "reduce file size" when saving PDFs. If the attachment is still larger than 20 MB, consider using a secure file-sharing service. Also, give the attached files logical names so the recipient knows at a glance the subject and the sender. Example: "Smith contract – GB version 8-22-19."
- Add the email address last. This ensures that you don't accidentally send an email before you have finished writing and proofing. Doublecheck your recipient list. Pay careful attention when typing a name from your address book on the "To" line. It's easy to select the wrong name, which can be embarrassing to you and to the person who receives the email by mistake. Email can be unforgiving. Thanks to high-speed Internet, it is almost impossible to "recall" an email. Even if you could, doing so would only call more attention to the original message, your mistake and your attempts to undo it.
- Email should not be used to resolve conflict or to say things that would not be said in person.

- Evaluate the importance of your email. If you overuse the “High Importance” feature, few people will take it seriously. Instead, use descriptive subject lines that explain exactly what a message is about.
- Your mistakes won't go unnoticed by the recipients. Don't rely solely on spellcheckers. Read and re-read your email a few times before sending it. Example: You intended to type, “Sorry for the inconvenience” but you accidentally typed, “Sorry for the incontinence.” Spellchecker will not correct that.
- Keep your fonts, colors, and sizes classic. Your emails should be easy for recipients to read. It's best to use 12- or 14-point type and an easy-to-read font such as Arial, Calibri, or Times New Roman. As for font color, black is the safest choice.
- Keep private material confidential. Assume that others will see what you write, so don't write anything you wouldn't want everyone to see. Email is dangerously easy to forward; it's better to be safe than sorry.
- When corresponding with a judge about a pending case, copy the opposing counsel (or opposing party if pro se) to avoid ex parte communications.

A. Replying to Email

Colleagues expect prompt responses to email questions. It is best practice not to leave the sender hanging. Depending on the sender and the nature of the email, responding within 24 to 48 hours is generally acceptable. If you cannot send a full response in a reasonable time, it is best practice to send a quick reply stating that you have received the message and give an estimate of when you will provide a more detailed response. If possible, you should reply to an email accidentally sent to you and especially if the sender is expecting a reply. Example: “I don't think you meant to send this to me, and I thought you should know so you can send it to the correct person.” However, refrain from sending one-liners: “Thanks,” and “Oh, OK” do not advance the conversation in any way. Consider putting “No Reply Necessary” at the top of emails if you don't anticipate a response.

An automatic response that says “Thank you for your email message. I will respond to you as soon as I can” is not helpful. Using one when you are out of the office – that tells when you will return or be able to respond – is.

It is also best practice to use “Reply All” only when appropriate. Be careful when replying to a message that was sent by a bulletin board or automatic remailer. Your reply may be sent to the entire audience subscribing to the bulletin board.

As a matter of both courtesy and efficiency, include the original email when replying. It avoids confusion and making the sender search for the original message. Where your reply is relevant to only a portion of the original message, consider excerpting and including in your reply only the relevant portions.

B. Rules for Email Discussion Groups

Group discussions on listservs are meant to stimulate conversation, not create contention. Here are best practices for navigating the realm of listservs:

- Do not post anything in a message that you would not want the world to see or that you would not want anyone to know came from you.
- Be aware that advertising rules apply to commercial messages or promotional information regarding yourself or your firm that is posted on the listserv (Rule 4-7.11).
- Do not post messages to all members of the list disparaging the system of justice or any individual who is a part of the system of justice. (Rule 4-8.2(a).)
- Do not use a listserv to vent about the particulars of a case (Rule 4-1.6; also, Rule 4-3.6 Trial Publicity and Rule 4-3.5 Impartiality).
- Do not post any information or other material protected by copyright without the permission of the copyright owner.
- Do not challenge or attack others. Let others have their say.

