Virginia State Bar Special Committee

THE FUTURE OF LAW PRACTICE

2022

INTRODUCTION

The Virginia State Bar Special Committee on Technology and the Future Practice of Law was formed in 2019 from the combination of the Study Committee on the Future of Law Practice and the Special Committee on Technology and the Practice of Law. Our combined Special Committee continues the work of both prior Committees, including the work of the Study Committee, originally tasked in 2014 to evaluate current developments in the legal landscape and assess how these changes will impact the practice of law.

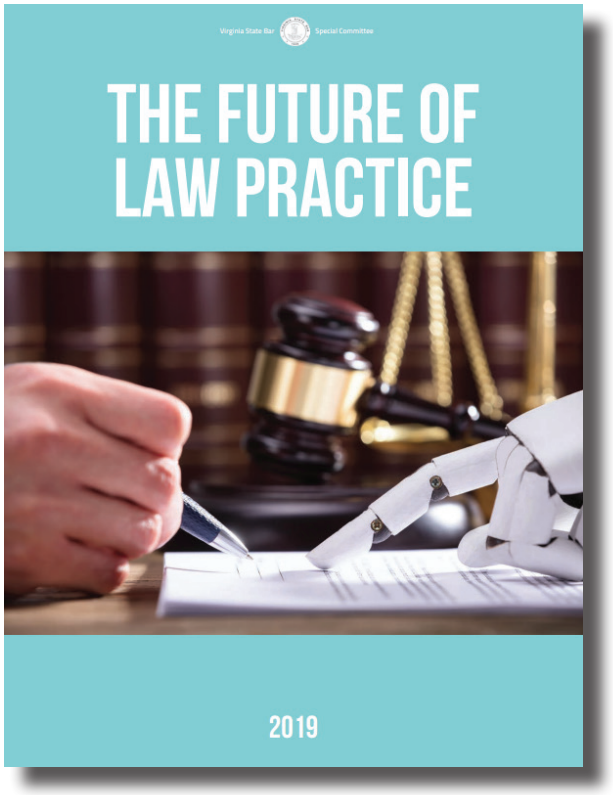
Committee members are from across the Commonwealth and represent the public and private sector, small and large law entities, and attorneys with general to specialized knowledge of technology and cybersecurity. Members stay current with the topics covered in this report, and the Committee's diversity ensures that the interests of each member reflects the broadest spectrum of the VSB membership as a whole.

Our 2019 report highlighted the following external forces affecting the practice of law:

- Advances in technology that have changed the way lawyers practice, giving clients the expectation that lawyers will provide services more efficiently and cheaply, and giving consumers the belief that they can obtain legal information and handle many legal matters on their own.
- Increasing competition from nonlawyer service providers that offer legal information and legal documents to consumers.

- Generational pressures that are likely to impact law firm business models — estimates are that 60% of law firm partners are baby boomers, while millennials have been the largest generation in the U.S. labor force since 2016.
- Clients' dissatisfaction with billable hour arrangements encouraging lawyers to offer fixed fees and other alternative billing arrangements.
- Increased insourcing of legal services by corporate clients, along with increased unbundling of tasks so that lawyers are only asked to complete the specific tasks that require legal judgment.
- Accelerated globalization of legal services via both traditional models and technology, leading to an increase in multi-jurisdictional law practice and a decreasing relevance of geographical boundaries.
- The advancement and incorporation of artificial intelligence and machine learning into the practice of law.
- Blockchain technology and its application to legal contracts and cryptocurrencies.

The 2019 report also addressed the access-to-justice and wellness challenges facing the legal profession. In recognition of the significance of those issues, each is now the subject of a dedicated VSB committee. Although the Committee believes access to justice and wellness merit continued study, those subjects are not included in this report given their separate representation in the VSB.



The Committee recognizes that the organized bar does not exist to regulate the market, and it thus does not engage in any form of protectionism. The mission of the VSB is to regulate the legal profession of Virginia, to advance the availability and quality of legal services provided to those living in Virginia, and to assist in improving the legal profession and judicial system.

The 2022 report is the third report issued, following the initial report in 2016 and the second in 2019. Now more than ever, the Committee recognizes the uncertainty that lawyers face in an ever-changing digital world. Its mission is to educate the bar by identifying and providing information on important developments in technology affecting the practice of law, so that practitioners may adapt and thrive by continuing to provide high quality legal services to their clients.

THE EVOLVED BUSINESS OF LAW

The COVID-19 pandemic rapidly transformed the famously (perhaps notoriously) anachronistic and rigid legal profession. Prior to the pandemic, law firms frowned upon — or even forbade — remote work, and nearly all hearings in Virginia courts were argued in person. Law firms expected their associates and junior partners to grind away long hours in the office. The law firm model that has lasted for centuries was designed almost exclusively for in-person client service.

Despite the Virginia State Bar authorizing virtual offices using cloud computing through LEO 1872 in 2013, remote work, teleconferencing, and videoconferencing were very much the exceptions to the in-person law firm rules. Even into early 2020, law practice was broadly conducted in the office and in court. According to Frank Barron, a retired partner at the New York firm of Cravath, Swaine & Moore LLP, the best way to teach students to be lawyers is by "watching and observing," which is best done in person.

Just as law firms encouraged physical presence in the office, most Virginia judges also required in-person appearances. Lawyers ordinarily made expensive physical appearances even for perfunctory and agreed motions that involved little more than handing an order to the judge for entry. Failure to appear for such a court hearing could land a lawyer in hot water.

The sudden and dramatic changes brought about by the COVID-19 pandemic forced law firms, courts, and the broader legal industry to rapidly accelerate their previously glacial embrace of technology practically overnight to meet client demands and pandemic strictures, ultimately transforming the business of law. These demands have continued throughout the pandemic. Even as case counts, hospitalizations, and deaths increased, clients rightfully expected their matters to be serviced. The essential work of the judicial system had to go on.

In response to those demands, law firms adjusted their workflow capabilities. To maintain profitability through the pandemic, law firm partners and administrators embraced technology and even remote work. While physical offices closed, firm lawyers worked from home or other remote locations. Cloud computing, videoconferencing, and remote desktops became critically important tools to facilitate legal work. Essentially overnight, the law firm model transitioned from the staid into the flexible by embracing technology.

Several technological applications have streamlined the transition from in-person employment to remote working. New (and even legacy) technologies have offered a way to perform work outside the office, grow business, and meet client demands. Successful integration of these technologies is now essential to a complete and successful law practice irrespective of firm size.

Many technological changes brought about by the COVID-19 pandemic will remain permanent in some form or another. This section discusses the tools that law firms can use to optimize and grow their practice and maintain financial success throughout the uncertainties of the pandemic and beyond.

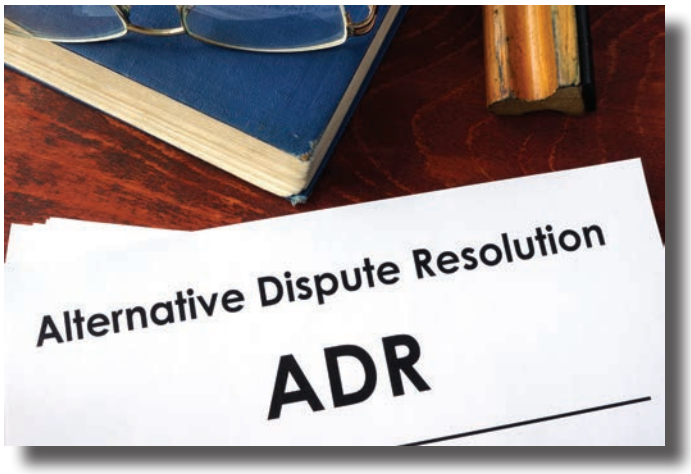
2.1 CLIENT EXPECTATIONS

Clients expect their matters to be serviced irrespective of their lawyer's location, and technology has allowed practitioners to meet those expectations almost seamlessly. Some of those technologies include videoconferencing, electronic signatures, and remote desktops.

Although the Virginia Rules of Professional Conduct do not contain a requirement for lawyers to meet clients in person, many practitioners conducted their initial intake meetings in-person. Many, if not most, clients now expect law firms to have virtual capability. In fact, theoretically, the entirety of a client representation can be conducted remotely. Videoconferencing software allows for "face-to-face" meetings, documents can be exchanged and marked up through cloud services, and signature-verification services allow for binding electronic signatures for transactional documents.

Clients expect, and may look elsewhere if practitioners do not offer, these remote work capabilities. Meeting remotely and signing documents electronically is usually far more convenient for clients than in-person alternatives. Remote practice saves clients travel time and enables them to conduct their business according to their schedule. Even if law practices return to a largely in-person setting, clients will continue to demand remote capabilities. More and more, practitioners will need to meet clients "where they are."

2.2 COURTS AND ALTERNATIVE DISPUTE RESOLUTION



The judiciary's move to remote hearings has had a significant impact on the practice of law, especially for Virginia lawyers. Before the pandemic, Virginia judges generally required lawyers to appear in-person at most hearings. Virginia lawyers would carve out several hours — with only some of them being billable — to appear for routine court hearings.

The pandemic's onset forced the judiciary to stay or continue nearly every pending matter, some for months. While some cases settled, many did not. To address the backlog while maintaining safety protocols, the Supreme Court of Virginia permitted remote hearings in April 2020. Individual courts then promulgated local rules for remote hearings and the resumption of in-person proceedings, including jury trials. To reduce the risk of disease spread among jurors, witnesses, and litigants, courts established elaborate trial-safety measures that had to be approved by the Supreme Court.

Remote hearings alleviate the need for complex social distancing regimes in courts. Remote hearings are particularly valuable for quick motions because they relieve lawyers of commuting to court, parking, clearing security, and then waiting for their matter to commence. This more efficient process saves time for the lawyer and reduces expense for the client. Despite Virginia courts' willingness to set matters remotely and accommodate social distancing, the COVID-19 case backlog has resulted in trial dates now commonly being calendared years in advance — a shock for clients familiar with the usually fast-paced Virginia practice. This new time cost of litigation has made alternative dispute resolution even more desirable for clients.

