

Trial®

TOP STORY

THE NEW NORMAL: WORKING FROM HOME

April 2020 - Karen Barth Menzies

As law firms nationwide transition to working remotely in response to the COVID-19 pandemic, here are some resources and tips for making sure your team stays connected and has the tech support it needs.

Three years ago, I wrote an article for *Trial* about working remotely that began: “Up to 30% of people in the United States work remotely—and that number has grown by almost 80% in the last decade.”¹ Now, with the world in the midst of the COVID-19 pandemic, the percentage of remote workers has increased drastically, with most law firms now nearly 100% remote.² Having remote workers is no longer avoidable and, for the time being, in-person interaction in the workplace is the exception. We have been forced to adapt to a legal system in which in-person hearings, depositions, mediations, and meetings have not been possible. Here are some tips, potential pitfalls, and resources to help navigate this new normal.

Social Distancing Orders

As of April 8, 42 states have stay-at-home or shelter-in-place (SIP) orders to help curb the spread of COVID-19, with more than 310 million Americans told to stay home except for “essential” activities.³ Judy Perry Martinez, president of the American Bar Association, made a plea to the Cybersecurity and Infrastructure Security Agency, which is the agency providing guidance to state and local jurisdictions during the pandemic, to include legal services as essential. She explained, “The American people and U.S. business community must have access to the legal services they need—when they need them most, in this time of crisis.”⁴ But many state orders have not deemed legal services essential. And even in states that have, law firms of all sizes are converting to a remote

workforce.⁵ These orders differ from state to state and even from county to county in some instances. It is important to understand how these orders affect your firm's ability to continue to operate.

When evaluating stay-at-home or shelter-in-place orders, two attorneys recommend considering five questions:⁶

1. "Is your business specifically identified as essential and excluded from provisions of the SIP order?"
2. "Does the SIP order exclude the 16 critical infrastructure sectors as identified by the National Cybersecurity and Infrastructure Agency, and, if so, does your business qualify as one of those?"
3. "Are there exceptions in the SIP order for employees to be physically present on the business premises and do they need to follow certain COVID-19 protocols to do so?"
4. "If your business or IT employees' activities are not excluded from the SIP order, does your IT department have a contingency for not being physically present?"
5. "Is it arguable that the SIP order implies the ability to maintain work-at-home operations for nonessential businesses even if it means occasional access to the physical facility for that purpose alone?"

Cybersecurity

Cybersecurity is always a concern for law firms. We need to protect the firm's internal proprietary information, our clients' personal information, and even defendants' information that we have access to and that may be subject to protective orders. But with everyone working remotely, firms must fortify all networks accessed from home and ensure that both the firm and its employees have proper security protocols in place.

Even the FBI has alerted the general public to a rise in fraud schemes related to the coronavirus pandemic, warning everyone to watch for fake Centers for Disease Control and Prevention emails, phishing emails, and sales of counterfeit treatments or equipment.⁷ The FBI alert contains a list of ways to maintain good "cyber hygiene"⁸:

- "Do not open attachments or click links within emails from senders you don't recognize.
- Do not provide your username, password, date of birth, Social Security Number, financial data, or other personal information in response to an email or robocall.
- Always verify the web address of legitimate websites and manually type them into your browser.
- Check for misspellings or wrong domains within a link (for example, an address that should end in a '.gov' ends in '.com' instead)."

Policies and procedures. Update (or implement) information security policies and procedures that address everything from passwords needed to access firm resources to a disaster recovery plan in the event of a data breach. Many resources designed to guide small law firms are available at no cost from vendors, such as Accellis Technology Group's comprehensive "Practical Guide to Cybersecurity for the Small Firm."⁹ Your IT vendor can help with obtaining and setting up security measures and also provide advice for procedures and information recovery tools if a breach occurs.

Your policies should address the potential misuse of company resources and, especially now, apply to the use of personal devices as well. For example, policies should address issues such as misusing personal email to send or receive firm email, storing business information on personal cloud accounts, misuse of unsecured wireless or conference call connections, and not properly storing or disposing of sensitive business information—among others.¹⁰

Provide updated training materials to employees about the firm's security policies, which should include specific examples that illustrate what a potential threat may look like and how it may manifest. For example, my firm's office manager, who is implementing the recommended cybersecurity measures, has found it helpful to give real examples of what phishing may look like, sending screenshots in our emails and reminding everyone that phishing can come via email, websites, phone calls, and even people knocking on our doors since we're all home during the day now.