C. Responding to an Angry Email

As email has made it easier for people to communicate very quickly, it also has made it easier for people to forget about civility. How do you react when you are the recipient of an angry email? How do you keep the situation from escalating? It is best practice to:

- Step away from the computer. An angry email will usually trigger your own anger. Never reply to the email right away; it will only escalate the issue. Never send an angry email or give a flip response. Give your message thoughtful consideration before sending it. If you feel angry, put your message in the “drafts” folder and review it again later.
- Identify the facts in the email. Does the writer have a reason to be angry? Did you say or do something that legitimately offended the person? Be objective.
- Evaluate what the writer got wrong. Did the writer misinterpret a letter or get the wrong information?
- Put yourself in the writer’s shoes. What kind of response would you expect? Understanding the writer’s perspective will aid in your response.
- Verify all the facts and fix what you can before writing back. Being able to state in your reply that you already have taken action will go a long way toward resolving the issue.
- Begin your reply with positives. Explain where the writer was right and that you understand why the writer is upset. Explain what has been done to fix the problem and apologize if necessary.
- Once you provide the positives, ease into explaining where the writer was wrong. Do not get emotional or confrontational. Avoid name-calling, placing the blame and

sarcasm. State your side of the issue. If it was a misunderstanding, try to interject that you understand what caused it.

- Do not be afraid to give consequences. If the business relationship cannot continue, say so. Be straightforward so it does not sound like a threat. Don't make ultimatums if you cannot or will not follow through. Do not threaten to file a Bar complaint or seek criminal prosecution, as these violate Rule 4-3.4(g) and (h).
- Be respectful and civil, even if the writer failed to show you the same respect.
- Think about how permanent emails are. They can be forwarded, printed and shared. Make sure you are prepared to stand by your words; do not write anything you might regret later.
- Save records of the correspondence. It is easier to defend yourself later if you have proof.

A lawyer should be mindful of Florida Bar Rule 4-8.4 Misconduct when engaging in an angry email exchange. In addition, review Rule 3-4.3 Misconduct and Minor Misconduct before responding.

Technology Considerations of Email

- When sending attachments, be aware that they may contain metadata that could disclose unwanted information to the recipient.
- Attachments may contain malicious software code. Use scanning software for both outbound and inbound emails.
- If you use email as form of confidential communication, you should know the risks and be familiar with the options of sending secure/encrypted messages.
- There is always a chance that your email may be intercepted. Many of these risks are mitigated if not entirely eradicated when using an encrypted email service.
- Secure client portals are an emerging and safe alternative to email. There are many case and practice management systems that offer a client portal component. You should seriously consider this option as a method of communication for confidential information.

IV. Social Media

Social media allows people to create and share information and ideas in virtual communities. Social media include but are not limited to blogging, micro-blogging (i.e., Twitter), social networking sites (Facebook, LinkedIn) and interactive multimedia sites (YouTube).

Here are best-practice tips, rules and real-life scenarios:



- The Florida Supreme Court's Civility Pledge added to the Oath of Admission in 2011 requires lawyers to promise fairness, integrity and civility, not only in court, but also in all written and oral communications. This includes emails, blogs and social media sites.
- Any communication made by a lawyer must refrain from fraud, deceit, dishonesty and misrepresentation (See Rules 4-7.13, 4-7.14, and 4-8.4(c)). These rules apply to posts on social media sites such as Twitter, Facebook, Instagram and LinkedIn. (For example, do not allow family members to praise your legal services on social media if they have not been a client.)
- Social media sites are not a way to circumvent the lawyer advertising rules. Information appearing on networking sites that is used to promote the lawyer or law firm is subject to the lawyer advertising rules and must comply with all substantive lawyer advertising rules (see Subchapter 4-7).
- Invitations sent directly from a social media site via instant message to a third party to view or link to the lawyer's page on an unsolicited basis for the purpose of obtaining, or attempting to obtain, legal business are solicitations and violate Rule 4-7.18(a), unless the recipient is the lawyer's client, former client or relative, has a prior professional relationship with the lawyer or is another lawyer.
- There is no expectation of privacy on the Internet. There is no such thing as a true delete of information. Privacy settings are not a safeguard to protect what you post, and information is stored forever.
- In general, if you would be ashamed to content on a billboard, do not post it.
- Do not disparage or seek to humiliate the judicial system, judges, opposing counsel, clients or others via social media (Rules 4.82 and 4.8-4(d)).
- Do not post inappropriate or unprofessional pictures.
- If misleading or dishonest information has been posted on your social media profile or account by others, remove the information.
- Visit your social media profile or account on a consistent basis to ensure that you are not running afoul of the rules of the disciplinary system or any of the lawyer advertising rules. If you are unable to actively engage on a social media site, deactivate your account to avoid inappropriate commentary being placed by hackers in your name.
- Responsible participation in social media is time-consuming. Keeping abreast of one social media site may be all that your schedule will allow.
- If you do not know much about the social media site, educate yourself before joining.
- Change your password frequently to avoid hackers and spam messages being sent to those with whom you interact.
- Log off after visiting your social media page.
- Delete browsing history, saved passwords and cookies on a regular basis to secure your social media accounts from hackers.

