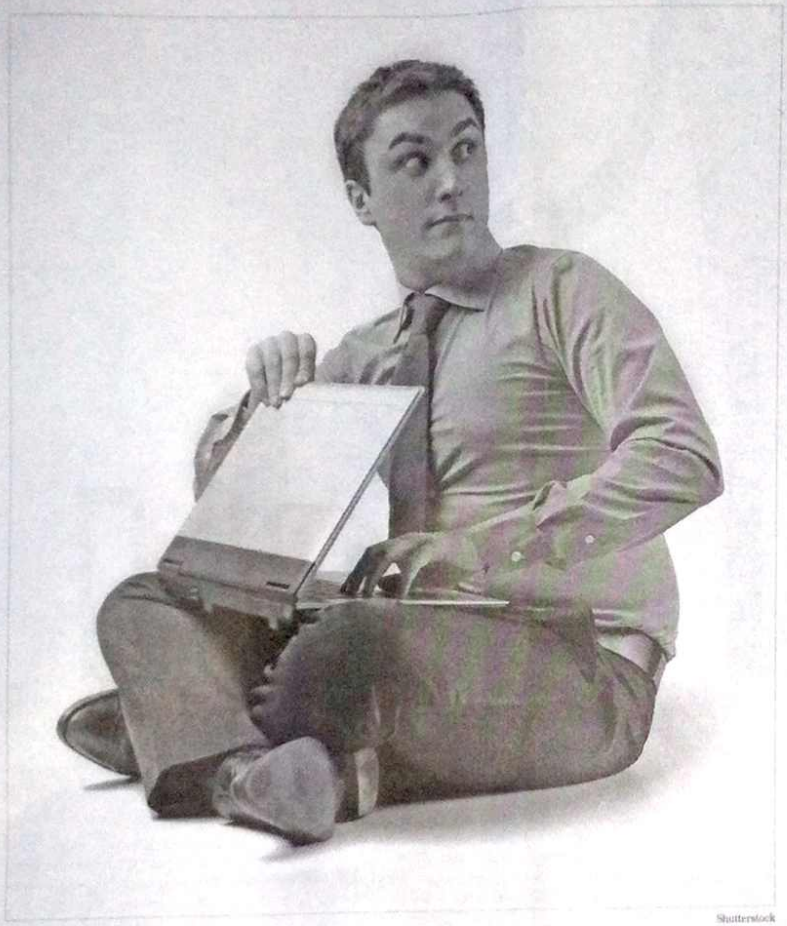
PROFESSIONAL RESPONSIBILITY

www.dailyjournal.com DAILY JOURNAL

Visual hacking: a threat to confidentiality

By Mari J. Frank



Shutterstock

Have you considered who might be viewing and collecting information about your clients and cases without your awareness? Many of us are tethered to our laptops, smartphones and other mobile devices. This exposes our clients' sensitive information to increased privacy and confidentiality vulnerabilities.

We hear daily about massive security breaches — most recently, millions of Home Depot shoppers had their personal information compromised. But security breaches are also accomplished in less remote ways. For example, there are unscrupulous employees who remove and sell electronic records on thumb drives, and negligent staff who inadvertently allow access to their computers through social engineering or by plain accident.

Inadvertent or unauthorized disclosures are particularly menacing. Given the proliferation of laptops, smartphones and other mobile devices, an under recognized yet enormous threat to confidentiality is "visual hacking" — the act of viewing sensitive, confidential and private information for unauthorized use — such as looking over someone's shoulder while they work at Starbucks or watching a neighbor type an email on a plane.

But visual hacking is not limited to public places. For instance, when an unauthorized person views confidential information on an active computer screen or hardcopy documents left on unattended desks. Many unreported breaches occur because of low-tech privacy intrusions rather than high-tech weaknesses. Law firms should consider whether lawyers or staff tend to leave files out afterhours, forget to lock file cabinets, fail to use shredders, leave computers on without password protection, or ignore other protocols to protect information.

