D. ***Increased opportunity for inadvertent disclosure of client information*** due to the greater ease of transmitting large amounts of information electronically.

An additional concern becomes the issue of the client's use of their own e-mail, cellphone, social media sites and other electronic devices and resources. It quickly becomes the lawyer's responsibility to advise and assist the client in managing those resources as well, since a compromise of client information by opposing party or counsel can be extremely detrimental to the client's matter.

II. CLIENT'S USE OF EMPLOYER'S COMPUTER

Several cases have examined what happens when employees communicate with their personal attorneys via employer-provided networks or computers. The courts analyzed whether the employer clearly reserved the right to monitor employees' electronic communications, thus eliminating any reasonable expectation of confidentiality and vitiating any claim of privilege.

III. CELL PHONES AND OTHER HANDHELD ELECTRONICS

Cell phones are routinely used by all of us as a major form of communication. While our carriers tell us the security of using cell phones has dramatically increased and the likelihood on interception of calls or other information is unlikely there are still precautions that need to be in place regarding the practice of law and the use of cell phones. Cell phones have become so much more than just a routine device to place telephone calls and have 24 hour access to communications.

Additionally, so many other electronic devices have been incorporated by lawyers to make our lives easier and more mobile, such as I Pads, Laptops, etc. The biggest risk of carrying your client information with you is a breach of security. If you leave the device, lose it, or have it stolen you risk a serious breach of client confidentiality, especially if all your client files and matters are stored electronically and accessible on this device.

Make sure that all cellphones, laptops, I Pads, etc., that are used in your firm or by you personally have the highest level of security. All cellphones should at a minimum be password protected in the event of loss or theft.

Additionally, the client needs to be advised regarding use of their cellphone as it may relate to their legal matter. Does the client use text messaging? What about Facebook posts? Or Instant Messaging?

Text messaging is only somewhat secure and is subject to spoofing. Apple says their software makes text messaging more secure, but admits that even with theirs a person can spoof another. As to how long your carrier stores your text messages: well it depends upon the carrier. The log of messages and calls usually is kept for at least a year but only some carriers retain the content of the message, and usually for a maximum of 3-5 days only. So if you're looking to subpoena a text message you have a very limited window of opportunity.