Social media can be a fun way for your practice to reach an entirely new audience. Following these tips will keep you safe and within the rules.

V. Telephone/Cell Phone

A. Telephone

Telephone calls frequently serve as introductions that could lead to a new client or business venture. Telephone conversations also provide an efficient means of negotiating, scheduling and generally informing all parties as a case progresses. It is best practice to:



- Answer a call before the fourth ring.
- Set your phone to divert to voicemail or an alternate line where another person or service will answer after the fourth ring.
- Before answering, determine whether you can devote your full attention to the caller; if not, allow it to go to voicemail and return the call within a reasonable amount of time.
- Ask for clarification – “If I understand you correctly ...”
- Take notes.
- If you need to place the caller on hold, ask first and assure it will not be long (15-30 seconds maximum). If you need longer, ask if you can return the call later.
- Consider whether the conversation is better suited for a face-to-face meeting.
- Place the caller on hold if seeking assistance of a co-worker rather than muffle the phone with your hand.
- If you need to transfer the caller, advise and provide the extension in case the caller is disconnected.

Lawyers should train their support staff to adopt these principles. Telephone calls cannot be recorded without the consent of all parties and generally are not recorded as a business practice. For communications that need to be memorialized, consider either a written communication or a telephone call followed by written confirmation.

B. Cell Phone

Most people use a cell phone on a daily basis and keep it close at all times. Use cell phones with caution, remaining mindful that conversations conducted in public regarding client affairs may inadvertently disclose confidential information to others (Rule 4-1.6). When using a cell phone, it is best practice to:



- Keep your voice low. Unless necessary, do not place or accept phone calls when you are in locations that will make it difficult for you to be heard.
- Ensure your phone is off or silenced when entering court or meetings. Federal courthouses have strict rules regarding cell phones.
- Keep conversations private. If you are expecting an important call or one that deals with confidential matters, remove yourself from the company of others. Be cautious of personal space and keep several feet from others when conducting legal matters.
- Know when to call. Best practice is normal business hours, which are 8 a.m.-5 p.m., unless you are authorized to call at other times. Keep time zones in mind.
- Use a speaker phone only when you are alone. Advise callers when you put them on a speaker phone.

C. Hostility via the Telephone/Cell Phone

Dealing with an angry person over the phone requires a patient and thoughtful response. As lawyers, we pledge to “abstain from all offensive personality.” It is best practice to:

- Keep your composure. Attempting to combat an angry caller will only escalate the situation.
- Listen. Figure out what is causing the hostility and begin to generate ideas on how to resolve the issue.
- Do not interrupt. Let the caller vent. If you cut the caller off, it will make constructive communication more difficult.
- Be empathetic. Is the anger valid? Indicate that insults and disrespect are not acceptable, but attempt to understand and address the root of the issue.
- Ask questions. Make sure you truly understand the situation.
- Seek a solution. Indicate you will do your best to resolve the matter.
- Apologize. We all make mistakes; if an apology is appropriate, offer one.
- Get solutions approved. Do not impose a solution; get the caller to agree.
- If all else fails, put the phone down. Politely explain that calmer heads may prevail and indicate that the conversation should be resumed at a later time. It is not ideal, but

sometimes it is your best option. Do not feel pressured to resolve the matter; the person could be having a bad day. Know when to end the call and move on.