Professional responsibility rules require us to protect our clients' personal information and keep their confidences. And our clients have a reasonable expectation that their private communications will be kept secret and securely maintained. Although it may be daunting to keep up with new laws and cases, new technology, run a practice, get paid, and employ best practices for privacy and confidentiality strategies, these multifaceted tasks are all part of lawyer competency. America Bar Association Rules of Professional Conduct, Rule 1.1 states: "A lawyer shall provide competent representation to a client. ... To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the *benefits and risks associated with relevant technology.*"

Permission is mandatory to share privileged communications, and when we no longer need to use the data, we must safely store it for a reasonable period of time, or return or destroy it completely when discarding. ABA Rule 1.6 address privacy and confidentiality issues in this context: "(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent ... (c) A lawyer shall make reasonable efforts to prevent the *inadvertent or unauthorized* disclosure of, or unauthorized access to, information relating to the representation of a client."

In addition to complying with the rules of professional responsibility, lawyers also are obligated to comply with laws regarding data privacy and security. Law offices often collect personal information such as Social Security numbers, driver's license numbers, bank account numbers, health insurance information, etc. Although there is no federal security breach law, attorneys in the 47 states that have passed security breach laws must disclose breaches, just as any other business would have to do. In California and other states, this includes printed documents that were derived from a computer, expanding the disclosure requirement to hard copies.

What to Do

With handy mobile gadgets available to use in almost any public place, we may easily become distracted and oblivious to snooping eyes around us. Even in our offices, how aware are we of visual displays of confidential data when clients, visitors, temporary employees and repair people are on the premises during the day? And who has access to our offices after hours and on weekends? We must be conscious in the office and when working remotely as to what is visible to unauthorized persons.

To address the privacy vulnerabilities while you are working at the office or remotely, take proactive steps to protect your clients and your practice. Here are some tips:

1. Create a visual privacy policy for the office. Then train, test, reward and enforce best practices.

2. Use privacy filters and privacy screen protectors for smartphones, computers, tablets and other electronic devices. Your privacy policy should require that privacy screens on devices be utilized at least while working in public places and where unauthorized persons can view screens.

3. Utilize passwords or secret design codes on smartphones and other devices. Change passwords often and after every instance of using public kiosks, in the event you could have been shoulder surfed. Be aware of your surroundings and where you are accessing sensitive information. Position your hands, body and devices to avoid intrusive onlookers.

4. Institute "timeouts" for computers and electronic devices and implement privacy settings. Lock electronic devices when not in use, activate screen savers, and set up a secure vault for remote access. Set up devices so that you may remotely erase them in case of loss or theft.

5. Implement encryption for sensitive data and utilize dual or multiple authentication practices for decryption. All parties must have the "key" to authenticate. Redact the information that needs to be secured before distribution.

6. Make sure you have shredders issued to all attorneys and personnel and place them next to copiers, fax machines and scanners. They also should be a prerequisite for all who qualify to telecommute or qualify to use secure remote network access.

7. Attach visual exposure security warning labels to all low-threat tech and tech-related devices such as scanners, printers, file cabinets, waste containers, video conferencing equipment, etc.

8. Operate on a strong "need to know only" policy when replicating or distributing information that needs to be secured. Adopt a "not in plain view" policy for desktops, conference rooms, mobile settings, teleworkers and remote activities.

Our clients depend upon us to safeguard their confidences and protect their private information from being seen by the wrong persons. Sensitive data displayed on a screen is vulnerable to viewing, either by "shoulder surfing" or by advanced optics used by sophisticated hackers. Technology is always improving, and the result will be more powerful mobile devices capable of containing mega confidential data easily accessible in public areas and facilities. Visual privacy is a crucial concern and sensitive data on screens and in plain view must be protected from risk of exposure by passersby. Visual privacy controls, such as privacy filters on computers and mobile electronic devices, along with visual privacy policies outlining specific actions, procedures, and best practices are vital to protecting confidences in the evolving practice of law.

Mari J. Frank *is an attorney-mediator and certified information privacy professional in Laguna Niguel. She may be reached at Mari@MariFrank.com.*

MARI FRANK
Attorney-mediator