Technology Ethics for Lawyers

Joseph A. Corsmeier, Esquire
Law Office of Joseph A. Corsmeier, P.A.
2999 Alt. 19 Suite A
Clearwater, Florida 34683
Office: (727) 799-1688
jcorsmeier@jac-law.com

Technology ethics topics

- Technology competence
- Model Rule 1.1 – technology competence
- Zoom and Alexa and other Devices
- Fee Agreement disclaimers
- E-portal Filing
- Remote Online Access to Client and Firm Files
- Electronic File Storage and Cloud Computing
- Outsourcing and Protection of Client Confidentiality
- Digital Storage Devices
- Social Media
- E-mails and Reply All
- Unsolicited information on website

Technology competence

- The comment to Model Rule 1.1 states that a lawyer should keep up with changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all CLE requirements.
- Rule 1.1 requires that lawyers understand the benefits and risks associated with relevant technology
- What is that? No definitions and this is somewhat of a moving target
- Where do lawyers go to obtain hands-on knowledge of technology in mobile devices, computers, social media platforms, and the dozens of apps and software?
- Can lawyers depend upon expertise of third-party software and technology vendors? Yes, if properly vetted
- Lawyer supervision of vendor is certainly required.

Technology ethics: using Zoom

- Using Zoom or other online meeting platform presents additional challenges.
- Require a passcode on the invitation; however, invitees can circulate the access information
- Create a waiting room for access. Identify before permitting access to meeting.
- This is the best security precaution; however, it is difficult a large group of attendees)
- Lock the meeting when it begins.
- Limit screensharing to allow one person at a time or host only
- Remove unauthorized participants.

Technology ethics: attending Zoom meetings

- Auto-mute audio when entering Zoom meeting
- Auto-hide video when entering meeting
- Use a virtual background, if necessary
- Be careful about sharing screen
- Determine whether you being recorded.

Technology ethics: Alexa and other devices

- Do Alexa and other devices in the home (and office) present a security (and potential ethics) issue?
- Working from home and confidential communications.
- Turning the device off until in use is one way to address this.
- Set up delete by voice (instructions on web)
- Ask what Alexa or the other device heard tell me what you heard
- Delete previous recordings
- Unplug or cover device
- Address same issues with cell phone, computer and I-Pad microphones and camera

Technology ethics: e-portal filing

- Florida Bar Ethics Opinion 12-2 (June 22, 2012)
- A lawyer may provide their log-in credentials to the E-Portal to trusted nonlawyer employees for the employees to file court documents that have been reviewed and approved by the lawyer, who remains responsible for the filing. The lawyer must properly supervise the nonlawyer, should monitor the nonlawyer's use of the E-Portal, and should immediately change the lawyer's password if the nonlawyer employee leaves the lawyer's employ or shows untrustworthiness in use of the E-Portal.

- Florida Bar Ethics Opinion 87-11 (Reconsideration) (June 27, 2014)
- A lawyer may permit a nonlawyer to place the lawyer's signature on solely electronic documents as permitted by Florida Rule of Judicial Administration 2.515 and only after reviewing and approving the document to be signed and filed. The lawyer remains responsible for the document.

Technology ethics: e-portal filing

- *In the Matter of: John A. Goudge*, No. 1024426, Commission No. 2012PR00085.
- Associate at Chicago law firm was responsible for contract cases from USDOJ to represent U.S. in debt collection cases involving student loans.
- Under lawyer's supervision and direction, non-lawyer assistant prepared complaints and exhibits and non-lawyer assistants/paralegals filed complaints and exhibits with the Ill. N. U.S. District Court for the Northern District of Illinois' CM/ECF (e-filing) system.
- CM/ECF requires box be checked stating that filings are in compliance Fed. Civil Proc. Rules and personal identifying information was redacted; however, confidential information was not redacted and became available to public and viewable on court's website.
- Lawyer admitted failure to make reasonable efforts to supervise non-lawyer, expressed remorse, and received reprimand.

