Legal Ethics and Technology

Col Linell A. Letendre
Maj Timothy Goines

Overview

• Introduction
• Applicable Rules
• Scenarios
  o Cloud Computing
  o Working from Home
  o Metadata
  o Receiving Inadvertent Attorney-Client Information
  o “Friend” Requests
  o Law of War
• Questions
Applicable Rules


Model Rule 1.1 - Competence

• “A lawyer shall provide competent representation to a client....”

• Comment 8 (2012): “… a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology ....”
Model Rule 1.3 - Diligence

• “A lawyer shall act with reasonable diligence and promptness in representing a client.”

Model Rule 1.6(a) – Confidentiality Of Information

• “A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent ....”
Model Rule 3.5 – Impartiality And Decorum Of The Tribunal

• “A lawyer shall not:
  
  (a) seek to influence a judge, juror, prospective juror or other official by means prohibited by law;

  (b) communicate ex parte with such a person during the proceeding unless authorized to do so by law or court order ....”

Model Rule 4.2 – Comm With Person Represented By Counsel

• “... 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 ....”
Model Rule 4.4(b) – Respect For Rights Of Third Persons

• “A lawyer who receives a document or electronically stored information relating to the representation of the lawyer's client and knows or reasonably should know that the document or electronically stored information was inadvertently sent shall promptly notify the sender.”

• Comment 2

Model Rule 5.3(b) – Responsibilities Regarding Nonlawyer Assistance

• “A lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer.”
Model Rule 8.4 – Misconduct

• “It is professional misconduct for a lawyer to:

(c) engage in conduct involving dishonesty, fraud, deceit or misrepresentation.”
Scenario #1

• It’s Thursday at the Legal Office and that means its “Will Day.” You sit down with your first client and he mentions that he is about to file for divorce from his wife, TSgt Smith, who works in the Comm Squadron. He would like to update his will to exclude her from the will and give everything to his new girlfriend, Trixie.
• You create the will, as directed, and save the file to the shared drive.
• Any issues?

Scenario #2

• Mr. Smith has also asked you for help on filling out the pro se divorce packet. Needing some more fodder for your LAMP Award package, you agree. Late in the day, you’re swamped, so you ask your paralegal to assist you in completing it.
• To increase efficiency, you decide to upload the file to Google Docs, so you and your paralegal can work on the file simultaneously.
• Any issues?
Scenario #3

- Your new Wing Commander has decided to streamline taskers by requiring that all items be processed through TMT.
- Your base processes about 100 administrative discharges per year. The Wing Commander informs you that he wants all of these processed through TMT.
- Any issues?

Scenario #4

- Congratulations, you’ve just been notified that TJAG has selected your office for an Article 6 Inspection. In 3 months, the MAJCOM will be arriving at your base to go through the checklist.
- As part of this inspection, they’ve asked you to complete the checklist in MICT and upload all your supporting documentation. This includes a number of example legal reviews, including CDIs, Referral, and Sexual Assault Legal Reviews.
- Any issues?
Cloud Computing

- Rules: 1.1, 1.3, 1.6, and 5.3
- Standard: Exercise reasonable care to prevent unintended disclosure
  - Universal in all states that have addressed it
- No set rules because technology changes

Reasonable Care (Factors*)

- The nature of the technology in relation to more traditional counterparts (i.e. e-mail versus mail).
- Reasonable precautions possible to improve the security of a given technology.
- Limitations on who can monitor the use of technology and disclose activity.
- The lawyer's own level of technological competence, and whether it's necessary to consult with an expert.
- Legal ramifications to third parties for intercepting or otherwise interfering with electronic information.
- The sensitivity of the data.
- Impact of possible disclosure on the client.
- Urgency of the situation.
- Client instructions.

* California Ethics Opinion 2010-179
Cloud Computing Recommendations

• Ask questions:
  o How does the system work?
  o What security is in place?
  o Who can change the security settings?
  o Who has access?
  o Can I limit access?
  o Can I protect the document/data?
  o How sensitive is the data?

• If you don’t understand the technology, find someone who does (or consult an expert)

• Take reasonable precautions
  o Email - Encryption not required, but recommended
  o Use “strong” passwords / don’t repeat passwords

Scenario #5

• It’s been a long Thursday, so you decide to head home. As you drive home, you realize that you forgot to finish Mr. Smith’s pro se filing. But, you’re in luck because you emailed the filing to your work account.

• When you arrive home, you boot up your wife’s MacBook Pro (or Surface Pro), login to your work email, and download the file to your desktop. After working on the file, your wife asks to use the computer to send a quick email to her best friend who, coincidentally, is also named Trixie.

• Any issues?
Scenario #6

• After your wife is done, you grab the computer, unplug it, and head downstairs to do some more work without interruption. You logon to your home wireless, which is unsecured because you get tired of having to remember the password.
• Any issues?

Scenario #7

• As you’re working, your wife reminds you that tonight is her weekly book club meeting and she is hosting. You decide to head to your favorite café (Panera) to complete your work.
• When you arrive, you order a bowl of Vegetarian Autumn Squash Soup and logon to their free wifi. You finish the file and email it to yourself again.
• Any issues?
Scenario #8

• While you are about to leave Panera, you realize that you need to review a charge sheet from your upcoming case, US v. Jones. You open it up, review the specifications, and then try to forward it to your work email.
• For some reason, your work email stops responding (you’ve been having CAC issues lately), so you decide to send it to your personal gmail account, planning to download it later.
• Any issues?