Mediation — a popular form of alternative dispute resolution before the pandemic — has taken on renewed importance. Mediation helps parties settle their matters confidentially and quickly without court intervention. The process is also voluntary with the parties agreeing to be bound by the results of the mediation.

An alternative to mediation is arbitration. Arbitration can be conducted quickly and confidentially. Whereas in mediation, the mediator is neutral that facilitates an agreement between the parties, in arbitration, the arbitrator is a neutral fact finder and

decision maker. The parties may agree that the arbitrator's decision is binding. Significantly, both arbitration and mediation can be conducted virtually, with many of Virginia's most frequent neutrals now having extensive experience in conducting remote mediations.

2.3 OPPORTUNITIES

A significant benefit provided by remote work, particularly to large law firms with large offices, is reduced overhead. Although most firms may not wish to make a complete transition to a virtual office, many firms have availed themselves of these technologies. Moving to a total virtual practice may alleviate the firm of expensive overhead in terms of office space, utilities, and real estate taxes. Even if the firm allows some sort of flexible schedule, this could limit the need for office space, allowing firms to downsize. Ideally, that savings should passed onto the client in the form of fewer billed hours.

Remote work also enables employees, especially those with young children, to work at home, allowing parents to play a larger role in their families' home lives. As long as school and day closures remain common, due to COVID-19 infections, staff shortages, or otherwise, the flexibility offered by remote work is rapidly becoming a necessity rather than a convenience. As COVID-19 ultimately moves toward an endemic disease, it is likely remote practice will remain a popular alternative to in-office law practice.

2.4 CHALLENGES

Although technology has allowed law firms to maintain financial success and productivity throughout the pandemic, that success has come with some drawbacks. Remote work is not without its challenges, and practices adopting a primarily remote office face the most significant challenges. As the VSB's landmark Lawyer Well-Being Report found, occupational risks of law practice — including employee isolation, a lack of work-life balance, and connectivity dependence — are increased by a virtual law practice.

Additionally, new employee onboarding and professional development of less experienced attorneys present challenges in the virtual practice environment. Newer attorneys lose the benefit of day-to-day interactions with more experienced attorneys that are part of the in-office practice experience. Working together as a team is generally considered a critical part of a law practice. Daily interactions between lawyers and staff engender familiarity, collegiality, and trust. When the entire workforce is at home, it may be more difficult to integrate new employees which may lead to employee isolation, due to a lack of distinction between the office and home.

Infrastructure issues are also important to consider. The virtual practice is wholly dependent on internet connectivity and platform reliability. Loss of internet connectivity or an unreliable connection can render remote work impossible, or at the least, difficult. This is a substantial risk, especially for those employees who reside in areas with poor connectivity, such as rural locations.

Perhaps the biggest business challenge with remote practice is obtaining new clients. Not all practices have transitioned to remote work. Those firms that have made that switch to remote practice must carefully manage their business development strategy to optimize the best way to capture new clients.

CRYPTOCURRENCIES BECOME PART OF THE LEGAL ECONOMY

In the 2019 report, the Committee discussed the advent of cryptocurrencies, such as Bitcoin, and their possible disruptive effects on the legal profession. Cryptocurrencies remain highly speculative, but developments in the intervening years show they are unlikely to be a passing fad. They are now taxed, subject to increasing regulation at the federal and state level, and becoming a rare — but at least recognized — way to pay for legal services.

A cryptocurrency is a currency that exists only digitally, uses a decentralized system to record transactions and manage the issuance of new units, and relies on cryptography to prevent counterfeiting and fraudulent transactions. Decentralization is the key trait of a cryptocurrency. Some form of intermediary is involved in nearly every ordinary transaction. A bank or credit card company is usually involved in even the simplest purchases, while more elaborate transactions involve escrow agents and lawyers, all with their accompanying fees and delays. These transaction costs are major considerations when planning any significant transaction.

Unlike every other medium of exchange, cryptocurrencies operate free from central authorities like banks or payment processors. Without middlemen, cryptocurrency users can buy and sell directly to one another in a peer-to-peer fashion without incurring the costs inherent in any centralized market. In fact, the only transaction cost associated with cryptocurrency use is the conversion fee for exchanging cryptocurrency for U.S. dollars or another traditional currency.

3.1 RECOGNIZING CRYPTOCURRENCIES

The benefits of cryptocurrencies over other currencies mean that many people want to purchase goods and services with cryptocurrency. Regulators have noticed. The IRS classifies cryptocurrency as property, which means it is taxable just like transactions in any other property. Short-term cryptocurrency gains are taxed as ordinary income, while cryptocurrency held for over a year is subject to long-term gains tax. Beyond these principles, however, much ambiguity and uncertainty continue to surround the financial implications of holding and transacting in cryptocurrency.

In perhaps the most high-profile acknowledgement that cryptocurrencies and other digital assets have staying power, the Biden administration on March 9, 2022 issued an "Executive Order on Ensuring Responsible Development of Digital Assets." Although the order does not require any specific action or establish any regulations, it outlines the first whole-of-government approach to the risks and benefits of digital assets and their underlying blockchain technology across six key priorities: consumer and investor protection; financial stability; illicit finance; U.S. leadership in the global financial system and economic competitiveness; financial inclusion; and responsible innovation.

3.2 CRYPTOCURRENCY AS PAYMENT FOR LEGAL FEES

Lawyers are most likely to encounter cryptocurrencies when clients ask to pay for legal services with them. As the Committee noted in the 2019 report, such transactions are fraught because cryptocurrencies currently rest in the grey area between money and property — and thus implicate the legal ethics principles concerning both. At the time of that report, Nebraska was the only state that had issued a legal ethics opinion on the topic, advising "lawyers to convert digital currency into U.S. dollars immediately upon receipt" because, given the "volatility of cryptocurrency prices, prompt sale of the cryptocurrency will ensure that the lawyer does not overcharge the client."

Since then, other jurisdictions have weighed in. The New York City Bar's opinion noted that the issue turned on whether the client and attorney were entering into a "business transaction." Any fee agreement involving cryptocurrency would have to account for the many variables involved in such transactions, making many lawyers unlikely to adopt the practice. Lawyers in Washington, D.C., however, may accept cryptocurrency as payment "so long as the fee is reasonable," but that opinion elided some of the ethical complications of accepting cryptocurrency as an advance fee. North Carolina has also addressed the question, concluding that "a lawyer may receive virtual currency as a flat fee for legal services" if the amount is reasonable but may not accept it as entrusted funds to be billed against.

At the time of writing, the VSB has circulated a draft opinion on the subject and is accepting public comment through May 4, 2022. In proposed LEO 1898, Virginia concludes that a lawyer may accept client property, including cryptocurrency, offered as an advance payment for the lawyer's services, provided the lawyer's fee is reasonable, and that:

- the transaction is fair and reasonable to the client,
- the transaction and terms are fully disclosed in writing in a manner the client understands,
- the client is advised of the opportunity to consult with independent counsel, and
- the client's consent is confirmed in writing.

When cryptocurrency is being held by the lawyer as an advance fee, it is considered property and thus the rules concerning safekeeping client property apply. They require that the lawyer take reasonable steps to secure the client's property against loss, theft, damage or destruction — including the cyber threats that uniquely threaten digital assets.

Despite these developments, the Committee's conclusion from the 2019 report remains applicable: Lawyer acceptance of cryptocurrency payment is a rapidly developing topic, and Virginia attorneys who are considering the practice — or who already accept cryptocurrencies for legal services — should monitor this area closely for further developments.

ALTERNATIVE LEGAL SERVICE PROVIDERS AND BUSINESS STRUCTURES

The Committee continues to monitor activities related to law firms that have nonlawyer owners or partners, known as alternative business structures (ABS). While a few states in the U.S. have moved toward ABS authorization, states continue to be inconsistent on whether to authorize licensed paraprofessionals to provide certain legal services.

4.1. ALTERNATIVE LICENSING OPTIONS

The Washington Supreme Court voted in 2020 to sunset its Limited License Legal Technician program, which had been in place since 2012. According to a letter from Washington State Bar Association treasurer Daniel Clark, as of May 2020, there were only 45 licensed (39 active) LLLTs in the state, and the program failed to meet its goal of being cost-neutral to the state bar. LLLTs who were already licensed are permitted to continue practicing, and some candidates already in the licensure pipeline were permitted to continue to pursue licensure, but no new candidates will be accepted.

In the meantime, California is considering a proposal to allow paraprofessionals to provide legal advice and even represent parties in court in certain situations. A decision on the proposal was initially expected in early 2022, but the process has been delayed and no new date has been announced as of the time of publication of this report. The New Hampshire legislature is also considering a bill, HB 1343, to allow paralegals to provide representation in court under certain conditions, including that they are employed or retained and supervised by an attorney. The bill passed the House in March 2022 and is before the Senate Judiciary committee as of the time of this report.

4.2. ALTERNATIVE LEGAL SERVICE PROVIDERS

Much has been written on the innovative legal services delivery models that have emerged over the last decade and how they have transformed the legal services market. Many of these models have been discussed in the Committee's previous reports. Perhaps most significant is the growth of alternative legal service providers (ALSPs), entities that are not law firms but that provide law-related services to law firms or to corporate law departments. Examples of services provided by ALSPs include eDiscovery, document review, contract management platforms, and flexible legal staffing companies.

A study published by ThomsonReuters and Georgetown University in 2021 reports that ALSPs continue to gain market share in the legal services sector, and that the industry seems to have reached maturity as ALSPs are used by most corporations and law firms. The 2019 estimated market size for all ALSPs was $13–14 billion, up from $8–9 billion in 2015. The largest percentage of the market continues to be independent ALSPs, but in-house/law firm captive providers are growing at the fastest rate, albeit from a much smaller base. Those law firm captive providers grew approximately 60% from 2017 to 2019, and the report notes this is likely an underestimate because of measurement difficulties.

More than 550 law firms and corporate legal departments were surveyed regarding their use of ALSPs. Approximately 79 percent of law firms, and 71 percent of corporations surveyed, used ALSPs in 2020. Initially, firms predominantly used ALSPs for document review and discovery, but that is changing. Law firms are likely to use ALSPs for eDiscovery support services, legal research services, and litigation and investigation support, while corporate legal departments are using ALSPs most commonly for regulatory risk and compliance services, legal research services, and specialized legal services provided by licensed lawyers. The study also reported an increasing level of collaboration, rather than competition between law firms and ALSPs, with law firms in some instances initiating the choice to use ALSPs rather than doing it only at the request of a client.