Finally, create or review your existing data security breach response plan—also called an incident response plan.¹¹ Employees should know who to contact if they fear they may have been hacked.¹²

Enhanced cybersecurity practices. To the extent that you have not already, implement specific practices and the use of technology to enhance security, particularly as it relates to accessing firm resources. Cybersecurity attorney Alexander Urbelis (a former hacker) has warned of “massive” remote work risks.¹³ He suggests that one way to guard against hacking is to implement the use of “MFA [multifactor authentication] or 2FA [two-factor authentication], in particular . . . using something other than just a password to access company resources is critical these days.”¹⁴ Firms should institute these added authentication measures for use with firm resources, such as company servers, shared networks, software programs, and emails and calendars—especially when employees use personal devices to access these resources.

People often are hacked through unsecured Wi-Fi networks, and now that virtually all employees are working from home, firms should make sure that employees' home Wi-Fi networks are secure.¹⁵ Employees' home Wi-Fi should include network security technology (Wireless Protected Access or WPA2).¹⁶ And firm policy should prohibit employees from using unsecured Wi-Fi sources when accessing company resources.

Similarly, firms should offer employees security-related software, such as anti-malware software, and other technology to protect their personal devices, including personal laptops, phones, and tablets.¹⁷

We also need to watch out for home devices that could compromise security, including smart speakers such as Alexa, Google Assistant, and Siri. Privacy and security experts are advising law firms to require attorneys and staff not to discuss sensitive information when these devices are within earshot.¹⁸

Essential Tech and Communication

Communication and the right technology—the keys to successful remote working discussed in my article three years ago—are even more important today. One major way that law firms are improving remote communication is with the use of videoconferencing. By now most people have heard of Zoom, which has seen its popularity soar over the last two months.¹⁹ Other videoconferencing systems include Skype for Business/Microsoft Teams, Google Hangouts Meet through G Suite, Cisco WebEx meetings, and GoToMeeting. Some of these programs offer free versions, but with time limits and restrictions on the number of users.²⁰

Maintaining communication with clients is, of course, also a must. Remote employees can seamlessly continue talking to clients using Voice over Internet Protocol (VoIP) services, which allow subscribers to connect their office phone lines to the internet. Once set up, calls can be made from the office lines as opposed to using personal cell phones. RingCentral is a VoIP service and app that provides both regular and video calls, while avoiding the use of personal cell phone numbers for calls with opposing counsel or clients.²¹ When using VoIP services, remote employees can route calls to other employees the same way they would if they were in the office.

Remote Management and Project Organization

Setting up remote firms and managing employees remotely have proven to be significant challenges. While attorneys already may be accustomed to working outside of the office and are set up with time and expense software for billing purposes, staff typically are in the office during work hours with the office manager or a supervisor present to oversee equipment and file access, production, and breaks.

“The most difficult issue was providing and ensuring that every employee had the necessary equipment and internet access to connect with our system. Depending on the employee’s position and responsibilities, it was necessary to establish different levels of access and communication,” Mike Arias, senior partner at Arias Sanguinetti Wang & Torrijos, said about setting up his staff for remote work. Arias also revised office procedures, including setting up a timekeeping system that requires staff to identify the tasks performed throughout the day and the time spent to complete them. He said, “It is important that the timekeeping is perceived and understood not to be ‘Big Brother,’ but simply more of the substitute office manager.”

Many tools are available for remotely organizing and managing team projects. For example, OmniFocus is a task management app for people who use Apple products. The app’s goal is to enable the user to immediately put thoughts and ideas into to-do lists—you can even use Siri to do this.

Evernote is a note-taking app that allows for easy searching and filing, creating a virtual “library” that can be accessed easily through a web browser or mobile device. If you install Evernote on your computer, you can access all of your notes and notebooks if you do not have internet access, and any edits you make will be synced once you go back online.²² Evernote also allows for image capture and clipping sections of webpages, image capture from cameras, and voice recording. Images containing text can be converted into editable and searchable text using optional character recognition—also known as OCR—and even annotated.

Trello, Slack, Confluence, and Jira are examples of popular project management tools. These are web-based applications (all of which also have mobile apps) that allow users to stay organized on many different levels—tasks, resources, deadlines, goals—and provide a team platform for easy coordination, functioning as a communal to-do list.

