

## The Remotest Idea: Practical and Ethical Lessons Learned During the Pandemic

By Pamela E. Barker, Melissa G. Powers, and Ben Lund

*Pamela E. Barker is a member at Lewis Rice LLC in St. Louis, Missouri. Melissa G. Powers is an associate at Lewis Rice LLC in St. Louis, Missouri. Ben Lund is a partner at Brann & Isaacson in Lewiston, Maine.*

It has now been more than two years since many lawyers began to work remotely as a result of the COVID-19 pandemic. For most, the nature of the public health emergency meant that the change had to be made with little advance preparation, training, or resources. This presented substantial challenges for those who had not previously considered the practical steps required to work remotely for an extended period of time. In addition, working remotely raised a number of potential ethical issues that lawyers had not previously needed to consider.

*Property & Probate* has already covered some of the practicalities of working remotely in previous articles—first, and perhaps presciently, “Common Cents for Lawyers—Go from Paper to Bytes with Payment Processing Software” (January 2020), and more recently, “Surviving the 24-7 Office” (January 2022) and “Learning to Love Remote Work” (March 2022). One should consult all of these articles for more detailed recommendations and links to resources for remote work, along with other articles available to members on the ABA’s website (search for “working remotely”). The first part of this article will build on those useful beginnings, and the second part will add to the discussion begun in “Lawyers Working Remotely—Navigating ABA Formal Opinion 495” (May 2021).

### The Paperless Office

As early as 1975, an article in *Business Week* predicted the coming of the “paperless office.” Instead, for most lawyers, the ease of document production permitted by office automation and the increase in electronic communication resulted in more production of paper files, not less. Still, approximately two decades ago, that trend began to reverse, due in part to the associated costs of paper, printers, and physical storage needs associated with all that paper, and also in part to a generational shift as “digital natives” entered the practice of law. This corresponded with an increase in the digital storage of documents and other information used by lawyers, either in their own office-based hardware or in “the cloud”—hardware provided by third parties and accessible using the Internet.

There were other good business reasons to make this transition. Stored in digital form, documents could be used as a “knowledge bank,” with the search for previous work product made simpler and faster. Digital documents also permitted simultaneous review and editing, expediting the drafting process and improving collaboration. Staff could be trained for billable knowledge-based tasks, rather than simply performing clerical tasks such as copying and filing. Risk management practices could be improved, with backups of documents and billing information stored in multiple locations for purposes of disaster recovery. Finally, remote work became a possibility for lawyers willing to invest in the necessary resources and training.

### What’s Past Is Prologue

Although some busy lawyers have always worked in more than one location, taking work home, or to

Published in Pub: Volume 36, Number 5, ©2022 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

another office, a registry of deeds, or courthouse, this remote working typically required the physical transportation of paper files and other supporting materials. Digital storage and portable devices have both lightened the physical load and enabled access to a lawyer's information resources from anywhere that has Internet access.

That said, for most, access to information is only part of the practice of law. As part of a 2021 ABA presentation, Dan Smith, of Omaha's Smith Slusky, and a long-time advocate for cloud-based legal practice, provided a succinct list of his work processes: "read emails (snail mail?); respond; save; log assignments to task list; capture attachments and facts; delegate and track delegated tasks; take and return phone calls; collaborate and brainstorm with colleagues and assistants; keep time; review documents; draft documents; send and receive paper—FedEx, etc.; do the d\*mned bills; and socialize—which is not nothing." His description is an accurate summary of the work of most transactional attorneys, which previously took place in a traditional office setting. One year into the pandemic, his observation about working remotely was that "we now know it can be done. But we also know it is less than ideal. How can we make it better?"

Dan shared a short list of his rules for office technology, which can be adapted to plan for what a law practice needs for remote work:

- Have the tools around me that work the way I need them to work.
- Get input from the people from whom I need input.
- Delegate tasks.
- Communicate quickly, informally, and formally.
- Have instant access to information I need to complete my task.
- Get document input/review from colleagues.
- Time entry—minimum hassle, always ready.
- I am alert to nontechnology (journal?) and technology improvements I can make.
- I am not a slave to new technology—time waster.
- I am not slavishly technology averse—"technology road-kill."
- I am always looking for friction points.