Big accounting firms have been providing these services for decades, transforming themselves from audit firms to globally integrated business solution providers with legal services as a component. The ThomsonReuters study shows that the Big Four continue slow but steady growth in legal services, from $900 million in 2015 to $1.4 billion in 2019. The study also indicates that the Big Four continue their focus on growth in these areas, including international expansion, while shifting to an "issues led" consulting approach.

4.3. ALTERNATIVE BUSINESS STRUCTURES

In the 1937 case of Richmond Association of Credit Men, Inc. v. The Bar Association of the City of Richmond, 167 Va. 327, the Supreme Court of Virginia ruled that a lay corporation cannot hire lawyers to provide legal services to its customers — only a law firm can provide such services. But that is exactly what is happening in the rapidly evolving legal services market. Although the case remains good law, market forces are running roughshod over unauthorized practice of law (UPL) rules and doctrine. In response to these market forces, a few states have begun taking steps toward possibly relaxing the traditional rules on UPL and ownership of legal services providers.

In 2020, the Utah Supreme Court adopted a pilot project called the "sandbox" in which Court-approved business structures may include nonlawyer owners in firms that provide legal services. As of February 2022, 31 entities are authorized to provide services through the sandbox, including established companies like Rocket Lawyer, nonprofit efforts focused on medical debt relief, and the first U.S. law firm entirely owned by nonlawyers, Law on Call. The program was initially planned to run for two years but has recently been extended to seven.

Entities, including those owned by nonlawyers, can apply to Utah's newly created Office of Legal Services Innovation for permission to provide legal services. Applicants must explain how they propose to offer legal services through technology or a nontraditional corporate structure. Successful applicants are authorized for the duration of the program to provide legal services in their area of law (e.g., healthcare or housing) using their approved model.

In 2021, Arizona's Supreme Court followed the recommendation of its Task Force on the Delivery of Legal Services and repealed its version of Rule 5.4, adopting a regulatory framework in which a nonlawyer owner or investor may be approved by the Supreme Court as an alternative business structure. Legal Zoom, which went public in June 2021, is the ninth company to be approved by the Supreme Court of Arizona. This means that Legal Zoom can directly provide limited legal services to clients in Arizona. Another noteworthy ABS now operating in Arizona is Elevate, which identifies itself as a "non-lawyer-owned law company" with an integrated law firm, ElevateNext.

The ABA appears to have recognized that ABS entities and changing models for investment in law firms are becoming more relevant and widespread. In the September 2021 Formal Opinion 499, it addressed whether a lawyer can passively invest in an ABS even though the lawyer is licensed in a jurisdiction that forbids nonlawyer ownership. The opinion concluded that the lawyer can make a passive investment as long as the lawyer does not practice law through the ABS, hold herself out as being a lawyer associated with the ABS, or have access to confidential information of clients of the ABS except as permitted by Rule 1.6. Any conflicts arising from the investment must also be managed appropriately. Although the ABA opinion is not binding in any jurisdiction, it highlights the growing attention to ABS entities and suggests they may be here to stay.

4.4. NONLAWYER ATTORNEY-CLIENT MATCHING SERVICES

Although many types of ABS entities are gaining increasing legitimacy in the legal sector, nonlawyer-operated matching services like Avvo Legal Services have declined since the last report. Avvo's new owner, Internet Brands (the parent company of Nolo, Martindale, and other legal brands), shut down Avvo's matching service after numerous state bar ethics challenges, although other parts of Avvo, including the lawyer ratings, still exist.

Meanwhile, new companies operated by nonlawyers continue to try to find a way into the marketplace. One significant development is the Florida Supreme Court's finding a company called TIKD engaged in the unauthorized practice of law. TIKD is a nonlawyer service that offered drivers legal assistance in resolving traffic tickets. Drivers could upload a picture of their traffic ticket, and TIKD would analyze the ticket and determine whether to take the case. If accepted, the driver paid a fee based on a percentage of the ticket's face value, and the driver's information was forwarded to a Florida-licensed attorney for representation. All costs, including court costs or fines, were paid by TIKD, so that the client was guaranteed to never pay more than the fee paid to TIKD at the outset. TIKD also provided a full refund if the driver received points against their license. Attorneys representing clients via TIKD were paid a flat fee per case, set by TIKD and paid from the fee paid by the driver.

The referee who heard the case initially found that TIKD was not engaged in UPL, because TIKD was providing only administrative and financial services. All legal services were provided by Florida-licensed attorneys, and the payment of attorney's fees by TIKD was permissible under third-party payment rules. The Florida Bar objected to the referee's report, and on de novo review, the Supreme Court found that TIKD was engaged in UPL and permanently enjoined its operation in Florida.

The Florida Supreme Court's analysis focused on the risks to the public from this business model, including the fact that TIKD would not be subject to any oversight by the Court as a nonlawyer entity. The Court also reaffirmed prior case law holding that "only attorneys licensed to practice law in Florida are authorized to act like a law firm by advertising and selling the legal services of lawyers to the public unless authorized by our rules." A dissent from the Court's opinion made a strong argument that the challenges to TIKD were about preserving an existing business model, not about protecting the public or regulating the practice of law. Florida has a longstanding reputation for being strict on UPL, and this case appears to be the latest example.

ELECTRONIC FILING IN VIRGINIA

Federal courts and the Virginia Workers' Compensation Commission have utilized electronic filing systems for more than 10 years. Federal courts use the Case Management/Electronic Case Filing ("CM/ECF") system. In addition, federal courts have historically used PACER for providing the public and attorneys with electronic access to court files. Federal appellate courts have all transitioned to the newest version called NextGen CM/ECF, which combines the electronic filing system with the PACER system through a single account login. Many district and bankruptcy courts are still making this transition.

Even though NextGen is live in Virginia, the Administrative Office of the U.S. Courts conducted a Path Analysis of the current system noting its deficiencies and opportunities to improve the e-filing experience. It concluded that the foundational technology is outdated, and an entirely new system should be built.

At the state level, the Virginia Workers' Compensation Commission utilizes WebFile for the electronic filing of documents and medical records. Unlike the federal system, only parties or counsel have access to the Workers' Compensation file through WebFile. To gain access to the file, an attorney must note his or her representation of a specific party. This prevents the publication of protected health information and eliminates the need for redaction of personal identifying data, which is required in other filing systems. Only medical records that are too voluminous to file electronically are submitted in paper form to the Clerk of the Commission.

5.1 THE EVOLUTION OF E-FILING IN VIRGINIA

The General Assembly laid the groundwork for e-filing in Virginia in 2005 by Senate Bill 992, which created Code § 17.1-258.2 et seq. and 55-142.10 et seq. These provisions established Virginia's first e-filing system in circuit courts focused on electronic recording of land records. In 2010, the General Assembly updated Chapter 4.1 of Title 17.1 and added Code § 8.01-271.01, noting that "[e]lectronic filings in civil actions and proceedings in circuit court shall be governed by Article 4.1 (§ 17.1-258.2 et seq.) of Chapter 2 of Title 17.1 and applicable Rules of the Supreme Court of Virginia.

Shortly thereafter, the Supreme Court of Virginia Office of Executive Secretary released the Virginia Judicial Electronic Filing System ("VJEFS") as a pilot program. The system was proclaimed as "a comprehensive automated system developed . . . to integrate the circuit court clerks' offices existing statewide Circuit Case Management, Case Imaging, and Financial Management Systems."

Only a select few jurisdictions actually implemented VJEFS. For instance, the Dinwiddie Circuit Court noted in June 2013 that it was participating in the pilot program and was only the fourth clerk's office to implement the new system.

At the beginning of the pandemic, on March 16, 2020, the Supreme Court of Virginia issued its first order declaring a judicial emergency and suspending "non-essential, non-emergency court proceedings in all circuit and district courts." Additionally, the Court noted requiring e-filing if available as one of the protective measures each court should implement. The Supreme Court further authorized electronic or facsimile filing of documents.

Judges, lawyers, and clerks throughout the Commonwealth have all endured the catastrophic effects of shutting down offices, courthouses, jury trials, and the like. Because of these serious health concerns, people were less likely to go into a clerk's office to file a lawsuit and pay a filing fee. Indeed, during some periods of this pandemic, people were prohibited or discouraged from physically entering a clerk's office.

Nonetheless, Virginians still had claims to litigate. Mail was an alternative, but the inconsistency of the United States Postal Service during that time made many litigants reluctant to rely on mail to meet filing deadlines.

The COVID-19 pandemic created needs that will likely incentivize judges, lawyers, and clerks to continue adapting to the future of litigation.

5.2 ELECTRONIC FILING IN VIRGINIA APPELLATE COURTS

On June 2, 2020, the Supreme Court issued an order directly addressing this issue. The Court declared that it "will permit and . . . encourage counsel and pro se litigants to file electronically all pleadings and documents that would otherwise be required to be filed in hard copy." Referencing the Virginia Appellate Courts eFiling System, or VACES, the Supreme Court shifted direction significantly toward electronic filing.

Now, all appellate submissions are all done through VACES. In fact, effective June 1, 2021, the Court modified its rules and declared, "All documents — other than the record on appeal — must be filed electronically, except for pro se prisoners or a litigant who has been granted leave by the Court to file documents in paper form." Rule 5:1B(b). This rule change is reflected by numerous other changes referencing Rule 5:1B throughout Part 5 of the Rules of the Supreme Court of Virginia.

For example, Rule 5:26, titled "General Requirements for All Briefs," adds the requirement in subsection (a) that "[a]ll briefs and the appendix must be filed in compliance with the requirements of Rule 5:1B." One need only peruse the red-lined version of the amendments to see references to Rule 5:1B in glaring red throughout the amendments.