Technology ethics: remote access to electronic client files

- New York State Bar Ethics Opinion 1019 (8/6/2014)
- Confidentiality; Remote Access to Firm's Electronic Files
- A law firm may give its lawyers remote access to client files, so that lawyers may work from home, as long as the firm determines that the particular technology used provides reasonable protection to client confidential information, or, in the absence of such reasonable protection, if the law firm obtains informed consent from the client, after informing the client of the risks.

Technology ethics: electronic file storage

- Florida Bar Ethics Opinion 06-1 (April 10, 2006)
- Lawyers may, but are not required to, store files electronically unless: a statute or rule requires retention of an original document, the original document is the property of the client, or destruction of a paper document adversely affects the client's interests. Files stored electronically must be readily reproducible and protected from inadvertent modification, degradation or destruction.

Technology ethics: "cloud computing"

- Florida Bar Ethics Opinion 12-3 (January 25, 2013)
- Lawyers may use cloud computing if they take reasonable precautions to ensure that confidentiality of client information is maintained, that the service provider maintains adequate security, and that the lawyer has adequate access to the information stored remotely. The lawyer should research the service provider to be used.
- New York State Bar Ethics Opinion 842 suggests the following steps involve the appropriate due diligence:
- Ensuring that the online data 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;
- Investigating the online data storage provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances;
- Employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored.

Technology ethics: electronic/digital outsourcing: conflicts and confidentiality

- Florida Bar Op. 07-02 (January 18, 2008).
- A lawyer is not prohibited from engaging the services of an overseas provider to provide paralegal assistance as long as the lawyer adequately addresses ethical obligations relating to assisting the unlicensed practice of law, supervision of nonlawyers, conflicts of interest, confidentiality, and billing. The lawyer should be mindful of any obligations under law regarding disclosure of sensitive information of opposing parties and third parties.
- Of particular concern is the ethical obligation of confidentiality. The inquirer states that the foreign attorneys will have remote access to the firm's computer files. The committee believes that the law firm should instead limit the overseas provider's access to only the information necessary to complete the work for the particular client. The law firm should include "contractual provisions addressing confidentiality and remedies in the event of breach, and periodic reminders regarding confidentiality."

Technology ethics: digital storage devices

- Florida Bar Ethics Opinion 10-2 (September 24, 2010)
- "A lawyer who chooses to use Devices that contain Storage Media such as printers, copiers, scanners, and facsimile machines must take reasonable steps to ensure that client confidentiality is maintained and that the Device is sanitized before disposition, including:
- (1) identification of the potential threat to confidentiality along with the development and implementation of policies to address the potential threat to confidentiality;
- (2) inventory of the Devices that contain Hard Drives or other Storage Media;
- (3) supervision of nonlawyers to obtain adequate assurances that confidentiality will be maintained; and
- (4) responsibility for sanitization of the Device by requiring meaningful assurances from the vendor at the intake of the Device and confirmation or certification of the sanitization at the disposition of the Device."

Technology ethics: metadata

- ABA Formal Opinion 06-442 and Formal Opinion 05-437
- No explicit duty regarding metadata is imposed, but a number of methods for eliminating metadata (including "scrubbing," negotiating a confidentiality agreement, or sending the file in a different format) are suggested for attorneys who are "concerned about the possibility of sending, producing, or providing to opposing counsel a document that contains or might contain metadata." [06-442]
- **"Mining" of metadata is not prohibited**. [06-442]
- ABA Model Rule 4.4(b) "obligates the receiving lawyer to notify the sender of the inadvertent transmission promptly" but "does not require the receiving lawyer either to refrain from examining the materials or to abide by the instructions of the sending lawyer." [05-437]

Technology ethics: metadata

- Florida Bar Ethics Opinion 06-2 (September 15, 2006)
- A lawyer who is sending an electronic document should take care to ensure the confidentiality of all information contained in the document, including metadata.
- A lawyer receiving an electronic document **should not try to obtain information from metadata** that the lawyer knows or should know is not intended for the receiving lawyer.
- A lawyer who inadvertently receives information via metadata in an electronic document should notify the sender of the information's receipt. The opinion is not intended to address metadata in the context of discovery documents.