D. Setting Voicemail

Keep things simple and to the point. It is best practice to:

- Identify your name and organization.
- State that you are unavailable and any other important information.
- Ask the caller to leave a message.

Change your voicemail if you go out of the office. Return calls as promised. Best practice dictates that a person leaving a voicemail should hear from you or your assistant within 24 hours (this advice does not circumvent Rule 4-1.4 Communication). The longer you wait to return calls, the more likely your backlog will get out of hand. After you have written the message down, delete it from your voicemail box. It can be very irritating to a caller to find a voicemail box that is full.



E. Leaving a Voicemail

When leaving a voicemail it is best practice to:

- Speak slowly and leave your number at both the beginning and end of the message.
- Limit your comments to one or two matters. Keep your message short.
- Never leave a message to defend your character, establish your reputation or resolve a feud.
- Make the call's purpose clear, beyond just please return my call.
- Don't leave confidential information on a voicemail; you could have dialed a wrong number (Rule 4-1.6). If you receive a voicemail related to the representation of your client that you reasonably should know was sent inadvertently, you should promptly notify the caller (See Rule 4-4.4(b)).

Here is an example of a professional voicemail:

"Hi, this is Cathy Smith with Dale and Dale Law Firm at 112-555-1245. I am calling to let you know that I received a settlement offer in your case, and I would like to schedule an appointment with

you. Please call me at your earliest convenience to schedule an appointment. Again, this is Cathy Smith with Dale and Dale Law Firm, and you can reach me at 112-555-1245. Thank you.”

VI. Laptop/Tablet Usage in Public and Cybersecurity

The ability to take work anywhere with a laptop or tablet comes with potential threats to confidentiality (Rule 4-1.6) and security of client information. It is best practice to:

- Use a virtual private security network (VPN). A VPN set up by your company allows you to connect remotely using a secure connection.
- Keep your laptop/tablet secure. A thief can physically steal your laptop, but you can keep your information secure by using a strong access password or passcode.
- Use built-in security features. Your device may already have security features built in. Use these features to keep hackers from accessing data.
- Keep your software updated. Many updates include security patches to correct problems found in outdated versions.
- Turn off sharing. You may have your device set up so others can access documents while you are in the office, but turn off this feature when you are in public.
- Be aware of your surroundings. Not all dangers in the digital world are high-tech. Someone may simply be looking over your shoulder.
- Use a privacy screen to keep people from looking over your shoulder and seeing your data.
- Avoid “free” and “unsecured” Wi-Fi connections. Always use a Wi-Fi service or connection that encrypts your data transmission.



It is critical in this day and age to ensure that cyber dangers are taken seriously in order to protect the integrity of your data and technology resources. If you follow the news at all, you have likely heard about another business or government agency that has had to invest significant resources to recover from damage caused by a careless user or malicious actor. Below are five steps that you can take to help ensure that your technology stays safe and sound.

1. **Educate users:** Awareness of basic computer security principles can go a long way in helping to keep your information safe. Create appropriate internet usage guidelines and rules of behavior for information resources.
2. **Protect your computer and network:** Installing the latest security software, web browser, and operating system updates are good defenses against viruses, malware, and other online threats.

3. **Make backup copies of important data and information:** Regularly backup your important data. If possible, backup the data automatically and store the copies offsite.
4. **Secure your Wi-Fi:** If you have a Wi-Fi network, make sure it is secure and password protected.
5. **Use strong passwords:** Use unique, strong passwords and change them routinely. If possible, consider implementing multi-factor authentication that requires additional information beyond a password.

VII. Records Management

A core asset of every law firm and legal organization is information. Lawyers sift through enormous amounts of information daily – everything from client files to printed contracts to the emails they receive. Making sense of all this information and ensuring that it is sufficiently protected and accessible is daunting but necessary.



There are several Bar rules dealing with record-keeping. (See “Ethics Informational Packet: Closed Files,” produced by The Florida Bar’s Ethics Department.)