At the same time, Part 5A of the Rules of the Supreme Court of Virginia, which governs practice before the Court of Appeals of Virginia, were also modified. These modifications, found primarily in Rule 5A:1(c), reflect the same mandatory

electronic filing: "Except as otherwise provided, all documents to be filed in this Court must be filed electronically, in Portable Document Format (PDF), with the clerk of this Court and electronically served on opposing counsel." Rule 5A:1(c)(1). Just like the amendments to Part 5 of the Rules, part 5A:1(c) is reflected throughout the amendments to Part 5A.

5.3 ELECTRONIC FILING IN VIRGINIA CIRCUIT COURTS

These appellate changes are a significant push forward in the Virginia judicial system. This top-down approach signifies a clear preference at the Supreme Court to usher Virginia lawyers into the 21st century.

Currently, electronic filing in circuit courts is permissible, but not mandatory. This is a striking distinction between the appellate filing structure and the trial court filing structure.

Circuit Court Clerks are elected constitutional officers and, pursuant to Article VII, § 4 of the Constitution of Virginia, they are only responsible for duties that are "prescribed by general law or special act." Because no general law or special act requires operation of an e-filing system, there is no consistent implementation of this paperless system.

That notwithstanding, the Supreme Court of Virginia has implemented the Virginia Judiciary E-Filing System ("VJEFS"). This system allows electronic filing of most civil cases in circuit court. As of this report, the following 51 localities are participating:

There are 121 circuit courts throughout Virginia. Thus, only 42% of localities are participating in VJEFS. Some courts use their own system for electronic filing system that is separate from VJEFS.

Virginia Judiciary E-Filing System (VJEFS)

1. Augusta
2. Bath
3. Bedford
4. Bristol
5. Brunswick
6. Caroline
7. Carrol
8. Chesapeake
9. Craig
10. Danville
11. Dickenson
12. Dinwiddie
13. Fauquier
14. Floyd
15. Fredericksburg
16. Grayson
17. Greene
18. Hanover
19. Henrico
20. Isle of Wight
21. King and Queen
22. Lee
23. Loudoun
24. Lynchburg
25. Mecklenburg
26. Montgomery
27. Newport News
28. Norfolk
29. Petersburg
30. Pittsylvania
31. Portsmouth
32. Powhatan
33. Prince Edward
34. Prince George
35. Prince William
36. Pulaski
37. Richmond City
38. Roanoke City
39. Roanoke County
40. Russell County
41. Salem
42. Shenandoah
43. Smyth
44. Southampton
45. Staunton
46. Tazewell
47. Warren
48. Washington
49. Waynesboro
50. Winchester
51. Williamsburg/James City

Many clerk's offices came online during and because of the COVID-19 pandemic. "Covid really served as the impetus for us implementing VJEFS because we wanted to keep foot traffic in our office down to protect the general public and our staff," noted K. Todd Swisher, Clerk of the Circuit Court for the City of Lynchburg. Lynchburg started offering the VJEFS in the summer of 2020.

This is probably big news to most lawyers throughout Virginia, especially because these localities are participating voluntarily. More interesting, however, is the mixture of rural and urban localities listed above. The value of e-filing extends beyond the borders of cities to all localities, regardless of where they are situated on the map.

Still, there are certainly challenges to implementing a paperless electronic filing system throughout all Virginia trial courts. That is not to say it cannot be done or that it should not be done. Rather, this Committee believes it is essential to continued progress and access to justice.

Paperless law offices have been a popular subject of discussion for at least the past 15 years. Indeed, many well-known websites are still creating content around whether a paperless law office is feasible or even practical for lawyers. Given the Supreme Court's approach to appellate filing, this is a conversation we should finally put to bed. As a competent Virginia lawyer, the standard should be a paperless law office. Even if a mirrored paper copy of everything is concurrently maintained, Virginia lawyers should also have a paperless version of everything as well. This is required in federal practice, and the Commonwealth should begin to follow suit.

Paperless clerk's offices are also becoming an increasingly popular topic of discussion. Some clerk's offices have effectively transitioned to being paperless. While that transition is not without its difficulties, paperless operation allows, at a minimum, access to a court file through the Officer of the Court Remote Access ("OCRA").

Access to OCRA is an expense for local clerk's offices to maintain, and it also bears a cost for lawyers who utilize it: approximately $100 per year per lawyer per court, although individual clerk's offices have discretion to set the fee amount. The fee is payable to the clerk of court, and it only covers that jurisdiction. It does not permit remote access to all clerk's offices using OCRA. If a lawyer wants access to all 121 clerk's offices, this becomes an expensive endeavor.

Although remote access in the trial courts is a good step forward, it is not near the degree of progress reflected by the Supreme Court in implementing VACES.

One problem for many practitioners is inconsistency in procedures for filing pleadings. For example, if a lawyer practices primarily in Lynchburg, she could file a lawsuit using VJEFS in Lynchburg and Bedford, but not in Campbell, Nelson, Appomattox, or Amherst. With a voluntary system, the process of filing a complaint looks different in neighboring circuit courts.

Additionally, VJEFS-participating circuit courts require that, if opposing counsel does not use VJEFS, then the case must be removed from VJEFS and filed in paper. This limits the applicability of VJEFS such that few cases have proceed electronically. Similarly, if the plaintiff chooses to file by paper, the entire case must be conducted by paper even if the defendant wants to use electronic filing.

Judge O. John Kuenhold and Robert T. Roper of Colorado noted in November 2007, that "an advantage of a permissive e-filing program at the beginning is that you can utilize the enthusiasts as a beta group to be sure you have things right." Virginia has enjoyed that advantage for the better part of a decade. Although the continued benefits of the permissive system are waning, transitioning to a mandatory system has thus far proven difficult.

The 2022 legislative session opened with a proposed house joint resolution requesting the Executive Secretary of the Supreme Court of Virginia "study the feasibility of establishing a uniform filing system for all state circuit, general district, and juvenile and domestic relations courts and provide a plan for the establishment of such system." This resolution would not implement a mandatory system but calls for a study of a mandatory uniform electronic filing system through Virginia conducted by the Office of the Executive Secretary. Even though it only required a study, the Senate Committee on Rules voted to continue the bill to 2023, effectively killing any progress on electronic filing for the near future.

Since 2016, the Virginia State Bar has emphasized that, as a matter of lawyer competence, "[a]ttention should be paid to the benefits and risks associated with technology." Rule of Professional Conduct 1:1, Comment 6. The mandatory implementation of VACES has accelerated that learning curve for many practitioners in Virginia. The implementation of mandatory e-filing in trial courts across Virginia may similarly burden practitioners for a short time. But, as we can see from other states and in our own Supreme Court, e-filing is the future of litigation.

NEW FORMS OF ADVOCACY ARE HERE TO STAY

Just as the COVID-19 pandemic transformed the day-to-day business of law by forcing the creation of new business models, adoption of new software platforms, and implementation of novel remote-work arrangements, it also revolutionized how attorneys practice law. A profession whose practice had long been confined to in-person courtrooms and conference rooms had to, in a manner of weeks, adapt to a new world of virtual law practice.

Although it took a pandemic to spur the innovations permitting virtual law practice, those changes are likely permanent. Clients and attorneys alike have come to appreciate the convenience and lower cost of videoconferencing and other forms of remote law practice, particularly in routine matters in which the benefits of an in-person presentation do not justify the extra costs. Courts, likewise, appreciate that hearings by videoconference offer previously unavailable benefits and flexibility. As a result, many seem poised to maintain remote hearings as an option even after the pandemic conditions abate.

6.1 THE PANDEMIC PAVES THE WAY FOR REMOTE ADVOCACY

Virginia laid the groundwork for some aspects of remote practice long before COVID-19 entered the scene. In 1983, the General Assembly enacted the Virginia Uniform Audio-Visual Deposition Act, Code §§ 8.01-412.2 to -412.7, which authorized the taking of depositions "by audio-visual means without a stenographic record." Code § 8.01-412.2. The Supreme Court of Virginia adopted Rule 4:7A the following year, establishing procedures and regulations governing the audio-visual depositions authorized by the Act.

As technology improved, the legislature permitted the use of electronic audio and visual communication systems for courtroom hearings in addition to depositions. See Code § 17.1-513.2 ("[I]n any civil proceeding . . . when otherwise authorized by the court, the court may, in its discretion, conduct any hearing using a telephonic communication system or an electronic audio and video communication system to provide for the appearance of any parties and witnesses.").

These statutes and rules provided the basis for a rapid transition to remote practice when COVID-19 upended the legal profession in Virginia. On March 15, 2020, just as the Commonwealth was first entering lockdowns and realizing the significant effects COVID-19 would have on every aspect of daily life, the Supreme Court issued Rule 1:27 implementing Code § 17.1-513.2 with detailed procedures and regulations for remote testimony and hearings in civil cases. The next day, the Court issued its first of many judicial emergency orders in which it required "attorneys to use e-Filing if available" and to use "telephonic or video technology . . . for all necessary hearings, trials, or other matters." From that moment on, Virginia courts and attorneys alike began innovating to ensure the public's legal business could go on despite the unavailability of traditional in-person venues. In doing so, they discovered that, notwithstanding its downsides, virtual law practice offered benefits that make it a valuable tool that will remain long after pandemic conditions end.

6.2 ADAPTING TO VIRTUAL LAW PRACTICE

Foremost among the advantages of virtual law practice is that it is remarkably more time- (and therefore cost-) effective for clients and attorneys alike. Prior to COVID-19, attorneys would drive or fly to distant locales to meet with clients and depose witnesses. Because no one knew of any practical alternative, clients footed the bill for both the meetings themselves and the travel costs.

No more. Now that clients realize the efficiency of meeting via videoconferencing software, they are considerably more reluctant to pay for expensive meetings and associated travel costs. To be sure, there are situations in which the significance of in-person meetings will justify their cost. Attorneys, however, can expect their clients to be more discerning in approving such meetings.

Remote hearings, depositions, mediations, and the like have their downsides. Even after two years of regular use, technical difficulties still plague attorneys, clients, and judges who use videoconferencing. The opening ritual of unmuting, selecting the correct microphone, adjusting the camera, and ensuring a stable internet connection has unfortunately become a familiar part of virtual law practice in all its manifestations. With preparation, however, many of these difficulties can be eliminated.