Technology ethics: social media

- Do not unintentionally create an attorney-client relationship
- ABA Formal Opinion 10-457 states that by enabling communications between prospective clients and lawyers, websites may give rise to inadvertent lawyer-client relationships and trigger ethical obligations to prospective clients under the rules.
- Use of disclaimers in a lawyer's or a law firm's social media profile or in connection with specific posts may help avoid inadvertently creating attorney-client relationships (of course the lawyer's or law firm's online conduct and communications must be consistent with the disclaimer).
- South Carolina Ethics Opinion 12-03 concluded that "[a]ttempting to disclaim (through buried language) an attorney-client relationship in advance of providing specific legal advice in a specific matter, and using similarly buried language to advise against reliance on the advice is patently unfair and misleading to laypersons."

Technology ethics: social media

- A lawyer cannot attempt to gain access to non-public social media content by using subterfuge, dishonesty, deception, pretext, false pretenses, or an alias.
- In the recent case of *John J. Robertelli v. The New Jersey Office of Attorney Ethics (A-62-14) (075584),* NJ Supreme Court ruled that attorney committed disciplinary rule violations for improperly accessing an opposing party's Facebook page. Court withheld formal discipline because offense occurred in 2008.
- Ethics opinions in Oregon (Op. 2013-189), Kentucky (Op. KBA E-434), New York State (Op. 843), and New York City (Op. 2010-2) concludes that lawyers are not permitted (either themselves or through agents) to engage in false or deceptive tactics to get around a social media users' privacy settings to reach non-public information.
- Ethics opinions by the Philadelphia Bar Association (Op. 2009-02) and the San Diego County Bar Association (Op. 2011-2), among others, conclude that lawyers must affirmatively disclose their reasons for communicating with the third party.

Technology ethics: social media

- Florida Bar Advisory Opinion 14-1 (approved June 25, 2015)
- Advising client to change privacy settings
- "A personal injury lawyer may advise a client pre-litigation to change privacy settings on the client's social media pages so that they are not publicly accessible. Provided that there is no violation of the rules or substantive law pertaining to the preservation and/or spoliation of evidence, the lawyer also may advise that a client remove information relevant to the foreseeable proceeding from social media pages as long as the social media information or data is preserved."
- This advisory opinion is consistent with NYC Lawyers Association Ethics Opinion 745 (2013) which states that a lawyer may advise client to use highest level of privacy setting on the client's social media pages and may advise client to remove information from social media page prior to litigation, regardless of its relevance to a reasonably foreseeable proceeding, as long as removal does not violate substantive law regarding preservation and/or spoliation of evidence.

Technology ethics: social media posts and blogs

- Social media profiles, posts, and blogs can be advertising
- Lawyer blogs will be advertisements if primary purpose is to obtain employment/clients
- Blogs must be informational and educational.

Technology ethics: negative reviews and blogs

- Lawyers cannot disclose privileged/confidential information in blogs and in responding to internet "complaints"
- Georgia Supreme Court imposed reprimand on lawyer who violated attorney/client confidentiality in response to negative reviews that client had made on the internet "consumer Internet pages". *In the Matter of Margrett A. Skinner*, Case No. S14Y0661 (Ga. Supreme Court 5/19/14) .
- Illinois Supreme Court suspended assistant public defender for 60 days for, inter alia, disparaging judges and blogging about clients and implying in a post that a client committed perjury. *In re Peshek*, M.R. 23794 (Ill. SC May 18, 2010).
- NYSBA Ethics Opinion 1032 (October 30, 2014) states that lawyers cannot reveal client confidences solely to respond to former client's criticism on lawyer-rating website.