Records information management, often abbreviated “RIM,” encompasses the policy, processes and procedures that law office administrators employ to manage such information. RIM is the process of identifying, organizing, maintaining and accessing all of the records created or received by an organization in its day-to-day operations. These records can be electronic or paper and include virtually everything that passes through an organization’s doors. There are many reasons a firm or individual lawyer might employ a particular RIM strategy, but the most important are the most practical: improving productivity, cutting costs and complying with legislative, regulatory, Bar-mandated and internal policy requirements.

VIII. Expectations

Best practice dictates that lawyers must manage expectations in electronic communication. When dealing with a client or opposing counsel, explain to them how your office works, and that if you are not available they are welcome to speak with your staff. Let them know when you generally return calls.

Before you give out your cell phone number, consider whether it is necessary for the contact to have this access. Advise whether it is for emergency purposes only. Let contacts know if you will receive and respond to text messages. If you are leaving the office for an extended period, set an away message for your email and voicemail. If you take a long vacation, file notices of unavailability on all of your cases.

Set limits on access to you via cell phone, email and text. If you do not work on weekends, let people know and set a message on your cell phone and work phone that calls will be returned during the workweek. When expectations are established in the beginning, people will generally respect boundaries.

IX. A discussion of Ethics Issues in Electronic Communication

The increased use of technology makes it imperative that lawyers be well-versed not only in technology but also in the issues that may arise with the use of technology. The Rules Regulating The Florida Bar and various Florida Bar ethics opinions set forth guidelines and limitations of the use of technology.

A. Creating Inadvertent Relationships

Lawyers should not give off-the-cuff advice via social networking sites or other electronic communication, particularly specific advice in response to online questions, to avoid inadvertently creating a lawyer-client relationship. Ethics rules do not create lawyer-client relationships; instead, they guide the lawyer's conduct once the relationship has been established. Whether a lawyer-client relationship has been established is a legal and factual matter based on the reasonable, subjective belief of the person seeking legal advice or services, not the lawyer's intent or belief.

B. Electronic Practice

Lawyers may provide legal services over the Internet, as long as the services do not require in-person consultation with the client or court appearances (Florida Ethics Opinion 00-4). All of the Rules of Professional Conduct apply to representation over the Internet, including diligence, competence, communication, confidentiality, conflicts of interest, etc. (*Id.*). Florida Ethics Opinion 00-4 was written before adoption of Rule 4-1.2(c), which permits limited representation as long as the limitation is reasonable under the circumstances and is not prohibited by law or rule, and the client gives informed consent in writing. Rule 4-1.2(c) applies if the Internet representation is a limited form of representation.

C. Confidentiality

Many lawyers treat confidentiality as synonymous with privilege, but the two are distinct, and confidentiality is much broader. A lawyer may not disclose any information relating to a client's representation, regardless of the source, without the client's informed consent (with limited exceptions) (Rule 4-1.6). For resources on how to keep information secure, see the Records Management section.

Many confidentiality issues relate to electronic communications. For example:

- Lawyers who use cloud computing must take appropriate care to ensure confidentiality of client information (Florida Ethics Opinion 12-3).
- Lawyers who use electronic devices such as printers, copiers and scanners should be aware that those devices can store data, and take appropriate steps to secure client information (Florida Ethics Opinion 10-2).
- A lawyer who uses electronic forms of communication should take care not to inadvertently provide confidential client information via metadata (see section on metadata below) (Florida Ethics Opinion 06-2).
- When a lawyer outsources paralegal services, communication often occurs via electronic means. The lawyer should take appropriate steps to ensure confidentiality of client information, including investigating any non-lawyer services to be used and appropriately supervising the non-lawyers involved (Florida Ethics Opinion 07-2). Consider a secure client portal when using outside services.

D. Inadvertent Disclosure via Metadata

Metadata is information about a particular document or data set that describes how, when and by whom it was created, modified and formatted. It helps users revise, organize and access electronically created files. Lawyers who send documents electronically (outside the discovery context) should take appropriate steps to prevent the disclosure of confidential client information via metadata (Florida Ethics Opinion 06-2). Lawyers should not “mine” the metadata of documents sent to them electronically (*Id.*). Lawyers who receive information inadvertently via metadata (e.g., tracked changes and comments) that were clearly not intended for them must notify the sender of the receipt of the information (*Id.*). After the adoption of Florida Ethics Opinion 06-2, Rule 4-4.4(b) was adopted, which states:

(b) A lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender.