Other programs, such as Sneek, can connect employees over video continuously throughout the day, but this has raised concerns about employee monitoring and privacy.²³ But after looking at it closer, Sneek may help create a cohesive, more office-like environment when all employees are entirely remote.²⁴

Imagine a group project being done in your office’s conference room, such as document review, when reviewers are working individually but also collaboratively. When everyone is in the same room, the ease of communication periodically throughout the day fosters brainstorming and the collective mind. No need to stop to send an email, make a phone call, or set up a conference call to discuss what reviewers are finding. Sneek provides this remotely, including the communication: It allows you to see your coworkers all day and start an instant video chat with a single click, either to the group or to an individual.²⁵

We should consider novel approaches to deal with what we miss when we are not able to be in the same room. We need to be flexible, creative, open to new ideas, and patient as we adapt to this new reality.

Stay Connected and Share Resources

Professional organizations, consultants, and vendors who serve the legal industry have responded quickly with information to help lawyers and law firms cope, much of which is offered at no cost. Your inbox has been filled with emails offering COVID-19 guides, webinars, podcasts, and articles with advice and guidance in a broad range of areas, including legal practice, cybersecurity, finance, employee management, and personal and family care.

Everyone is sharing suggestions and resources through emails, group texts, list servers, social media, and phone calls, which also helps people stay connected. In fact, what would seem obvious—old-fashioned picking up the phone—is often the first or second piece of advice for better communication in today’s remote environment. People are feeling disconnected and isolated, while at the same time work life has been intertwined with home life. We must create remote office environments that embrace these changes and look at work in a new way. Cameos of kids and pets on work-related videoconferences are now invited rather than viewed as embarrassing interruptions.²⁶

The Unknown Future

Perhaps the hardest part of the COVID-19 pandemic is all the unknowns, particularly *when* it will end. For our work lives, how long before we can go back to court and before we can conduct depositions and mediations in person again? Will legal services be deemed “essential” on a national basis at some point?

We do not yet know how the justice system will be affected. What we do know is that we all have been forced down this path and have no choice but to adapt to some level of remote working, at least for now. Despite the adversarial nature inherent in our business, we are in this together.

Karen Barth Menzies is a partner at Gibbs Law Group in Oakland, Calif., and can be reached at kbm@classlawgroup.com. The views expressed in this article are the author’s and do not constitute an endorsement of any product or service by *Trial* or AAJ.

Additional Resources

- AAJ: [justice.org/covid](https://www.justice.org/covid)
- Thomson Reuters: <https://www.thomsonreuters.com/en/resources/covid-19.html>
- Public Justice: <https://www.publicjustice.net/justice-delayed-justice-denied/>
- Xantrion, *A Manager’s Guide for Full Remote Working*, <https://tinyurl.com/tfowb78>.
- Sandeep Kashyap, *A Manager’s Guide to Manage Remote Team*, ProofHub (Mar. 13, 2020), <https://www.proofhub.com/articles/managing-remote-teams>.

Notes

1. Karen Barth Menzies, *Bringing the Remote Office Closer*, *Trial* 28 (March 2017).
2. Red Bee Group, a consulting firm that advises businesses including law firms, conducted an online survey of lawyers and legal staff between March 23–24, and found that 96% of those who responded reported that their workplaces had announced a move to remote work by March 24. The Red Bee Group LLC, *A National Survey on the New Normal of Working Remotely: Best Practices for Legal Employers During the COVID-19 Pandemic* (March 2020), <https://www.theredbeegroup.com/wp-content/uploads/2020/03/The-Red-Bee-Group-New-Normal-SURVEY-and-REPORT.pdf>.
3. Jorge L. Ortiz & Grace Hauck, *Coronavirus in the US: How All 50 States Are Responding—And Why Eight Still Refuse to Issue Stay-At-Home Orders*, *USA Today* (Apr. 8, 2020),

<https://www.usatoday.com/story/news/nation/2020/03/30/coronavirus-stay-home-shelter-in-place-orders-by-state/5092413002/>.