Technology ethics: social media

- Be careful communicating with unrepresented third parties
- A lawyer (or lawyer's agent/paralegal) may not attempt to gain access to non-public social media content by using subterfuge, dishonesty, deception, pretext, false pretenses, or an alias.
- Ethics opinions in Oregon (Op. 2013-189), Kentucky (Op. KBA E-434), New York State (Op. 843), and New York City (Op. 2010-2) concluded that lawyers are not permitted (either themselves or through agents) to engage in false or deceptive tactics to circumvent a social media users' privacy settings to reach non-public information.
- Ethics opinions by the Philadelphia Bar Association (Op. 2009-02) and the San Diego County Bar Association (Op. 2011-2), among others, concluded that lawyers must affirmatively disclose their reasons for communicating with the third party.

Technology ethics: e-mail encryption, storage system, and backup

- Email encryption obscures the content of the email in order to prevent people other than the sender and the receptor from reading it.
- System encryption makes the data of a desktop or laptop computer inaccessible or illegible without a passkey regardless of the application with which the file was created.
- Backup system should be encrypted/secure as well. Many portable storage drives will allow encryption of backup data.
- See: ABA article - FYI: Playing it Safe With Encryption http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/FYI_Playing_it_safe.html

Technology Ethics: copying client with email and reply all

- NYSBA Ethics Op. 1076 (Dec. 2015).
- Although it is not deceptive for a lawyer to send client blind copies of communications with opposing counsel, there are reasons not to send an email to the client with either "cc:" or "bcc".
- Copying the client would disclose the client's e-mail address and could be deemed by opposing counsel to be an invitation to send communications to the inquirer's client.
- Sending the client a blind copy may initially avoid the problem of disclosing the client's email address; however, it raises other problems if the client responds to the e-mail by "reply all."

Technology Ethics: employer's lawyer receipt of employee's e-mail communications with counsel

- ABA Formal Opinion 11-460 - Duty when Lawyer Receives Copies of a Third Party's E-mail Communications with Counsel (August 4, 2011)
- When an employer's lawyer receives copies of an employee's private communications with counsel, which the employer located in the employee's business e-mail file or on the employee's workplace computer or other device, **neither Rule 4.4(b) nor any other Rule requires the employer's lawyer to notify opposing counsel of the receipt of the communications**. However, court decisions, civil procedure rules, or other law may impose such a notification duty, which a lawyer may then be subject to discipline for violating. If the law governing potential disclosure is unclear, Rule 1.6(b)(6) allows the employer's lawyer to disclose that the employer has retrieved the employee's attorney-client e-mail communications to the extent the lawyer reasonably believes it is necessary to do so to comply with the relevant law. If no law can reasonably be read as establishing a notification obligation, however, then the decision whether to give notice must be made by the employer-client, and the employer's lawyer must explain the implications of disclosure, and the available alternatives, as necessary to enable the employer to make an informed decision.

Technology ethics: tips

- be very careful if you allow text messages with clients
- be sure you have permission to text the person
- texts are accessible/hackable and are not permanent
- expectation of privacy v. e-mails?
- use of electronic devices in public- confidentiality issues
- do not use public wi-fi in public place for confidential communications-
- use VPN when using outside/public wi-fi.
- keep your laptop/tablet secure
- use built-in security features
- turn off sharing
- be aware of surroundings
- consider using privacy screen

Technology ethics: tips

- use available social media platforms but be careful using them
- consider positive client reviews/endorsements and testimonials and follow the rules
- endorsements by other lawyers typically permitted
- handle negative posts professionally-not online unless anonymous
- if you blog, do not advertise! Provide relevant information/education
- develop appropriate social media strategy and policy
- actively monitor/manage your professional social media presence and online reputation
- be aware of lawyer advertising rules which now apply to all media
- keep things private
- modify privacy and search settings on your Facebook, Twitter, LinkedIn, or other social network accounts.
- take advantage of the privacy features on your blog or personal website.
- no expectation of privacy

The End

- Thanks for your attention
- Stay safe and be careful out there!