As I have not yet had the chance to communicate with you in 2020, let me take this opportunity to wish all of you a happy, healthy, and prosperous new year. I find it somewhat interesting that the year bears the numerals “2020.” As most of you know, we most frequently encounter that collection of numerals as a reference to vision. The gold standard for vision for many years, 20/20 remains a measuring standard for the quality of vision. We all want to have 20/20 vision, and for those of us who do not (or never did) have it naturally, we want our doctors to correct our vision to 20/20 with contacts, glasses, or surgery. The reference to 20/20 appears elsewhere in our consciousness as we have all heard the saying that “hindsight is 20/20.” I have a new take on that for this year. When it comes to technology, we need 20/20 foresight.

More and more jurisdictions have taken the same position as the ABA that technological competence has become an essential part of practice competence for attorneys. While I understand that such rules may create angst among many practitioners who do not yet feel comfortable with technology, I think that it represents not only a trend but a proper direction for the evolution of the profession.

Throughout the time I have practiced law, I have seen technology evolve and grow to increasing importance in the day-to-day life and work of the average attorney. As important as it has become to the office-bound attorney, it always was and remains even more important to attorneys who practice out of the office as well as in it. Interestingly, in the wake of the expansion of technology, practicing out of the office has grown more and more common, to the point that most attorneys practice both in and out of the office and, to that extent, have joined the ranks of attorneys who rightly think of themselves as road warriors.

Accordingly, in honor of 2020 and the tradition of New Year’s resolutions, I have created a list of New Year’s resolutions respecting technology, designed to help with handling technology in and out of the office. Recognize that if you practice as a road warrior, having technology operating correctly, reliably, and securely in your office serves as a prerequisite to technology working well for you outside the office. Many jurisdictions have allowed credit for technology classes directly related to the practice of law. Some have credited general technology classes. Perhaps more will come due to the changing requirements respecting technology, but the simple truth of the matter lies in a different location. Lawyers must learn to use technology effectively and efficiently if they plan on practicing competently going forward. Whether or not they get CLE credit for learning about technology should not serve as the standard. While I personally...
think that they should, I think it is more important that lawyers learn technology than that they get CLE credit for doing so.

With this in mind and my best wishes to each of you for a wonderful 2020, my list of resolutions follows. I hope you find them suitable for you to adopt. I present them to you in no special order, other than I have listed first the resolutions that relate to things that I expect (hope) that most of you have heard before, learned, and already have in practice. I consider all of them important, but I anticipate that for most of you, compliance with numbers 8, 9, 10, and 11 will prove the newest and, perhaps, most difficult. Accordingly, I offer you my 11 resolutions (along with a few explanatory notes and comments).

1. I will always use secure passwords for accessing my office, my data, and each of my accounts. I will make sure that everyone in the office does the same. Note that when it comes to passwords, longer is stronger. Passwords should have no less than eight characters; more gives you greater security. Passwords should have a combination of alphabetical characters (upper and lower case), numeric characters, and symbolic characters (such as @#$%).

2. I will use biometric security wherever possible in my practice. While some accounts can make use of biometric access, the ability to engage such techniques depends on having appropriate hardware. Accordingly, you should look for hardware that accommodates biometric security. The most common biometric devices include fingerprints, facial recognition, and retina scans.

3. I will regularly back up my data to a local hardware device and to the cloud in properly secured accounts. In today’s world, paper files have diminished in importance. More and more attorneys have started maintaining their files in electronic formats. This has the advantage of allowing easier location of specific documents and the ability to easily back up the entire collection of data and documents. Data safety requires that you have multiple backups, that some should be off-premises, and that you have at least one copy in the cloud.

4. I will regularly check for updates to the operating systems and application software on all my devices and install updates when available. I will make sure that everyone in my firm does the same. Publishers of operating systems and software often update their work to address bugs in performance and weaknesses in programming that allow hackers to break into their coding. A hacker breaking into an operating system or program software can take control of a computer or add malware to the computer or both. Getting the most recent updates can help make your system resistant to hacking.