### **Imagine the Perfect Productivity World and Aim in That General Direction**

For remote work to be productive, the key is to use tools that will reproduce the lawyer's preferred work environment as completely as possible. This requires a combination of hardware, software, and communications technology. Each user may have specific needs, but the basic hardware should include a portable computer, docking station, full-sized monitor or monitors, webcam, and keyboard. Together with a secure VPN (virtual private network) connection to the office, or a cloud-based or remote "workspace" solution, these will allow lawyers and staff to work in a hardware and software environment that is essentially identical to that available at the office. A high-speed Internet connection at home is also vital, along with enough bandwidth at the office or cloud solution to handle anticipated peak usage.

Communication technology is crucial. In addition to portable computers, law practices should provide all remote users with mobile smartphones, tablets, or data allowances for those who prefer to use their own device. Another approach is to use existing "VOIP" (voice over internet protocol) office telephone systems, which are frequently cloud-based or can be adapted to function in the cloud. This allows users who will not be returning to the office for an extended period to take their phone handsets to their remote work locations; once connected to the internet, the phones function as if they were in the office, allowing client calls to be answered and transferred, voice messages to be left and retrieved, conference calling, and other usual system functions.

Published in Pub: Volume 36, Number 5, ©2022 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

In addition to phones, videoconferencing has proved to be another important tool for communications, adding visual cues to enhance verbal communication and collaboration and permitting real-time document sharing. Widely adopted platforms include Zoom Meetings, Microsoft Teams, Google Meet, GoToMeeting, Webex, and Facetime, and there are a number of other providers. Some of these platforms can be integrated with an office telephone system to provide an integrated set of communications tools.

Access to information can be accomplished with the use of a law practice management system or document management system (typically used in tandem with or integrated with a time and billing system). Like other platforms, these can be operated from office-based hardware and accessed using a VPN, or from the cloud and used with a secure Internet connection. Generally, these will be more successful if they provide a uniform user interface—menus and commands that are similar across different tools. For example, many offices use Microsoft's Exchange Server, which provides tools for e-mail, calendars, contacts, and tasks through the Outlook client. Many law practice management or document management systems can be integrated with Exchange to provide the user with a more familiar software environment. In addition to document storage and retrieval, most of the systems can also be used as a knowledge bank, with full-text searching and classification to allow users to identify examples of documents developed in other transactions that can provide a starting point for a current transaction.

Even if an office is being operated on a fully remote basis, there will inevitably be paper involved, such as that used in connection with service of process or the delivery of physical notices or other hard-copy correspondence. A scanner will be necessary at whatever location these deliveries are received, to distribute the documents to the recipients and store them in the document management system. In addition, although many law practices and clients have shifted to electronic payment systems or credit cards, some clients will continue to pay using paper checks. If so, when operating remotely, it may be preferable to use a check scanner to make deposits, rather than making regular visits to drive-through bank teller windows.

Finally, all of the tools described above will not be productive without an investment in user training. Encourage and actively solicit feedback from users about what is working and what is not. This is particularly important in a remote work setting, which lacks many of the more informal office feedback channels. Encourage everyone to pick up the phone or start a videoconference, particularly where a conversation will be more efficient than a series of messages and replies. Consider regular meetings with a standing agenda to check in on how everyone is doing, to try to identify problems and solutions, and to maintain a sense of community.

### **Some Form of Remote Work Is Here to Stay**

Based on anecdotes and reports in the news media, remote work in some form is here to stay. Recent surveys suggest that there is an increasing trend toward hybrid work, in which employees are working remotely some of the time, and almost half of surveyed employers have made remote work a permanent option. A majority of employers report that remote work has not reduced productivity or collaboration and has not negatively affected workplace culture. Given this trend and a tight labor market, from a competitive perspective, it will be important for law practices to invest in the tools and training to allow effective and secure remote work.

### **Let's Get (and Stay) Ethical**

Although remote work may be a relatively new trend, the ABA Model Rules of Professional Conduct are not. Originally published in 1983, the Model Rules govern attorney behavior, in both a paperless practice and a traditional office setting. Even when working from the comfort of their homes, lawyers must not get too comfortable with their ethical duties. In the remote work environment, four of the Model Rules

Published in Pub: Volume 36, Number 5, ©2022 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

become particularly important:

- (1) Rule 1.1: Competence;
- (2) Rule 1.6(c): Confidentiality of Information;
- (3) Rule 4.4: Respect for Rights of Third Persons; and
- (4) Rule 5.3: Responsibilities Regarding Nonlawyer Assistance.