Working from Home

• Rules: 1.1, 1.3, 1.6, and 5.3
• Standard: Exercise reasonable care to prevent unintended disclosure
  o Universal in all states that have addressed it
• Same Factors to consider
## Working from Home Recommendations

- **Shared Computers**
  - Use separate User Accounts
  - Password protect files/folders

- **Secure home network (use strong password)**
  - Enable guest account

- **Public Wifi**
  - Use VPN
  - Encrypt connection

## Scenario #9

- It’s Friday (finally!), so you head into work hoping for a relaxing day. You arrive and open your email to find a motion that you wrote sent back to you from the senior counsel on the case. Opening the file, you find a number of tracked changes, along with comments on your argument and a detailed explanation of why the senior counsel thinks that you will lose the argument.
- You review (and accept) all the changes and delete the comments before filing the motion.
- Any issues?
Metadata

• Documents that may contain metadata:
  o Motion
  o PTAs
  o MSPB Filings
  o Other Documents that contained Attorney-Client Privileged Info or Attorney Work Product

• Rules: 1.1, 1.3, 1.6, and 5.3
• Standard: Exercise reasonable care to eliminate confidential information in metadata
• Same Factors to consider
Metadata Recommendations

• Sanitize all metadata before sending

• Save file in another format (PDF) to eliminate metadata

Scenario #10

• It's Friday afternoon and you receive an email from opposing counsel in US v. Jones. The email contains a long email “trail” with twenty (20) emails with responses. At the very bottom, you see that the last two emails contain an exchange between the Attorney and the Accused discussing potential PTA terms and the possibility that he may plead guilty.

• What do you do?
Scenario #11

- As expected, you receive a PTA from the opposing counsel. You immediately open the file and review the terms. It dawns on you that you could potentially “mine” the metadata in the file to see the changes made to the file. This may reveal some “inside” information regarding the case.
- Any issues?

Scenario #12

- In preparation for your MSPB hearing (you’re a jack of all trades), you forward a draft of your argument to your legal team – your co-counsel and paralegal. As you are about to leave for the day, you see an email from your paralegal with comments on your argument. You also notice that the opposing counsel is cc’d on the email.
- What do you do?
Sending/Receiving Inadvertent Attorney-Client Information

- Examples of documents:
  - Emails
  - Motions
  - PTAs
  - MSPB Filings

- Rule: 4.4(b)
- Obligation: “promptly notify the sender”
- Return/destroy the document?
  - Not required by this rule; just notification
  - But, check state bar rules
Sending/Receiving Inadvertent Attorney-Client Information

- “Inadvertent”
  - Assume confidential information was sent inadvertently
  - If not inadvertent, no obligation to notify

- Metadata – States disagree on duty
  - CO – You can mine the document for metadata (Ethics Op 119)
    - But, must comply with Rule 4.4(b)
  - FL – should not obtain information from the metadata (Ethics Op 06-02)

Recommendations

- Receiving
  - Check state bar for rules/obligations
  - If in doubt, notify opposing counsel and return/destroy document

- Sending
  - Immediately notify receiver that it was inadvertent
  - Check state bar for rules/obligations
Scenario #13

As you are preparing for US v. Jones, you start to prepare for the victim’s testimony. In the evidence, you find a printout of the victim’s Facebook profile. Your curiosity piqued, you head to Facebook and send a “Friend” request to the victim in order to check out activity.

- Any issues?
- What if you are the defense counsel?

Scenario #14

With less than a week until trial, you start preparing for Voir Dire. In order to get a sense of your members’ leanings, you decide to check out their profiles on social media. Many of them are private, so you have to “friend” them to see their posts.

- Any issues?
- What if you “friend” the judge?
Scenario #15

- Now, you are the SJA and you found out that Lt Col Johnson is the judge appointed to US v. Jones. Lt Col Johnson and you went to JASOC together and have kept in contact with one another. In fact, you are also Facebook “friends.”
- Any issues?

“Friend” Requests

- Rules: 4.2, 5.3, and 8.4
- Four issues
  - “Friend” Victim, Don’t ID as Attorney:
    - Violation of Rule 8.4 (deception)
    - California, Philadelphia, and San Diego
  - “Friend” Victim, represented by counsel (SVC):
    - Violation of Rule 4.2 (ex parte communication)
    - San Diego (Ethics Op 2011-2)
  - “Friend” Judge/Member:
    - Violation of Rule 3.5(b)
    - ABA (Ethics Op 466)
  - SJA “Friends” with Judge
    - Creates the appearance of partiality
“Friend” Recommendations

• Don’t “friend” if not required
• Always ID yourself as an Attorney
• Be aware if they are represented by counsel
• Don’t “friend” Judges/Members
  o If already “friends,” discuss on the record
• If SJA “Friends” with Judge, discuss on record

Scenario #16

• You are counsel for the Air Force Research Labs. The engineer invited you to a meeting to discuss their newest project – a cutting edge autonomous weapon. He wants to consult with you regarding the legality of the weapon and any other thoughts you have.
• What do you do?
Autonomous Weapons

- Understand DoD guidance on Autonomous systems and LOAC principles

- Do homework on technology itself...requires ask engineers/designers a lot of questions
  - What level of autonomy will system have?
  - How has system been tested?
  - What type of control algorithms being used and why?
  - How does the system learn? Does human have check on this?
  - How if at all does system share its deductive reasoning with operator?
  - For what type of inductive reasoning does system rely on operator?

Scenario #17

- You are in the CAOC and a new target is identified - a computer network that assists the enemy’s military. It also controls a number of civilian resources (power, water, and gas).
- Is the target lawful?
- What’s the standard?
Questions