Protecting Client Information During Remote Lawyering

BY SARAH M. MOLLECK, ESQ.

"Remote lawyering" is a concept that many attorneys are familiar with but likely few embraced until the COVID-19 pandemic shuttered our brick-and-mortar offices and found us writing briefs in our sweatpants. The pandemic prompted a swift change in how attorneys practice law, demanding a working familiarity with platforms like Zoom, Microsoft Teams and LogMeIn. Before COVID-19, about 20 percent of attorneys worked solely from home. After the pandemic, 88 percent of firms now offer remote access, 47 percent of attorneys report using their laptop as their primary workstation, 79 percent rely on the cloud to store client information and 67 percent offer electronic share-and-sign software in lieu of meeting clients in the office.[1]

Remote lawyering is expected to become a new normal, not only for attorneys but for their clients as well. The pandemic has prompted clients to seek technologically capable attorneys to expedite legal services and achieve client goals and expectations. For example, in its 2020 Legal Trends Survey, Clio reports that 69 percent of clients preferred to share documents electronically, 65 percent preferred to pay their bills online and 56 percent preferred video conferencing with their attorney to a telephone call.[2] Clients expect their attorneys to be familiar with and implement current technology to aid in the administration of their case and reduce overall cost to the client.

In fact, an understanding of current technology is part of an attorney's ethical obligation to competently represent his or her clients. Nevada Rule of Professional Conduct (NRPC) 1.1 states that, "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." Comment 8 to the Model Rules of Professional Conduct provides guidance to NRCP 1.1 by advising counsel that to maintain the requisite knowledge and skill required under Rule 1.1, "a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology … ." Indeed, given that many courts have adopted the use of videoconference technology during the pandemic to conduct arraignments, hearings, settlement conferences and trials, practitioners in Nevada must have some baseline technological understanding to adequately represent their clients. There are many indicators that courts will continue "virtual court" well after the pandemic is under control.

With all the benefits that technology offers attorneys,

however, there are attendant risks and opportunities for serious missteps that could result in a violation of the ethical rules and lead to attorney discipline. The most prevalent concern for attorneys is maintaining client confidentiality in the digital age. An attorney has an 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." NRCP 1.6. This rule invokes the competency requirement above by requiring attorneys to be knowledgeable in the steps they can take to safeguard client information from unauthorized or inadvertent disclosure.

Working remotely has increased opportunities for the breach of client information to occur. The opportunities for unauthorized disclosure can occur in a variety of ways, from inadvertent disclosure by employees to attempts by hackers to pierce security measures in place. A recent study reveals that law firms are at the top of the list of legal organizations that are targeted by ransomware, with 61 percent of attacks occurring on law firms as opposed to 22 percent on the courts.[3] Ransomware attacks have increased as law firms quickly shifted attorneys and staff to work-from-home models without putting in place appropriate security protocols. Small law firms are a particular target, with 57 percent of ransomware attacks occurring at firms with 19 or fewer attorneys, as compared with 27 percent of attacks occurring at firms with 20 or more attorneys.[4]

> **With all the benefits that technology offers attorneys, however, there are attendant risks and opportunities for serious missteps that could result in a violation of the ethical rules and lead to attorney discipline.**

Ransomware attacks often occur through phishing emails posing as legitimate requests, where the unsuspecting then click on a hyperlink and download the ransomware. Law firms are an attractive target for ransomware attacks because they host a significant amount of confidential client information in one location, as opposed to a hacker going after each client one-by-one for the information. The repercussions of ransomware attacks can be costly, with the average ransomware attack costing a business $133,000.[5] For attorneys, a ransomware attack means time away from representing clients and generating income while still having to pay overhead, hiring information technology experts for recovery of client data if appropriate back-up measures were not taken, the cost of the ransom itself, the costs associated with informing clients of the breach under applicable state law and reputational damage that could be long-lasting.

These risks are why it is essential for attorneys in both the public and private sectors to take steps to protect client information and their practice while working remotely. While the Nevada Rules of Professional Conduct do not demand perfection, they do require "reasonable efforts" by an attorney to prevent access to or disclosure of client information from falling into the wrong hands. Comment 18 to Model Rule 1.6 informs us that the "reasonable efforts" analysis is based on five factors, which include:

- The sensitivity of the information;
- The likelihood of disclosure if additional safeguards are not employed;
- The cost of employing additional safeguards;
- The difficulty of implementing the safeguards; and
- The extent to which the safeguards adversely affect a lawyer's ability to represent clients, for example, by excessively complex software that makes adequate representation of the client difficult.