Model Rule 1.1 sets forth a lawyer's duty of competence. It requires that lawyers keep abreast of changes in the law and their practices, including the benefits and risks associated with relevant technology. For example, when the COVID-19 pandemic hit, use of videoconferencing expanded rapidly across various platforms like Zoom Meetings, Microsoft Teams, Google Hangouts, GoToMeeting, Webex, and Skype. Many lawyers had to quickly download and familiarize themselves with these new technologies to have meetings with clients or even to attend court hearings. Maintaining competence across many applications was not only a necessity resulting from the pandemic but also part of a lawyer's ethical obligations under Model Rule 1.1.

Model Rule 1.6 sets forth a lawyer's duty of confidentiality, perhaps one of a lawyer's most critical duties. With respect to paperless offices and remote work environments, Model Rule 1.6(c) is particularly important. Under this Model Rule, lawyers have a duty to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, client information, and a lawyer's efforts to prevent the unauthorized access to such information are judged by a reasonableness test. It is worth noting that Model Rule 1.6(c) has not been adopted in all states. In states that have not adopted this rule, lawyers may consider the prevention of the inadvertent or unauthorized disclosure of, or unauthorized access to, client information more of an industry best practice.

As the use of technology continues to develop, a lawyer's ethical obligations so too develop. In April 2022, the New York Bar issued an opinion regarding maintaining the confidentiality of client identity information stored on a lawyer's smartphone. In particular, it restricts lawyers who store confidential client identity information in their contacts on their smartphone from consenting to share these contacts with a smartphone app, unless the lawyer determines that (1) no person will view the information and (2) the information will not be sold or transferred to additional third parties without the client's consent. Although this opinion is based on the New York Rules of Professional Conduct Rule 1.6(c), that rule is substantially the same as Model Rule 1.6(c), so this may serve as an illustrative example for lawyers outside of New York with similar rules of confidentiality.

Not only does Model Rule 1.6(c) work to the benefit of clients, but also it aims to benefit a lawyer's practice. For example, returning to the multitude of videoconferencing platforms, Model Rule 1.6(c) would instill a duty for lawyers to analyze the security features of the various videoconferencing platforms and features that can be used to maintain client confidentiality. For example, Zoom allows users to set a meeting password to help prevent unauthorized individuals from attending the meeting. During the COVID-19 pandemic, many people would guess Zoom meeting IDs and randomly enter a meeting and disrupt it, a practice that became known as "Zoom-bombing." Using a password helps to prevent this and creates an extra layer of security. Additionally, some videoconferencing applications allow the host to individually approve each user and have the user sit in a virtual waiting room until the host approves them to enter the meeting. Taking extra steps such as these works to benefit clients but also enhances the digital and security posture of a lawyer's practice overall, which should protect not only client

Published in Pub: Volume 36, Number 5, ©2022 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

confidentiality but also the ability for a lawyer to practice effectively and securely.

### **It's Not You, It's Us**

Another rule that plays a pivotal role in working remotely or in a paperless law office is Model Rule 4.4: Respect for Rights of Third Persons. Under this Model Rule, a lawyer who receives a document or electronically stored information and knows or reasonably should know that it was inadvertently sent has a duty to notify the sender. This Model Rule has been important since long before the pandemic. The ABA adopted this Model Rule in February 2002, after electronic transmission of information started to become the standard form of communication. However, when the pandemic hit, lawyers even more heavily relied on electronic transmission and storage of information, and Model Rule 4.4 became even more important. For purposes of this Model Rule, “document or electronically stored information” is a broadly-defined term that includes not only paper documents, email, and other forms of electronically stored information, but also embedded data (known as “metadata”).

Another Model Rule that long predates the pandemic, but that has become of heightened importance in the pandemic era of remote work and increased reliance on a paperless law office, is Model Rule 5.3: Responsibilities Regarding Nonlawyer Assistance. Pursuant to this Model Rule, lawyers have a duty to make reasonable efforts to ensure the services are provided in a manner that is compatible with the lawyer’s professional obligations when using nonlawyers to assist with a lawyer’s services. These nonlawyers include internal players: secretaries, investigators, law student interns, and paraprofessionals. They also include external players, such as document management companies and cloud-based technology providers.