The comment provides further guidance:

Subdivision (b) recognizes that lawyers sometimes receive documents that were mistakenly sent or produced by opposing parties or their lawyers. If a lawyer knows or reasonably should know that such a document was sent inadvertently, then this rule requires the lawyer to promptly notify the sender in order to permit that person to take protective measures. Whether the lawyer is required to take additional steps, such as returning the original document, is a matter of law beyond the scope of these rules, as is the question of whether the privileged status of a document has been waived. Similarly, this rule does not address the legal duties of a lawyer who receives a document that the lawyer knows or reasonably should know may have been wrongfully obtained by the

sending person. For purposes of this rule, "document" includes email or other electronic modes of transmission subject to being read or put into readable form.

Some lawyers may choose to return a document unread, for example, when the lawyer learns before receiving the document that it was inadvertently sent to the wrong address. Where a lawyer is not required by applicable law to do so, the decision to voluntarily return such a document is a matter of professional judgment ordinarily reserved to the lawyer. See Rules 4-1.2 and 4-1.4.

Microsoft Word documents can contain the following types of hidden data and personal information:

- Comments, revision marks from tracked changes, versions and ink annotations.
- Document properties and personal information.
- Headers, footers and watermarks.
- Hidden text.
- Document server properties.
- Custom XML data.

In Microsoft Word, the Document Inspector can be used to find and remove hidden data and personal information in Word documents. Refer to the help function to search for instructions specific to a particular version of Word.

E. Impugning Integrity of Judges

Electronic communications create the possibility that lawyers may impugn the integrity of a judge, which is prohibited under the rules. Social media and blogging in particular create a situation in which lawyers may post information without thinking about the potential consequences (Rule 4-8.2 and *The Florida Bar v. Conway*, Case No. SC08-326 (2008)).

F. Communication with/Investigating Witnesses

A lawyer generally may view the public social networking pages of a witness. A lawyer generally may subpoena the social networking page of a witness (See New York City Ethics Opinion 2010-2). A lawyer may or may not be able to "friend" an unrepresented witness using the lawyer's own name and profile. Although at least one state has taken the position that a lawyer may do so, The Florida Bar Professional Ethics Committee has not addressed the issue and may take the position that any friend request would have to clearly indicate that a lawyer is making the request in a representational capacity (New York City Ethics Opinion 2010-2).

Rule 4-4.3 prohibits a lawyer from "stating or implying the lawyer is disinterested." A lawyer also "may not engage in conduct involving fraud, dishonesty, deceit or misrepresentation" under Rule 4-8.4(c), nor violate the rules of conduct through an agent under 4-8.4(a). Thus, a lawyer may not

create a false social networking profile to “friend” an unrepresented witness to obtain information, or use an investigator to create a false profile to make a “friend” request (New York City Ethics Opinion 2010-2). A lawyer also may not use an investigator or other third person to “friend” an unrepresented witness to obtain possible impeachment material, because use of the third party is deceptive (See Philadelphia Ethics Opinion 2009-02).

G. Communicating with Represented Persons via Social Networking Sites or Other Electronic Means

A lawyer may access the public pages of an opposing party’s social networking site (See New York State Bar Ethics Opinion 843 (2010)). A lawyer may subpoena an opposing party’s social networking site pages, including private portions of the profile (See *Romano v. Steelcase, Inc.*, 907 N.Y.S.2d (N.Y. Sup. 2010)). A lawyer may not make a “friend” request to high-ranking employees of a represented corporation that is the defendant in a lawyer’s case who have supervisory authority, whose statements can be imputed to the corporation, or who can bind the corporation. They are considered represented for purposes of the ex parte rule (See, San Diego Ethics Opinion 2011-2; Rule 4-4.2, 4-8.4(c)). A lawyer would not be able to use an investigator to do so either (Rule 4-4.2, 4-8.4(c) and 4-8.4(a)).