Special situations may further inform this analysis where the case involves sensitive information such as healthcare, banking, proprietary information or trade secrets. Similarly, if the client and attorney enter into an agreement whereby the attorney agrees to take special precautions to safeguard information, a failure to do so may result in a breach of the attorney's ethical obligations.

The common acceptance of BYOD (Bring-Your-Own-Device) and COPE (Corporate-Owned, Personally Enabled) devices in the legal profession heightens opportunities for inadvertent or unauthorized disclosure, making it important for attorneys to:

- Assess the risk,
- Be aware of how client data is accessed and stored, and
- Understand and use reasonable electronic security measures to protect client information.

With more than 3.1 million smartphones stolen in the U.S. in one year, cellphones should be protected with a PIN longer than four digits to guard against brute-force attacks.[6] A brute-force attack involves using hacking software that can run through up to 2 million password combinations per second, meaning that a thief can gain access to your firm's mail app on your smartphone in a matter of minutes.[7] As attorneys work from home, they should also enable automatic screen lock after a brief period of inactivity and disable notifications from mail or practice manager apps that may appear on the phone's lock-screen to prevent family members or other residents in the home from viewing client information.

The brute-force attacks mentioned above also occur to remote access desktop accounts, particularly when those accounts are unprotected by a virtual private network or multifactor identification. In January 2020, brute-force attacks on remote desktop accounts in the U.S. hovered around 200,000 per day. In March 2020, that number jumped to more than 1 million attacks per day on remote desktop accounts as businesses quickly implemented work-from-home access for employees.[8] There are some essential security steps attorneys can take to ensure that their remote connections are protected: employ complex passwords with a combination of upper and lowercase letters, numbers and symbols that are frequently changed; always use a VPN to connect; employ multi-factor identification for logging in; and limit remote access to essential personnel.

Similarly, attorneys should have robust BYOD policies in place for their firms or agencies to protect client information and remain in compliance with ethical

CONTINUED ON PAGE 16

CONTINUED FROM PAGE 15

Protecting Client Information During Remote Lawyering

requirements. Rules 5.1 and 5.3 of the NRCP impose supervisory obligations on attorneys for the actions of other lawyers and staff to ensure that the conduct of those persons comply with an attorney's obligation to keep client information confidential. This obligation remains the same whether working in the office or having staff work remotely from home on personal laptops, which could be shared by other family members.

Finally, if a breach does occur, an attorney should assess reporting obligations under the Nevada Privacy Data Act (NRS 603A.010 *et seq.*), which applies broadly to governmental or business entities that handle, collect, or "otherwise deal with" personal information such a person's first and last name and their date of birth, social security number, medical ID, bank account or email account. A hack and data breach may impose disclosure obligations under the act.

Whenever information is stored or accessed online, security is not absolute. The ethical rules do not demand perfection, but they do not excuse ignorance. Instead, attorneys should undertake continued reassessment to ensure their legal obligations keep pace with the ever-changing technological landscape.

1. ABA 2020 Practice Management Report, Nov. 23, 2020.
2. Clio 2020 Legal Trends Report.
3. Schreider, Tari, "Ransomware Attacks in the Legal Profession," (May 26, 2020).
4. *Id.*
5. Dyble, Jonathan, "Average Cost of Ransomware Attack," (Jan. 31, 2020).
6. Consumer Reports, "Smart phone thefts rose to 3.1 million in 2013," (May 28, 2014).
7. Kaspersky, "Brute Force Attack: Definition and Examples" (accessed 12/7/2020).
8. Seals, Tara, "Millions of Brute Force Attacks Hit Remote Desktop Accounts," (April 29, 2020).

SARAH M. MOLLECK is an associate at Lemons Grundy & Eisenberg, where she practices civil litigation defense and appeals. She is a member of the Standing Committee of Ethics & Professional Responsibility. She is a graduate of University of Nevada, Reno and graduated magna cum laude from Gonzaga University School of Law in 2015. She clerked for two years for the Honorable Lynne K. Simons of the Second Judicial District Court before entering private practice.