4. Letter From Judy Perry Martinez, ABA President, to Christopher C. Krebs, Director, Cybersecurity & Infrastructure Sec. Agency, U.S. Dep't of Homeland Sec., *Access to Critical Legal Services During Coronavirus (COVID-19) Pandemic* (Mar. 24, 2020), https://www.abajournal.com/files/aba-covid-cisa_.pdf.
5. For a running list of state orders and court status updates, visit AAJ's resource page at <https://tinyurl.com/CourtCovid19>.
6. Erin Illman & Steve Snyder, *Shelter-In-Place Orders Raise 5 Business Operations Issues*, Law360 (Mar. 31, 2020), <https://www.law360.com/california/articles/1258776/shelter-in-place-orders-raise-5-business-operations-issues>.
7. Fed. Bureau of Investigations, Alert No. I-032020-PSA (Mar. 20, 2020), <https://www.ic3.gov/media/2020/200320.aspx>.
8. *Id.*
9. Accellis Tech. Grp., *Practical Guide to Cybersecurity for the Small Firm*, <https://accellis.com/wp-content/uploads/Practical-Guide-to-Cybersecurity-for-the-Small-Law-Firm.pdf>.
10. Angela P. Doughty & Erica B.E. Rogers, *Working Remotely and Cyber Security During the COVID-19 Outbreak*, Nat'l Law Rev. (Mar. 26, 2020), <https://www.natlawreview.com/article/working-remotely-and-cyber-security-during-covid-19-outbreak>.
11. Accellis Tech. Grp., *supra* note 9 at 5.
12. Doughty & Rogers, *supra* note 10.
13. Mohamad Elbardicy & Emma Bowman, *Cybersecurity Lawyer Who Flagged The WHO Hack Warns of 'Massive' Remote Work Risks*, NPR (Mar. 30, 2020), <https://www.npr.org/sections/coronavirus-live-updates/2020/03/30/822687397/cybersecurity-lawyer-who-flagged-the-who-hack-warns-of-massive-remote-work-risks>.
14. *Id.*
15. Natalie Rodriguez, *3 Telework Tips for Solos and Small Firms Amid COVID-19*, Law360 (Mar. 27, 2020), <https://www.law360.com/california/articles/1257969/3-telework-tips-for-solos-and-small-firms-amid-covid-19>.
16. "WPA2 is a type of encryption used to secure networks by, basically, scrambling the data to make it harder for hackers to perceive the data." Doughty & Rogers, *supra* note 10.
17. For more about the different types of cyberattacks and malicious software, see Forcepoint, *What Is Malware?*, <https://www.forcepoint.com/cyber-edu/malware>.
18. Michael Cogley, *Lawyers Urged to Switch Off Alexa When Working From Home*, The Telegraph (Mar. 30, 2020), <https://www.telegraph.co.uk/technology/2020/03/30/lawyers-urged-switch-alexa-working-home/>.
19. Rupert Neate, *Zoom Booms As Demand for Video-Conferencing Tech Grows*, The Guardian (Mar. 31, 2020), <https://www.theguardian.com/technology/2020/mar/31/zoom-booms-as-demand-for-video-conferencing-tech-grows-in-coronavirus-outbreak>; see also Danny Hakim & Natasha Singer, *New York Attorney General Looks Into Zoom's Privacy Practices*, N.Y. Times (Mar. 30, 2020), <https://www.nytimes.com/2020/03/30/technology/new-york-attorney-general-zoom-privacy.html>.
20. David Conrad et al., *Client Advocacy Tips for Remote Hearings During COVID-19*, Law360 (Mar. 30, 2020), <https://www.law360.com/productliability/articles/1258235/client-advocacy-tips-for-remote-hearings-during-covid-19>.
21. Other VoIP services include Intermedia Unite, 8x8 X Series, Vonage, AT&T Business, Freshcaller, Grasshopper, Ooma Office, Dialpad, and Line2. For a comparison of these services, see Wayne Rash, *The*

Best Business VoIP Providers for 2020, PC Magazine (Apr. 8, 2020), <https://www.pcmag.com/picks/the-best-business-voip-providers>.

22. Evernote, *How to Access Notes Offline*, <https://help.evernote.com/hc/en-us/articles/209005917-How-to-access-notes-offline>.
23. Aaron Holmes, *Employees at Home Are Being Photographed Every 5 Minutes by an Always-on Video Service to Ensure They're Actually Working—and the Service Is Seeing a Rapid Expansion Since the Coronavirus Outbreak*, Business Insider (Mar. 23, 2020), <https://www.businessinsider.com/work-from-home-sneek-webcam-picture-5-minutes-monitor-video-2020-3>.
24. Sneek, <https://sneek.io/>.
25. *Id.*
26. William Oxley & Meghan Rohling Kelly, *3 Steps to Building Effective Teams While on Lockdown*, Law360 (Mar. 31, 2020), <https://www.law360.com/productliability/articles/1258102/3-steps-to-building-effective-teams-while-on-lockdown>.

777 6TH STREET, NW, SUITE 200 WASHINGTON, DC 20001

800.424.2725 | 202.965.3500

© 2019. American Association for Justice, All Rights Reserved

[Privacy Policy](#)