A lawyer should be careful about use of “reply all.” A lawyer should not assume that an opposing counsel has given consent to direct communication with the opposing counsel’s client merely because the opposing counsel has copied the opposing counsel’s own client on an email. (See Alaska Ethics Opinion 2018-1; Kentucky Ethics Opinion E-442; New York City Bar Opinion 2009-1 .) Lawyers should also not copy their own clients on email because it risks a client “replying all” and waiving lawyer-client privilege or confidences. A better practice is to blind copy a client on email or forward an email to the client after sending it to opposing counsel. *Id.*

H. Social Networking, Electronic Communication and Judges

Judges should be careful regarding social networking. In Florida, a judge who is a Facebook “friend” of a lawyer who appears before the judge is not necessarily subject to disqualification according to *Herssein and Herssein, P.A. v. United Services Automobile Association*, 271 So.3d 889 (Fla. 2018). However, in *Herssein*, a concurring opinion “strongly urge[s] judges not to participate in Facebook.”

Judges also should avoid the potential for ex parte communications – at least one judge has received a public reprimand for ex parte communications on Facebook with a lawyer for a party in a pending matter before him (See North Carolina Judicial Standards Commission 08-234). Similarly, judges should avoid ex parte communications via email. Judges should consider not communicating via email to avoid accidental ex parte, but if a judge chooses to communicate via email, the judge should be careful to copy both parties or their lawyers. See *In re Contini*, 205 So.3d 1281 (Fla. 2016).

Judges should be careful regarding their campaign activities relating to social media. In Florida, judges' election committees may have social networking sites that comply with campaign requirements and may allow lawyers to list themselves as "fans" as long as the committees/judges do not control who may list themselves as fans (See Florida Judicial Ethics Advisory Opinion 2009-20).

I. Social Networking and Mediators

In Florida, a mediator may "friend" lawyers and parties appearing before the mediator on the mediator's social networking page and may become a "friend" on the pages of parties or lawyers appearing before the mediator. However, doing so may limit a mediator's ability to handle future mediations, as "friending" may create an appearance that the party or lawyer can influence the mediator, and the mediator would therefore lack the required impartiality (See Florida Mediator Ethics Advisory Opinion 2010-001).

J. Social Networking and Jurors

Lawyers may view public portions of prospective jurors' networking sites. However, lawyers may not "friend," contact, communicate or subscribe to Twitter accounts of jurors. Lawyers also may not make any misrepresentation or engage in any deceit in viewing jurors' social networking sites (See New York County Ethics Opinion 743 (2011); New York City Formal Opinion 2012-2). Lawyers must bring juror misconduct to the court's attention following rules on court and juror contact (*Id.*; see also Rule Regulating The Florida Bar 4-3.5). Lawyers also should be mindful of any rules of civil or criminal procedure that address juror contact (e.g., Fla. R. Civ. Pro. 1.431(h), Fla. R. Crim. Pro. 3.575, which prohibit a lawyer from communicating with a juror after trial unless the lawyer has legal grounds, has filed a motion and has obtained an order permitting the contact).

Juror misconduct during trials relating to social media includes: researching information on the Internet, posting real time information about ongoing trials, "friending" a defendant in an ongoing trial and polling friends to determine the juror's verdict (e.g., "Social Media, Jury Duty a Bad Mix," *Miami Herald*, May 5, 2012).

Resources

The Florida Bar

850-561-5600

800-342-8060

www.floridabar.org

The Henry Latimer Center for Professionalism

850-561-5747

www.flabar.org/professionalism

The Florida Bar Ethics and Advertising Department

850-561-5780

Ethics Hotline (for Florida Bar Members Only)

800-235-8619

www.floridabar.org/ethics

FLA, Inc. (Florida Lawyers Assistance – Substance Abuse Help)

800-282-8981

www.fla-lap.org

The Florida Bar’s LegalFuel

866-730-2020

www.legalfuel.com

The Florida Bar Attorney Client Assistance Program (ACAP)

850-561-5673

866-352-0707

www.floridabar.org/ACAP

The Florida Bar Unlicensed Practice of Law

850-561-5840

www.floridabar.org/UPL

Florida Board of Bar Examiners

850-487-1292

www.floridabarexam.org