The use of cloud computing has been growing in recent years. The ABA reports that cloud usage was at 54.6 percent in 2018, with solo and small firms leading the way. A 2018 survey by the ABA asked cloud users to identify their biggest concerns, and the topic titled “confidentiality/security concerns” was number one with 63 percent. Although it is possible for lawyers ethically to entrust client information to “nonlawyer” cloud-computing companies, and although lawyers can use cloud computing services in their practices without breaching their duty of competence or confidentiality, addressing confidentiality and security concerns requires effort. Pursuant to Model Rule 5.3, lawyers will need to make reasonable efforts to ensure any cloud-based services are provided in a manner that is compatible with the lawyer’s professional obligations. Further, it is becoming more common for clients to require specialized security measures, or at least mandate a baseline security level, for their information.

Model Rule 5.3 also plays a role in our videoconferencing example. It requires a lawyer to make reasonable efforts to ensure that videoconferencing services are provided in a manner that is compatible with the lawyer’s professional obligations. Many videoconferencing vendors were not prepared for the drastic increase in the number of users when COVID-19 hit, and their security features were lacking. For example, Zoom had to quickly revamp its security practices and privacy policy in response to public backlash and a risk of missing out on the drastic rise in the users of its platform. Even when expected to use a number of videoconferencing platforms, in each instance, lawyers need to choose and use secure videoconferencing technologies. Further, with the ability to work remotely from anywhere, especially in public places, lawyers generally need to be wary that they are not breaching any ethical obligations, such as confidentiality or the duty to ensure that third-party service providers are operating in a way to meet a lawyer’s ethical obligations.

### **If You Build It, They Will Come**

In the remote work environment and paperless law offices, a firm’s technology footprint tends to grow to facilitate “business as usual” without some of the usual tools, such as paper, in-person communications,

Published in Pub: Volume 36, Number 5, ©2022 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

printers, hand-offs of documents, etc. Though such modernization is often a huge asset for firms, it comes with risk. As firms build robust and interconnected technology structures and mount their operations on top of them, the risk of vulnerability increases, and the pandemic has brought its own cyber challenges and risks, too.

In response to a data breach, state breach notification statutes create obligations for businesses, including law firms. In addition, under Model Rule 1.4, lawyers have an ethical obligation to notify clients of a breach that involves or has a substantial likelihood of involving material client information. Because of the sensitive, personal, and material information collected, law firms are attractive targets for hackers. A 2018 ABA survey found that one in four law firms has experienced a data breach.

The US Department of Homeland Security encouraged companies preparing for the impact of COVID-19 to adopt heightened cybersecurity standards as well as make efforts to mitigate the risk of cyber threats from employees working remotely. In April 2020, the FBI reported that the number of complaints about cyberattacks to their Cyber Division was up to as many as 4,000 a day. That represents a 400 percent increase from pre-COVID-19. Microsoft reported in June 2020 that COVID-19-themed attacks, where cybercriminals get access to a system through the use of phishing or social engineering attacks, had jumped to 20,000 to 30,000 a day in the US alone. These types of attacks are a particular risk in the remote work environment, where deception is more easily attainable.

For law firms, it can help to be proactive rather than reactive, especially because, under Model Rule 1.15, lawyers have an obligation to appropriately safeguard property of a client or third party that is in a lawyer's possession. With cyberattacks more of a "when" than an "if," one way law firms take a proactive approach is by seeking cybersecurity insurance, knowing that in spite of their best efforts to prevent hacks and mitigate risk, hacks are an inevitable possibility. Cybersecurity insurance is intended to assist companies and other organizations with the financial aspects of data recovery and other activities in the unfortunate event of a cyberattack. But most crime and cyber policies require a computer hack or active invasion of a computer system by a criminal to trigger coverage, which can create coverage gaps. It is important for policyholders, such as lawyers and law firms, to adequately gauge their requisite cybersecurity coverage.

### **Looking Forward, but Cautiously Optimistic**

To an extent, the remote work environment, paperless law offices, the COVID-19 pandemic, and all of the related shifts in technology have created a new standard in the context of legal malpractice. There is more to know about and different duties to uphold in new contexts. Lawyers must not lose sight of their ethical obligations, but also they cannot remain stagnant in their application.

The 1957 sci-fi film *Plan 9 from Outer Space* has a line—"We are all interested in the future, for that is where you and I are going to spend the rest of our lives." The future of the legal profession is looking more and more like the remote work environments and paperless law offices we have seen spring up in recent years and take flight during the pandemic, and lawyers are going to spend their lives living and working that way. But they cannot do so successfully without keeping in mind the ethical considerations that may potentially arise out of doing so.