Beyond technical difficulties, attorneys also need to prepare to apply their advocacy skills in the virtual context. What works in an in-person hearing, mediation, or deposition may not be effective when staring at a box-filled screen. The remainder of this section offers suggestions for attorneys to tame technology and bring their advocacy A-game to remote hearings.

1. Become Familiar with the Software

The day of the deposition, hearing, or mediation is not the time to learn how a new videoconferencing platform works. Download whatever application you will be using well in advance, then make an account if necessary and familiarize yourself with the software's features and controls. Each platform functions differently — do not assume that familiarity with one will translate to another.

If preparing for a remote argument, the most useful resource for ensuring that your device is ready is the court's clerk's office. Most clerks' offices offer resources for attorneys preparing for videoconference arguments, including scheduling test videoconferences. The value of a test meeting cannot be overstated because it will be the only opportunity prior to the argument itself to connect your device to the court's system. In doing so, you may uncover connectivity issues, like interference from your local firewall, which would go undiscovered in test calls within your organization.

2. Prepare Your Workspace

Another advantage of a test meeting is that it provides an opportunity to familiarize yourself with the screen layout. Be sure to know the locations of the judge or judges, opposing counsel, witnesses, and the timer, if any, so you can plan accordingly. Ensure that your off-screen space is prepared as well. If you use multiple monitors, make sure you know on which screen the videoconference will display.

Your appearance on camera matters too. Use soft lighting to illuminate your face and position yourself so that the camera shows your head and shoulders. Take care in selecting a background because windows will cause your face to be shaded and busy backgrounds are distracting. Most videoconferencing programs offer virtual backgrounds if a neutral real-life background is unavailable. Be warned, however, that these backgrounds can blur the edges of your face and cause distracting distortions.

3. Minimize Disruptions

To minimize technical issues, connect using a wired connection rather than a wireless network if possible. Likewise, avoid competing with other users for bandwidth during the videoconference. Consider using wired headphones and a high-quality external microphone rather than your computer's defaults to improve sound quality, and make sure to silence other devices.

Following courtroom etiquette for remote arguments do much to avoid disruption. Treat joining the videoconference as you would walking into a courtroom during another hearing by minimizing your presence. You can accomplish this by muting your microphone and turning off your video before joining, not immediately afterward — having a new box with someone's face appear for a few seconds before disappearing is distracting for attorneys and judges alike. In any situation, remain muted unless you are actively speaking.

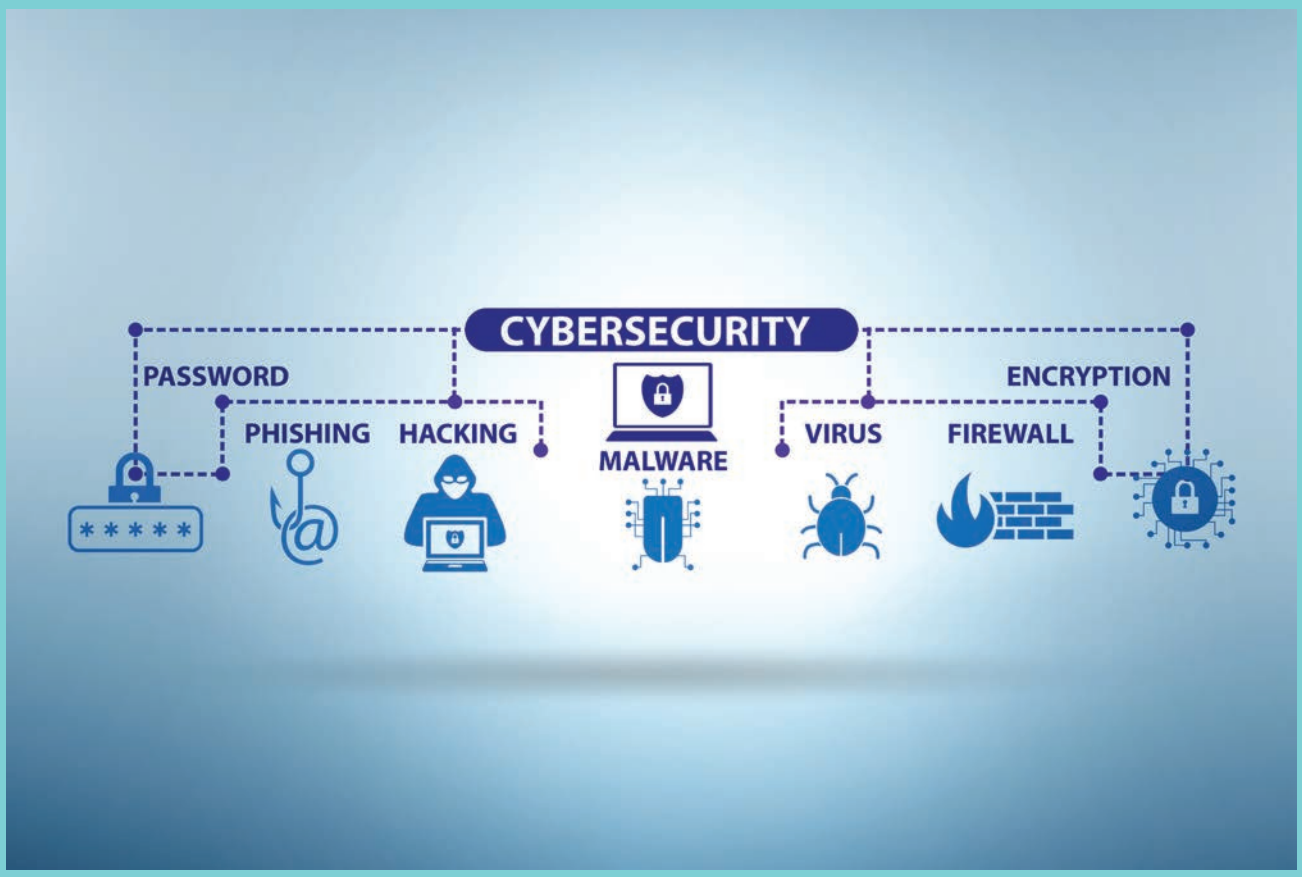
4. Respond to Your Audience

The biggest advantage of videoconferencing over more traditional teleconferencing is that you can see your audience and the other participants can see you. Look into the camera lens to make "eye contact," but scan the screen to look for cues from the other participants. Participants' body language can signal that a question or interjection is forthcoming during an in-person argument or mediation/negotiation. These subtle signals can be lost in a videoconference with counsel focused on the camera.

Although once a novelty for counsel and courts alike, virtual law practice will likely remain a regular part of the legal profession long after COVID-19 is gone. Developing best practices for virtual meetings and arguments now is a prudent way to adapt to the future practice of law.

CYBERSECURITY

Cyber insurance is an important risk mitigation tool for the modern attorney. Every day, the technology and methods cyber criminals use to steal data become more and more sophisticated. When one security flaw is fixed, another opens or when one phishing scheme becomes ineffective, social engineers create new scams. The constantly evolving threats make it difficult for the best firms to avoid compromise. Therefore, it's important for attorneys to not only be aware of cyber threats but to also know how to insure themselves against the threats that their security technology and cyber incident planning might miss.



7.1 DOUBLE EXTORTION RANSOMWARE: THE NEXT WAVE OF CYBER TERROR

The Cybersecurity and Infrastructure Security Agency defines ransomware as "a form of malware designed to encrypt files on a device, rendering any files and systems that rely on them unusable," unless a ransom is paid in exchange for a decryption key. With double extortion ransomware, threat actors go beyond encrypting data in place by also exporting victim data for sale or threat of publication. Now, cyber gangs have begun offering "ransomware-as-a-service" or RaaS, with threat groups offering malware and infrastructure in exchange for a fee or profit sharing. Cyber-criminal cartels began to emerge, with cyber criminals operating Soprano's-style gang families, both locking data and stealing it. The threat actors employ sophisticated tactics to execute their malicious activity, often utilizing software scripts to execute the removal of data and anti-forensic techniques to hide their tracks.

7.2 CYBER RISK INSURANCE AS A TOOL FOR PROTECTING CLIENT DATA AND FIRM RESOURCES

A data incident (data breach, ransomware, social engineering, fraudulent instruction, or phishing attack) can be devastating to a law firm. Data incidents create new business risks that law firms did not have to worry about a few years ago. As two leading law practice management commentators have observed, a data incident could mean "exposing sensitive client information and communications, totally wiping out all of a firms' electronic data, or freezing access to it." Mary Ann Altman & Robert I. Weil, 2 How to Manage Your Law Office § 13.04 (2021). Making the situation worse, the American Bar Association's 2021 Legal Technology Survey Report states that 25% of respondents reported that their law firm experienced a security breach at some point — a figure that is steadily increasing. No firm is truly safe. The firms that experienced a data incident range from solo practitioners to firms of over one hundred attorneys. In addition to the devastating nature of data incidents and their increased frequency, the cost to remediate a data incident is rising. Because of this, the ABA recommends that law firms of all sizes evaluate the utility of cyber risk insurance coverage as a way to transfer some of their risk as a part of their risk assessment process.

Insuring Against the Financial Risk of a Data Breach

Cyber risk insurance is a broad term that encompasses a variety of insurance products which mitigate the financial and other risks that "emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks." The financial implications of a serious data breach can cripple a law firm. According to IBM, the average total cost of a data breach in 2021 was $4.24 million, with higher costs incurred where remote work was a factor in causing the breach. Some of the costs associated with mitigating the impact of a data breach include forensic investigative activities, crisis management, business disruption, lost customers, reputational damage, notification to affected individuals and regulatory bodies, provision of call centers and credit monitoring for affected individuals, and regulatory fines.

The coverages provided in cyber risk insurance policies protect law firms from mitigation costs and provide access to knowledgeable cyber risk claims attorneys and other professionals. These individuals can coach a law firm through the incident response process and ensure that the firm has complied with all applicable state and federal laws.

