

# Securing Electronic Data

Contributed by Jano Hanna

More and more attorneys and other professionals are utilizing mobile devices to support their law practices and their personal lives. The risk of utilizing mobile devices such as a PDA, cell phones, and even flash drives is that private information may fall into the wrong hands.

To help keep your mobile devices, as well as private client information stored within the mobile device secure, consider utilizing the following safeguards:

- Enable password protection and pins on all mobile devices, flash drives, CDs, etc. When choosing a password, do not use your address, date of birth or children names, or phone number. It is recommended that you choose a more obscure name or phrase that you can remember.
- Change passwords to your mobile devices every 3-4 months. Make sure the new password is different from the prior password.
- Do not use the same password to access all devices or online logins.
- Consider backing-up or syncing your mobile device to a stationary computer. This way you have access to information if the mobile device becomes lost or stolen.
- Clear or remove unneeded information from flash drives and CDs when not in use.
- Insure the devices in case of loss or theft.
- Disable bluetooth or wireless networking when not in use.
- Note: The new iPhone 3G offers a "remote wipe" whereby if you lose or misplace the iPhone you can remotely clear the phone of all its content. This is a great feature which allows you to secure and protect the access to private information. If the iPhone is later retrieved, you can simply re-sync the phone to re-load the wiped data.