LAWYER'S DUTY OF TECHNOLOGY COMPETENCE –

WHAT SHOULD AN ETHICAL LAWYER KNOW ABOUT TECHNOLOGY?

Ana Khurtsidze

Tbilisi, Georgia

2020

AMERICAN BAR ASSOCIATION - MODEL RULES OF PROFESSIONAL RESPONSIBILITY

Comment 8 to Rule 1.1,

lawyers should "keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology."

Nowadays thirty-one states have adopted rules requiring technological competence.

WHAT TYPES OF TECHNOLOGY ARE LAWYERS USING?

- **Local technology** - primary computers, home computers, operating systems, law firm servers, mobile devices, such as laptops, smartphones and tablets, printers, scanners, copiers, external hard drives, external media, and email.
- **Cloud-based technology** - technology controlled by third parties and accessed over the Internet.

WHAT SHOULD AN ETHICAL LAWYER KNOW ABOUT TECHNOLOGY?

- Understand the cybersecurity risks and threats of an Internet connection and protect and secure client information accordingly;
- Use the Internet consistent with ethical responsibilities for client development through websites, social media, and marketing;
- Provide more efficient legal services using cloud-based systems to manage a legal practice;
- Conduct electronic discovery in litigation sometimes involving mass amounts of information requiring third-party investigative and document assembly and management services.

WHAT ARE THE TECHNOLOGICAL SKILLS?

1. Cybersecurity Norms = Reasonable security efforts to prevent

interception of confidential data (e.g. firewalls, password protection, encryption, and third party access by cloud providers)

2. Metadata and ESI = Knowledge of inadvertent receipt of information with metadata and security of confidential electronically stored information during the discovery process and course of client representation.

3. E-discovery = Performance of e-discovery based on Federal and State rules, intake norms for e-discovery, relevancy of ESI, and scrubbing metadata or conversion of documents.

4. Cloud Computing = Knowledge of cloud computing technologies and storage, third-party access, and reasonable safeguards to store data.

5. Wi-Fi Security = Basic security options, non-use of public Wi-Fi, reasonable protection(s) to prevent interception of client data, and encryption for confidential client information.

WHAT ARE THE TECHNOLOGICAL SKILLS?

6. E-mail and Encryption = Knowledge of encrypted and unencrypted email, reasonable protection to protect confidential or highly sensitive client email, and e-discovery implications for practice.

7. Virtual Law Firms = Reasonable electronic communication and accurate marketing to clients and duty to keep clients informed throughout client representation and understanding of state ethical norms for virtual lawyering.

8. Social Media = Knowledge of social media tools, development of law firm social media policies, understanding of e-discovery implications, and informed consent for client(s) when needed upon intake of case.

9. Digital Documents = Basic digital document management, use of an expert when outside attorney area of competency, prevention of interception, encryption or password protection with highly sensitive data, and scrubbing documentation for e-discovery.

10. Modern Communication Methods = Effective communication methods in addition to traditional norms, including texting, emailing, social media, and secure online or cloud client messaging services.

WHAT LAWYERS SHOULD EVALUATE WHEN USING EMAILS?

1. Communicating highly sensitive or confidential information via email or unencrypted email connections;

2. Sending an email to or from an account that the email sender or recipient shares with others;

3. Sending an email to a client when it is possible that a third person knows the password to the email account, or to an individual client at that client's work email account, especially if the email relates to a client's employment dispute with his employer;

4. Sending an email from a public computer or a borrowed computer or where the lawyer knows that the emails the lawyer sends are being read on a public or borrowed computer or on an unsecure network;

5. Sending an email if the lawyer knows that the email recipient is accessing the email on devices that are potentially accessible to third persons or are not protected by a password;

6. Sending an email if the lawyer is concerned that law enforcement agency may read the lawyer's email communication, with or without a warrant.

THANK YOU!