Choosing Coverage

Cyber risk insurance is an evolving insurance market with over 19 categories of coverage available, "including first- and third-party coverage related to data breaches, cyber extortion, business interruption, data and software loss, physical damage,

and death and bodily injury." See Guidance Concerning Stand-Alone Cyber Liability Insurance Policies Under the Terrorism Risk Insurance Program, 81 Fed. Reg. 95313 (Dec. 27, 2016). Buyers should also beware that there are no standard forms or coverages. Therefore, the available coverages, exclusions, and costs may vary greatly based on insurers. Nevertheless, most policies contain some form of a few first and third-party coverages.

First-party coverages cover the firm's own losses or damages incurred when responding to a data incident within their own network. These coverages can include incident response (legal cost associated with responding to, investigating, and reporting a data incident), data forensic services (forensic investigation by computer scientists), affected party notification and credit monitoring (cost of mailing notices and providing credit monitoring to affected parties), business interruption (coverage for lost income due to a data incident), contingent business interruption (coverage for lost income due to the failure of a third party's computer system relied upon for business operations), cyber extortion (coverage for ransomware incidents), and reputational damage (coverage for certain public relations services for internal and external communications). See generally William E. Knepper & Dan A. Bailey, 2 Liability of Corporate Officers and Directors § 28.10 (2021).

Third-party coverage provides protection to law firms if a third party makes a claim against a law firm due to a data incident. Third parties include firm clients, regulatory agencies, and vendors. The most common causes of action are related to privacy violations. Third-party coverages include security and privacy liability (coverage for insurance defense and settlement cost), regulatory penalties (coverage for fines, and penalties associated with regulatory investigations), and Payment Card Industry Data Security Standards (PCI DSS) Liability (coverage for amounts a firm might pay as fines or penalties imposed by banks or credit card companies due to non-compliance with payment card company rules).

It is important to note that, in Virginia, lawyers have an obligation to make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, protected client information. Rule of Professional Conduct 1.6(d). A lawyer is not subject to discipline if he or she has made reasonable efforts to protect electronic data in the event of a data breach. *Id.* cmt. 20. However, the lawyer may still be subject to class action lawsuits and regulatory inquires and fines for not properly securing client data.

Law firms in the market for cyber insurance should also take note of the following five cyber insurance policy exclusions. First, firms should note if the policy restricts incident response counsel and vendors to a pre-approved list of the insurer's panel providers. A firm might be able to add its preferred counsel or vendors to the policy. However, insurers are often reluctant to utilize incident counsel and vendors that are not on their pre-approved list. Second and closely related, many polices require prior written consent before a firm can incur any cost in response to a data incident. This includes counsel, vendors, and ransom payments. Third, cyber insurance policies can have strict provisions that require notice within a certain time period after an incident. Notice exclusions are often linked to the discovery of an incident by key individuals within an organization, e.g., CEO, CFO. Fourth, some notice exclusions are drafted to exclude all remediation expenses incurred prior to the insurer receiving notice of the claim. Finally, lawyers should be aware of retroactive date exclusions. This exclusion would exclude coverage for incidents or events unknown to the lawyer prior to the beginning of the policy period. This is important because it is common for hackers to breach a victims' network 30 to 90 days before the breach is detected.

As stated above, there are no standard forms for cyber insurance. This is due to the lack of maturity of the cyber insurance market and the ever-evolving nature of cyber risk. Therefore, not every cyber risk policy affords the same protection. For instance, not every first-party policy will provide coverage for business interruption, which can be a large loss for a law firm experiencing a cyber incident. Because cyber risk policies can provide drastically different coverage depending on the provider, it is important that law firm directors select a policy that is tailored to the firm's needs and the type of data stored. Likewise, the amount of coverage needed varies with the size and type of firm and should be factored into the firm's analysis of what cyber risk policy to purchase.

Claims-Made and Reported Policies v. Occurrence Policies

Another factor to take into consideration when deciding which cyber risk policy to obtain is whether the policy is a claims-made and reported policy or an occurrence policy. Under a claims made and reported policy, the events that trigger coverage must take place and be reported to the cyber insurer during the same one-year period that the policy is effective. This policy requires law firms to be vigilant and diligent about reporting cyber incidents. As one court considering a cyber insurance policy's application observed, "[i]f a claim is not reported, no coverage is triggered, even if the events underlying the claim took place during the policy period. And after the policy expires, 'the insurer's potential liability ends." Gateway Residences at Exch., LLC v. Ill. Union Ins. Co., 917 F.3d 269, 274 (4th Cir. 2019) (quoting T.H.E. Ins. Co. v. P.T.P. Inc., 331 Md. 406, 628 A.2d 223, 227 (Md. 1993)).

Under an occurrence policy, coverage is afforded when a specific occurrence happens and does not depend on when the claim itself is filed. See Jeremiah Spires, 2 Doing Business in the United States § 29.18 (Matthew Bender, Rev. Ed. 2021). Importantly, coverage is only afforded for occurrences that happen during the policy period and occurrences that happen before the retroactive date will not be covered. It does not matter if the law firm is covered when a suit or other action is brought, so long as the occurrence happened when the policy was in force.

Claims-made and reported and occurrence policies are typically identical except for the sections dealing with the coverage-triggering event. Thus, it is important for law firms to determine what type of policy works best for the firm's needs.

Silent Cyber Coverage

Even if your firm does not have cyber risk insurance and suffers a cyber incident, it may still be possible for the firm to recover some of its losses under its other existing insurance policies. "Silent Cyber" coverage is a phenomenon where a cyber incident is covered under a business' traditional insurance policies. Firms should check their property or commercial general liability policies to determine whether they can categorize elements of the cyber incident as a theft, casualty, property loss, or business interruption.

It is important, however, for law firms not to rely on this safety net. Insurance providers are wising up to this workaround and are taking steps to include cyber exclusions in their policies.

Conclusion

In addition to taking reasonable steps to secure the firm's network, cyber risk insurance can help firms insure themselves against the fiscal impact of a serious data incident. Cyber insurance is now a necessary modern risk mitigation tool. The cyber insurance market is still maturing, and unlike other traditional insurance products, the coverages and exclusions have not been standardized. Therefore, lawyers should shop around to both select the right product for their firm and find a truly knowledgeable broker with experience selling cyber coverage. Another recommendation is to seek counsel from a data privacy and security attorney that has experience dealing with cyber insurance coverage.

ADVANCES IN VIRGINIA DATA PRIVACY LEGISLATION

Rarely do California and Virginia line up on legislative issues, but in 2021, the Virginia General Assembly made considerable progress toward protecting the personal data of the Commonwealth's residents by passing Virginia's Consumer Data Protection Act (VCDPA), Code § 59.1-575 *et seq*. In doing so, it became the second state — behind California — to pass sweeping consumer data privacy legislation. With an effective date of January 1, 2023, the VCDPA has many similarities to other comprehensive data protection laws such as California's Consumer Privacy Act (CCPA) and the European Union's General Data Protection Regulation, (GDPR).

8.1 VIRGINIA'S CONSUMER DATA PROTECTION ACT

The VCDPA is designed to capture those businesses processing Virginia resident consumer information. The VCDPA applies to "persons" that either (1) conduct business in Virginia, or (2) produce products or services that are targeted to residents of Virginia that, during a calendar year:

(i) control or process personal data of at least 100,000 consumers or,

(ii) control or process personal data of at least 25,000 consumers and derive over 50 percent of gross revenue from the sale of personal data.

It is important to remember that conducting business in the age of e-commerce can mean simply operating a website that targets residents in Virginia. The VCDPA — in a departure from California's CCPA — does not have a dollar threshold and instead focuses solely on consumers served or data sold.

The VCDPA provides certain rights to consumers regarding the collection and processing of their personal data. The VCDPA defines a "consumer" as a natural person who is a resident of Virginia acting in an individual or household context; it does not include a natural person acting in a commercial or employment context. In other words, it appears that employee information does not fall under the VCDPA.

The VCDPA exempts numerous entities from its provisions, including any "body, authority, board, bureau, commission, district, or agency" of Virginia or any of its political subdivisions; financial institutions subject to the federal Gramm-Leach-Bliley Act; covered entities or business associates governed by HIPAA or the HITECH Act; nonprofit organizations; and institutions of higher education.

8.2 CATEGORIES OF DATA

The VCDPA creates three categories of data; (1) "personal data", (2) "sensitive data" and, (3) "biometric data." Each contains carve-outs that distinguish Virginia's Act from many enacted privacy regulatory schemes. The VCDPA defines "personal data" as "any information" linked or reasonably linkable to an identified or identifiable natural person. It does not include de-identified data. The VCDPA also creates a sub-category of personal data called "sensitive data," which includes racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, citizenship, or immigration status and requires a consumer's consent before processing. Finally, the VCDPA governs "biometric data" and states that while such information includes information "of an individual's biological characteristics, such as fingerprint, voiceprint, eye retinas," it does not include "a physical or digital photograph, a video or audio recording," or information created for "healthcare treatment, payment, or operations under HIPAA."

8.3 CONTROLLERS

The VCDPA defines "controller" and "processor" similarly to the GDPR and imposes numerous requirements on both controllers and processors when collecting and processing personal data of consumers. Also similarly to the GDPR and the CCPA, the VCDPA affords consumers certain rights, such as the rights to:

- Confirm whether a controller is processing the consumer's personal data,
- Correct inaccuracies in the consumer's personal data,
- Delete personal data provided by or obtained about the consumer,
- Obtain a copy of the consumer's personal data, and
- Opt-out of the processing of personal data for certain purposes.

Controllers have 45 days to respond to a consumer's request, which may be extended for an additional 45 days, provided the controller informs the consumer within the initial 45-day period and provides the reason for the extension. With regard to consumer requests for information, the VCDPA requires a controller to "establish" and "describe in the privacy notice, one or more secure and reliable means for consumers to submit a request to exercise their rights under this chapter." This secure communication protocol "shall take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of such requests, and the ability of the controller to authenticate the identity of the consumer making the request." A controller cannot require a consumer to create a new account in order to exercise their consumer rights.

