BACK STORY

INSECURITY ABROAD:

DATA SAFETY FOR PRACTITIONERS AWAY FROM THE OFFICE

BY ANDREW P. DUNNING, ESQ.

Imagine the following scenario: you are out of town for a deposition and take the opportunity to catch up on some work in your downtime. You set up your laptop or tablet and pray that there is free Wi-Fi at your home away from home. You are hopeful your hotel, airport terminal or coffee shop (who are we kidding, we all know it is a Starbucks) will have the gratis network connection you need in order to respond to those accumulating emails and complete that back-burner research project or brief. The strongest password-free connection looks official enough, "RealHotel_Guest," and you quickly corroborate its legitimacy with the "FREE INTERNET" placard near the front desk. Nothing stands between you and precious productivity.

Although the above hypothetical situation seems innocuous, it actually raises legitimate security concerns for practitioners. As open public Wi-Fi becomes increasingly prevalent, so do its associated risks. Unsecured networks allow discrete access to users' browsing information or present fake login pages. If a device is not secure, nefarious individuals can access internet history, data and personal information. Indeed, not every threat is a conspicuous solicitation from a Nigerian prince or phishing scam sliding into[1] your DMs:[2] scammers can infiltrate data through "fake" Wi-Fi hotspots, unsecured websites, Bluetooth connections and other means.

Once an attorney's data is compromised, it is too late. The risks are compounded when the information is related to their clients and practice, thus invoking their professional obligations.

All Nevada attorneys have confidentiality obligations to their clients. Nevada Rule of Professional Conduct (RPC) 1.6(a), along with its parallel under the American Bar Association's Model Rules of Professional Conduct, provides that "[a] lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent" or the disclosure is otherwise authorized. In addition to duties of confidentiality, competence and diligence, attorneys have an affirmative obligation to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[3]

Comment 18 to ABA Model Rule 1.6 includes a non-exhaustive list of factors in determining the "reasonableness" of an attorney's efforts, including:

1. The sensitivity of the information;
2. The likelihood of disclosure if additional safeguards are not employed;
3. The cost of employing additional safeguards;
4. The difficulty in employing additional safeguards; and
5. The extent to which the safeguards adversely affect an attorney's ability to represent clients.

Stricter obligations associated with protected information (think HIPAA,[4] FERPA[5] or FINRA[6] regulations), and deal- or case-specific requirements (read: protective orders, data preservation, non-disclosure/confidentiality agreements, electronically-stored information discovery protocols) up the ante. Per Comment 19 to the ABA Model Rule 1.6, the reasonableness of an attorney's expectation of privacy can be determined by, among other things, the:

1. Sensitivity of the information; and
2. Extent to which the privacy of the communication is protected by law or by a confidentiality agreement.

As discussed in the March 2018 Law Practice Management issue of *Nevada Lawyer*, technological lapses and breaches in an attorney's practice can also have serious implications on both privileged communications and work-product.

Being proactive about data security is the best defense. Attorneys should avoid unknown networks and opt for safer alternatives like virtual private networks (VPN); mobile broadband (portable modems); or a cellular hotspot (phone tethering). Regardless of network-end solutions, attorneys should encrypt data on their devices, storage and email servers, whether in transit or at rest. Secure passwords (through a management program like LastPass) provide additional peace of mind, especially when combined with multifactor authentication. Licensing individual users for practice services (like cloud storage, timekeeping software or research databases), rather than sharing an account among multiple users, affords another layer of safety.

If an attorney is in a pinch, and "RealHotel_Guest" is the only option, they still can take preventative measures. Using SSL-encrypted websites for data transfers (like the old staple, DropBox), activating an encrypted device's "safe" mode, transferring only encrypted files, deactivating sharing (you can, actually, turn "AirDrop" off), and implementing firewalls, antivirus software and other protective tools can go a long way.

When you are feeling insecure (as we all occasionally do), be thoughtful about your and your clients' data: tread lightly, be proactive and, if necessary, consult a technical services company for tailored security solutions.

Special thanks to Russel E. Burkett IV of Advantage Computers in Reno, Nevada, for consulting on this Back Story article and topic. **NL**

1. "Being sent to [by said ne'er do well]."
2. "Direct Messages" according to the youths.
3. NRPC 1.6(c); see also MODEL RULES OF PROFESSIONAL CONDUCT R. 1.6(c) (2017).
4. The Health Insurance Portability and Accountability Act of 1996 and related regulations, most notably the Privacy Rule and Security Rule, found within the Code of Federal Regulations at 45 C.F.R. Part 160 and Part 164, Subparts A, C, and E.
5. The Family Educational Rights and Privacy Act of 1974 and related legislation.
6. The Financial Industry Regulatory Authority, the largest independent regulator of the United States securities industry.

ANDREW P. DUNNING is an associate attorney at Schwartz Flansburg PLLC in Las Vegas. He represents clients in a wide variety of civil matters, with an emphasis on business litigation, personal injury and transactional work. Dunning can be reached at (702) 802-2256 or Andrew@NVFirm.com.