5. I will carry my own cellular hot spot and stay off public WiFi as much as possible. Public WiFi includes the WiFi in your hotel, Starbucks, and other similar locations as well as WiFi in the airport and, in some cities, in public areas. The fact that someone owns it does not make it private. The fact that numbers of unrelated people can access it makes it public. Public WiFi offers the attraction of costing you little or nothing. Conversely, it creates the danger that while you use it the bad guys can get access to your devices and steal data or add malware. Better to carry your own secure, password-protected hot spot and use it instead.

6. I will not use public WiFi without also employing a virtual private network (VPN). A virtual private network can protect you while you use public WiFi. While I don’t encourage you to use public WiFi, at some point you will likely do so out of convenience. You can reduce your risk dramatically by employing a VPN to insulate your communications from third-party access. Think of it as an escort/bodyguard for your communications. In fact, it can’t hurt to use a VPN even in connection with your own network as it affords extra protection.

7. I will obtain anti-malware software and regularly scan all my devices (including external drives) for malware. You can find good anti-malware software for the major operating systems and for most devices, although the software for computers generally works better than for smartphones and tablets. You should invest in a reliable program for your operating systems and regularly use it to run a full check on your systems.
You can also set up many of the programs to scan information as it comes into your device. Get the program, use the program, and take corrective action should it ever report that you have malware on your systems. A little hassle can save a lot of angst.

8. **I will take classes to help me learn about technology in general and my software and hardware in particular.** As more jurisdictions follow the trending pattern to expect attorneys to have a working knowledge of technology, more and more providers have started offering classes in technology for attorneys. While I certainly would not suggest that you forgo substantive law classes in your areas of practice to take a technology class, I would also not suggest that you forgo technology classes to take a class in another area. Simply put, you need to pay as much attention to learning technology as you do to learning substantive law. Do not limit yourself to CLE classes that have accreditation from your local jurisdiction. Classes that do not provide CLE credit may still be useful in terms of advancing your knowledge. While we all need to meet the CLE requirements of our licensing jurisdiction(s), the acquisition of knowledge provides its own rewards.

9. **I will look for and take the time to read articles about technology in general and in particular technology to support my legal practice.** You did not learn all that you know about the law in a classroom. You learned from a variety of sources, including the classroom, reading cases and statutes, reading articles by experienced practitioners, and talking to experienced attorneys. Learning the technology you need to practice law effectively and efficiently in today’s world will require a similar approach. Take classes, talk to experts, and read as much and as widely as you can.

10. **I will learn about e-discovery and how to conduct it.** Whether you like it or not, if you engage in litigation or related discovery, you need to understand e-discovery. You need to know it when you see it, know when you need it, and know how to do it. As more and more businesses and individuals evolve from paper accounts and records to electronic records and online storage, e-discovery will evolve into an inescapable essential of discovery practice. One could make the argument that we have already reached that point; however, it remains clear that the significance of e-discovery in modern litigation continues to grow. If you do not understand it, you will not likely use it effectively. If you fail to use it or deal with it appropriately, given the increasing requirements of technological competence among attorneys, it is more likely that you will commit malpractice for failing to properly employ e-discovery. Don’t take that risk.

11. **I will not engage with technology that I do not understand in the course of my practice without the advice and counsel of a professional knowledgeable in that technology.** Simple common sense should get you to this point. If you do not have expertise in tax law, you should not take a tax case, at least not without associating someone with the required expertise. Similarly, for other areas of substantive law. Now we take the rule one step further, into technology. If you lack familiarity with a particular technology that you want or need to employ in a case, you need to learn it quickly and, until you do, you need to associate someone with the required expertise to advise and guide the use of the technology.

Consider yourself strongly encouraged to adopt and comply with my 11 resolutions. If you do, you increase the likelihood that you will look at your technology with 20/20 vision and anticipate and guard against most problems with 20/20 foresight.