In addition, recent legislation passed by the General Assembly provides that a controller that has obtained personal data about a consumer from a third party shall be deemed in compliance with a consumer's request to delete such data if the controller either (i) retains a record of the deletion request and the minimum data necessary for the purpose of ensuring that the consumer's personal data remains deleted and does not use such retained data for any other purpose, or (ii) opts the consumer out of the processing of that data for any purpose except those purposes exempted pursuant to the VCDPA. Some other recent changes include the exemption of political organizations and certain § 501(c)(4) organizations from the VCDPA's provisions and the abolishment of the Consumer Privacy Fund originally created by the law.

8.4 ENFORCEMENT

The VCDPA provides the Virginia Attorney General with exclusive enforcement authority and the ability to issue a civil investigative demand to investigate violations. Violators are allowed a 30-day cure period to correct violations. Penalties include injunctive relief and fines of up to $7,500 for each uncured violation. The Attorney General may recover reasonable expenses incurred from investigation and case preparation, including reasonable attorney fees. The VCDPA provides no private right of action. Notably, in November 2021, a report issued by the VCDPA Work Group recommended certain modifications to the law which may result in changes prior to its effective date.

8.5 OTHER STATES IN COMPARISON

California, known for its current data protection laws, has taken additional steps. Although not fully effective until January 1, 2023, California's Privacy Rights Act, also known as Proposition 24, amends the CCPA by, among other things, narrowing the scope of businesses subject to the law, creating a new dedicated privacy agency — the California Privacy Protection Agency — and providing additional rights to consumers such as:

- Allowing consumers to request businesses to correct inaccurate information (with some exceptions),
- Requiring businesses to provide advanced notice if they intend to collect sensitive personal information from consumers and allowing consumers to request businesses stop selling, sharing, and using it,

- Requiring businesses to minimize use, retention, and sharing of personal information to what is reasonably necessary and proportionate to achieve the purposes for which the information is collected,
- Allowing consumers the ability to opt out of both the sharing and selling of personal information to third parties,
- Allowing consumers to request access to any information collected about them, regardless of when it was collected, unless doing so proves impossible or would involve a disproportionate effort, and
- Allowing consumers the right to sue a business directly for a data breach that exposes personal information such as usernames and passwords if the breach results from a business's failure to use reasonable security measures.

In addition, Colorado recently became the third state behind California and Virginia to pass comprehensive data privacy legislation when the Colorado Privacy Act (CPA) was signed into law in July 2021. Scheduled to take effect on July 1, 2023, the CPA is similar to both the CCPA and the VCDPA and provides consumers certain rights such as the rights to:

- Opt-out of processing of personal data under certain circumstances,
- Access data processed by a controller,
- Correction of inaccuracies in personal data,
- Deletion of personal data, and
- Data portability.

Although they are similar, the three pieces of legislation contain important differences, and practitioners should review each state's provisions carefully. Given these developments and pending data privacy initiatives in other states, 2022 is poised to be a busy year for data protection legislation.

CLOUD COMPUTING

Attention to cloud computing was gathering well before COVID came onto the scene in 2020. With the necessity of remote work and the increased expectations of clients for remote access to their data, the pandemic made cloud computing more important to the legal profession than ever before.

9.1 CLOUD COMPUTING USE

Surprisingly, the 2021 ABA Legal Technology Survey Report found only a 1% increase in the usage of cloud computing, up to 60% in 2021 from 59% in 2020 (which had stayed flat from 59% in 2019). Those reporting no usage of cloud services dropped slightly from 28% in 2020 to 25% in 2021. Small and medium-sized firms reported the highest use of cloud-based services at roughly 65%. Lawyers use popular cloud-based services at relatively high rates, like Dropbox (62%), Microsoft Teams (41%), Microsoft 365 (48%), and Evernote (11%). In addition, according to the 2020 CLIO Legal Trends Report, in 2019, firms using online client portals received 11% more casework than other firms, highlighting the importance of online access to clients.

9.2 CLOUD COMPUTING SECURITY

Beyond the advantages of remote access by lawyers and clients, cloud computing — if done properly — is more secure than local hosting. By utilizing a cloud service provider, a law firm unloads a good portion of its cybersecurity responsibility to that provider. The law firm's need to update and replace its software and hardware decreases. Additionally, a cloud service provider's security infrastructure will almost always be larger, stronger, and more complex than that of a law firm. Cloud service providers also generally have geographic redundancy to ensure that no data is lost if an event occurs at one server location.

It is important to note, however, that lawyers maintain the responsibility of protecting their client's information under Rule 1.6 of the Rules of Professional Responsibility. This specifically includes making "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to [client information]." Rule 1.6(d).

9.3 CLOUD SERVICE PROVIDERS

When utilizing cloud computing for client data, it is also important for lawyers to properly investigate the cloud service provider. In March of 2016, the Legal Cloud Computing Association, a group of cloud service providers, issued a list of security standards to which providers should conform in order to meet the highest standards of professionalism as well as ethical and legal obligations. Lawyers should review prospective (or current) cloud service providers to ensure they meet these standards.

- Physical and Environmental Measures:
  - Must disclose where data is housed — physically and geographically
  - Must meet certain industry certifications (SOC 2, or ISO 27001 or 27018)
  - Geographical redundancy — must have data centers in multiple locations
- Data Integrity Measures:
  - Encryption for storage at and transmitting data to and from data center
  - Disclose practices and frequency of testing for hacking and vulnerability
  - Disclose policies on limiting access by third parties and requests/subpoenas by third parties to obtain customer data, including customer notification
  - Have a data retention policy
- Users and Access Control:
  - End user authentication (multi-factor, password strength, device authentication, certificate protocols)
  - Addition/deletion of authorized users

    - Tracking, use of audit logs
    - End user's ability to add or delete data
    - Ability to retrieve data in a non-proprietary format; restoration or back up of inadvertently deleted data
- Terms of Service and Privacy Policy:
    - Terms of service understandable to end user
    - Privacy policy and restrictions on employee access
    - Uptime guaranty or assurance
    - Confidentiality of user's data
    - Ownership of data
    - Data breach notification
    - Disaster recovery

Cloud computing is no longer the "future of the practice of law." As more and more firms adopt cloud technology, it is the present. Understanding the landscape and ensuring proper precautions when engaging in the cloud space is not just good business — it is ethically mandated to ensure client data is protected. Fortunately, Rule 1.6 of the Rules of the Professional Conduct (and specifically Comments 19, 20, and 21) provides a roadmap to what "reasonable measures" mean, aiding lawyers as they adapt to this crucial new technology.

ARTIFICIAL INTELLIGENCE

In the 2019 Report, we asked if Artificial Intelligence (AI) would win if pitted against lawyers. Three years later, AI is keeping pace with humans and even surpassing them. Although AI has taken a backseat to the pandemic with remote work and its consequences being the primary focus of the legal profession, AI continues to grow and advance. The question today is how can AI complement what humans do?

The VSB does not endorse specific brands, however, we provide examples of specific products in this section to show what AI can already do for lawyers. Major legal research providers Fastcase, Lexis, and Westlaw all now offer litigation analytics services that analyze and deliver a judge's rulings on a certain issue in seconds, giving a lawyer a percentage likelihood that their client will win on that specific issue in front of that specific judge. These programs can also assess opponent lawyers and law firms; providing data analysis on how they behave, how they file, what are their go-to motions, and the success rate of their "tactics." This knowledge supplies a clearer picture on what to argue in court and a data-based decision on whether to take on a case or a client.

Another service, BriefCatch, uses AI to review draft briefs for citation compliance, sentence structure, and string citations, creating writing products that are easier to read and verify. This product is based on feedback from judges on the briefs they read. When a judge provides feedback, that feedback is incorporated into the product's algorithms, allowing lawyers to draft briefs with fewer errors that aggravate the judge.

AI is not just for litigation. MyLegalEinstein changes the way we review contracts by using AI to filter a term such as "payment" or "choice of law" to give you every mention of the topic and its sister terms, providing a complete picture of the topic in minutes instead of days. The issues show up faster, issue-focused reviews become timelier, and lawyers get a grasp of the draft contract in front of them with less effort.

While AI supplies much potential to change the legal profession in the future, it is shaping how the legal profession processes information and changing how lawyers and clients make decisions. Unfortunately, AI also unearths new threats to lawyers and clients.

10.1 AI AND THE LAW OFFICE

AI entered the legal profession the same way as many first-year associates entered the profession: by reviewing documents. Large piles of paper are now gigabytes of data on a computer or in the cloud. Concepts are now keywords that limit millions of documents to a few "hot" emails that prove your argument. Contracts can be thoroughly reviewed and compared against one another in an hour, a task that formerly took days or weeks of intense reading.

But AI is not a panacea. AI depends on a human to train it to perform that human's objectives. As a result, AI cannot perform some types of critical thinking and complicated decision making involving, for example, legal conclusions where multiple areas of law are implicated. AI, as of this writing, may not be able to independently make interdisciplinary decisions on matters involving legal, financial, or public relations considerations. Nevertheless, as commentators have observed, AI continues to make gains with improved decision skills. The legal profession, as with other professions, will have to deal with the implications of the gains and improvements of AI and how it will affect clients, the judicial system, and the public.

10.2 AI, ITS DARK SIDE, AND ITS SKEPTICS

Although AI wows its fans and performs more and more tasks that humans once performed, it still has its skeptics and naysayers. In October 2020, the ABA Law Practice Division's Legal Technology Resource Center (LTRC) found through a survey that 7% of lawyers use AI-based tools, a one percentage decrease from 2019. An additional 23% stated that they were not interested in adopting AI and 34% did not have enough information to decide whether AI could benefit them.

Cost, training, and implementation are major concerns for lawyers considering AI as a tool in their firms to improve their practices. Of lawyers LTRC surveyed, 35% were concerned about AI's accuracy and 21% cited cost as a reason not to adopt AI. The LTRC found that firms with over 100 lawyers were more likely to adopt AI as a firm tool.

Sometimes, AI gives its skeptics easy reasons to support their views. For example, chatbots on Facebook were taught to lie when negotiating purchases. These bots were trained to value maximizing sales and deceived to achieve those goals. These bots feigned interest in valueless issues to both parties, allowing Facebook to appear to make concessions by compromising on these valueless issues.

As another example, Microsoft introduced a chatbot named Tay in 2016. Users could talk to Tay and it would learn from user statements. It was pulled 24 hours later after users fed Tay racist and homophobic comments, leading it to inappropriate conclusions.

