FAMILY LAW IN A DIGITAL WORLD

Top 10 Tips to Discuss with Clients

1. **Trust your instincts** If your client suspects that the abusive person knows too much, it is possible that their phone, computer, email, driving or other activities are being monitored.

2. **Plan for safety** Navigating technology is a vital step in safety planning today. Make sure you discuss with your client what technologies are being used such as: online dating, social media, Bluetooth, GPS, On-Star, and more.

3. **Change passwords** Advise your client to change all account passwords that may disclose information about their location or activities. Don't forget about changing security questions on accounts, especially if the abusive party knows the answers.

4. **Check cell phone settings** If your client is using a smartphone, check the location services in the Settings menu to see if the phone is giving away their location. Also ask your client to turn off Bluetooth when it's not being used. This can prevent the abusive party from monitoring or installing malicious software on the phone.

5. **Consider using a donated or new cell phone** If your client's cell phone was provided by the abusive party, ask if they are willing to switch to a new phone. When making or receiving private calls or arranging escape plans, try not to use the phone provided by the abusive party as it may be monitored.

6. **Use a safer computer** If an abusive party has access to your client's computer, they might be monitoring that devices activity. Ask your client to use a different computer when searching for help, looking for a new place to live, making travel plans, etc. Public computers at libraries, community centers, or internet cafés can be a safer (and cheaper) option.

7. **Search for your name on the internet** By using popular search engines like Google, Spokeo, or Bing, it is important to see what information may be being made public about your client. Start your search by entering your first and last name in quotations followed by your city and state. This will help avoid finding irrelevant information from duplicate names. Don't forget to also view the "images" portion of the search engine to see what possible pictures may be public.

8. **Update privacy settings on all social media accounts** Talk to your client about updating their privacy settings for any and all social media accounts they use. It may be important to update some of these settings to ensure that your client's location is not being compromised or that harmful information is not being shared.

9. **Ask about your records and data** Many court systems and government agencies are publishing records to the internet. Ask agencies how they protect or publish your records and request that court, government, post office, and others seal or restrict access to your files to protect your and your client's safety.

10. **Consider optional phone services** Using services like Google Voice may be a better alternative in keeping your personal phone numbers safe. With services such as these, you can sign up for one phone number and have that number forward calls and messages to up to five different phones. That way, if your client's phone number is compromised, they can log in and change one phone number rather than having to contact the phone companies and changing many.