One of the scariest uses of AI is the deepfake, or video created with AI to show someone doing or stating something that he or she did not actually say. A perpetrator can use the words of someone else, even superimposing someone else's mouth or body onto the victim's body. The AI studies the victim's behavior, pulling from past video, audio, or written statements, and recreates the victim's voice for the impersonation.

These deepfake videos can deceive viewers into believing that the victim actually said or did what was on the video, because, as the unwitting would say, "video never lies." The challenge is showing how the video does lie, or for those who believe the video is true, how the video does not lie. Such challenges create new ethical dilemmas for all professions, especially the legal profession.

10.3 NEW ETHICAL LANDSCAPES (OR NOT)

New technology creates new challenges as nothing can be a complete panacea. As lawyers are delegating their duties, we continue to have the duty to supervise whoever we delegate our tasks, whether a person or a computer.

According to David Curle, Director of the Technology and Innovation Platform at the Legal Executive Institute of Thomson Reuters, "The ethical issues raised by AI are in many ways not that different from the ethical issues that lawyers have faced before. . . . When using tools in their work, whether AI-powered tools or any others, lawyers still have the same duties, including duties of supervision and independent judgment."

Therefore, lawyers will need to understand the fundamentals of AI and how it works as part of a lawyer's duties involving competence, diligence, supervision, and protection of client confidentiality and privilege. This includes knowing where the client's (and the lawyer's) data is stored, how he or she can access and alter the data, if needed, and how AI makes its conclusions based on the data stored.

Lawyers still have a duty to supervise (Rules 5.1, 5.2, and 5.3) those performing work on their behalf, whether it is another human or a computer doing the work. For example, when does data become encrypted and when does it unencrypt? Are these processes automatic or must someone ask the computer/AI to encrypt/decrypt? In other words, the AI cannot be in a black box in which the inputs and processes are impenetrable or not able to be discovered. Lawyers will need to know where the data is coming from and whether the AI is making biased conclusions.

More specifically, what biases are in the data? It will be essential to know how data works including where its flaws lie. Such knowledge may be gained through studying the history of the topic at interest to locate where assumptions may not have been accurate. For example, Loomis v. Wisconsin, as noted in the 2019 report, showed that an AI program, COMPAS, can influence a sentencing decision based on biased data to turn a defendant's sentence for crimes that did not mandate prison time into an 11-year sentence. The court denied the defendant's request to seek the data that COMPAS used to determine his sentence, a ruling that the Supreme Court decided not to review.

A lawyer should also be able to explain how a client's data gets processed through AI and what the lawyer does with the AI-driven conclusion.

The lawyer should also examine the AI vendor's security procedures, to ensure that client information remains confidential. These procedures should be outlined in frequently asked questions or in the terms of service and if not, the lawyer may contact the vendor for that information.

In order to help lawyers keep up with the changing landscape, vendors, bar associations, and lawyers "in the know" should educate their fellow lawyers on AI, its possibilities, the differences between black box AI and explainable AI, the operational basics with each program, and how client data is protected and processed. As Curle has noted, "The current rules of professional responsibility are general enough to cover the situation. They suggest two things: that lawyers must understand enough about a new technology to see the risks, and that lawyers must understand enough to see the benefits."

The goal is not for lawyers to understand everything going on with the AI, but rather to have a basic knowledge of how AI works. This basic knowledge should ensure that a lawyer can assess the benefits and risks of AI to accomplish needed tasks, shop for an AI vendor that fulfills his or her needs, be able to assess the quality of data that is getting fed into the AI program, and assure a client of the confidentiality and security of their data that is provided to the AI program.

Lawyers in the future will need to know how to read data and be able to detect issues that are either helpful or detrimental to clients. If an AI-generated conclusion does not look right, investigate the data to determine how the AI arrived at its conclusions; this can include figuring out the data's sources, accuracy, and bias. Such work helps all involved learn not only about the advantages AI has to offer but also the issues that AI has brought to the forefront.

CONCLUSION: THE LASTING TECHNOLOGICAL EFFECTS OF THE PANDEMIC

The COVID-19 pandemic forced most Virginia lawyers into some form of remote work for nearly two years. But when a full return to the office and the courtroom is safe, will everything really go back to the way it was? Or will bedroom slippers and sweatpants remain part of every professional's wardrobe?

All signs suggest that technological changes to the legal practice spurred by the pandemic are here to stay — at least in some form. Surveys show that even some of the more dramatic changes in day-to-day legal practice will continue after the pandemic. For example, one survey found that 83% of lawyers plan to continue meeting clients through videoconferencing. Less radical innovations are even more likely to become permanent. At least 95% of lawyers surveyed plan to continue storing data in the cloud, supporting electronic documents and e-signatures, accepting electronic payments, and using practice management software.

Perhaps more important than what lawyers themselves prefer, prospective clients see value in many pandemic-driven technological advances and want to keep them. Whereas in 2018 only 23% of consumers were open to the idea of working with a lawyer remotely, the same group found in 2021 that "79% of survey respondents saw the option to work remotely with a lawyer as an important factor that would have a positive influence on their decision to hire that lawyer."

Of course, the decision to retain technological systems created by the pandemic does not foreclose a general return to the office. Firms can continue to give their clients the option to meet remotely via Zoom while requiring that its lawyers attend those Zoom meetings from the firm's brick-and-mortar office. And data collected by office security provider Kastle Systems suggests that lawyers are physically returning to the office at meaningfully higher rates than other occupations. In April 2021,

near the beginning of widespread vaccination, law firms were operating at about 37% occupancy compared to 24% in other industries. While occupancy rates have fluctuated, that gap has persisted.

The push to return to physical offices could be driven in part by the culture of the legal profession. But law firm managers have also started to press physical presence requirements. Above the Law compiled the return-to-office policies for many national law firms and — despite delays due to later COVID-19 surges — the policies show that firms will require a return to using physical offices as the routine workspace once it's safe. Though some initially resisted these policies — especially the younger crowd — many lawyers are itching to see their colleagues and bosses again (or perhaps be seen by their bosses). Thus, as one author has observed, "an emerging consensus holds that predictions of the law office's demise were premature."

Still, remote legal work won't disappear completely. A Thomson Reuters survey of senior risk managers from 74 major U.S. law firms found 81 percent believe that "a significant increase in remote working (as compared to the pre-COVID period) will remain a permanent feature of their firms' operations." Some firms may close their brick-and-mortar spaces. But that's not likely to be the general rule. Instead, hybrid options and more flexibility surrounding remote work is likely to be the pandemic's lasting legacy in that regard.

Even if lawyers are physically going back to the office on a routine basis, more flexibility and hybrid work options will make tools like practice management software critical moving forward. Thankfully, most firms have adopted these technologies already. Stragglers will likely be punished by the market for falling behind. If your firm is falling behind, you could start a search for new software at this helpful blog post.

Although most lawyers and firms now have the logistical and technical capability to work remotely, it is worth a brief mention that consistent remote work from a location outside Virginia could present legal and ethical issues. Foreign lawyers working physically from Virginia but practicing entirely in another jurisdiction should have nothing to worry about now that the Supreme Court of Virginia has adopted Legal Ethics Opinion 1896. In doing so, the Court endorsed the view that Virginia

"has no interest in restricting the practice of a lawyer whose only connection to Virginia is a physical location within the state." As such, the DC lawyer can keep working remotely from her Alexandria home without a problem. The inverse is not true, however, as DC UPL Opinion 24-20 (2020) allows a foreign lawyer to practice law from her DC residence only if she is "practicing from home due to the COVID-19 pandemic." When the pandemic subsides, the DC lawyer's work-from-home options may be technologically feasible but raise important questions concerning the unauthorized practice of law.

Finally, the pandemic changed how lawyers interact with the court. Places like Fairfax County established remote court appearance procedures early in the pandemic, others followed soon after and Virginia courts have done their best to adapt to the challenges of the pandemic. Changes to court access for counsel and litigants have been significant, but less so for the public. The Virginian-Pilot recently reported that, although the pandemic ushered in dramatic changes to remote public access to courts in other states, those changes eluded most Virginians. "Despite 23 orders from the state Supreme Court addressing how and what court officials can and must do during the pandemic-induced 'judicial emergency,' none of the 120 circuit courts in Virginia appear to have availed themselves of video or audio feeds that would allow the public to see how their government is working without having to physically visit courthouses." It is hard to predict the long-term fate of those pandemic-driven technological changes we have seen in the courtroom. This is, in part, because authorization for some remote practices in Virginia's state and federal courts are tied to the state of emergency. See Code § 32.1-48.013:1 (allowing courts to authorize certain electronic filings when necessary "to protect the public, court officials, or others participating in the proceedings from exposure to a communicable disease"); Coronavirus Aid, Relief, and Economic Security Act, PL 116-136 (Mar. 27, 2020) (authority for remote hearings in criminal cases "shall terminate on … the last day of the covered emergency period").

Inertia itself will not be sufficient to keep all pandemic-driven innovations in place. And although the experience of practicing during the pandemic has shown courts what technology makes possible, that still leaves trickier normative questions. We now know what we can do, but what should we do?

Judges and lawyers adapted quickly when change was necessary to survival. The pandemic showed that specific technological tools can improve our practice. Videoconferences work and are often far more efficient than a cross-country flight. But perhaps more importantly, the last two years demonstrated that a profession sometimes mocked for its stodginess and resistance to change has the capacity to modernize and innovate rapidly. It would be nice to remember that going forward.

SUBMITTED BY

Respectfully submitted,

The Special Committee on Technology and The Future Practice of Law

May 23, 2022

Kellam T. Parks, Co-Chair
Jonathan V. Gallo, Co-Chair
Emily Hedrick, VSB Liaison
Graham K. Bryant
Seth R. Lindberg
Brittany S. Johnson
Brandon S. Osterbind
Andrew W. Grindrod
Darius K. Davenport
Christopher R. Fortier
Lisa S. Brook
Elizabeth M. Yusi
Reid Trautz
Sachin B. Kheterpal
Beth Burgin Waller

With special thanks to Geri Clark and Lia Cumming for their assistance with the design of this report.