Virginia State Bar Special Committee

THE FUTURE OF LAW PRACTICE

2019

INTRODUCTION

The VSB Special Committee on the Future of Law Practice was charged in 2014 with evaluating current developments in the legal landscape and assessing how these changes will impact the practice of law. In 2016, we issued our first report to the VSB along with a set of recommendations. To say that the pace of change in the practice of law has accelerated is an understatement.

As with the first report, we hope to illuminate the changing landscape of the practice of law both to help educate lawyers and to help prepare them for a continually morphing future. Even the early drafts of this report had to be edited to account for additional changes as we were writing.

Committee members have undertaken to meet regularly and work on a continuing basis to read everything we can find on the future of law practice - articles, ethics opinions, studies by other bar associations – the list goes on and on.

We previously identified a number of external forces affecting the practice of law:

1) 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;

2) increasing competition from nonlawyers service providers that offer legal information and legal documents to consumers;

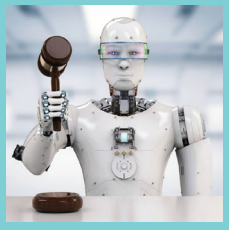
3) generational pressures that are likely to impact law firm business models – estimates are that 70% of law firm partners are baby boomers, while millennials are expected to make up half the global workforce in the next two years;

4) clients' dissatisfaction with billable hour arrangements encouraging lawyers to offer fixed fees and other alternative billing arrangements;

5) 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; and

6) accelerated globalization of legal services via both traditional models and technology, leading to an increase in multijurisdictional law practice and a decreasing relevance of geographical boundaries.

Recently, we have added artificial intelligence, blockchain and cryptocurrencies to the forces that are impacting the practice of law.



Additionally, the profession has taken on a focus of well-being for the legal community.

SUBCOMMITTEES

The committee is divided into three subcommittees:

TECHNOLOGY AND THE PRACTICE OF LAW

This subcommittee looked at advances in technology and how new technologies are changing law practice. It also studied how the internet and other forces have created a market for nonlawyer legal service providers.

ACCESS TO JUSTICE

This subcommittee focused on the "justice gap" — the unmet legal needs of a large majority of our low and middle-income population despite an over-supply of lawyers in the U.S. It also focused attention on initiatives by the organized bar and the efforts of other organizations to address the justice gap, including some projects in other U.S. jurisdictions to allow licensed paraprofessionals to deliver legal services.

ALTERNATIVE BUSINESS STRUCTURES

This subcommittee looked at jurisdictions outside the U.S. that permit nonlawyers to participate and have ownership in legal services firms, as well as the status of any similar initiatives or proposals in U.S. jurisdictions.

We realized that we needed input from outside our Committee and sought the perspective of some of those involved in shaping the future of law practice. The following people possessed knowledge and experience of interest to the Committee, and we invited them to make presentations to further our knowledge followed by wide-ranging questions from Committee members. We thank all of the guests below.

- Brian Kuhn, Co-Founder of IBM Watson Legal
- James Coyle, Colorado Supreme Court, Office of Attorney Regulation Counsel
- I.V. Ashton, President & Founder of LegalServer and Houston.AI
- Colin Rule, Vice President of Online Dispute Resolution, Tyler Technologies
- Robert Craig, CIO at Baker Hostetler
- Judy Selby, Principal, Judy Selby Consulting LLC/Insurance Consulting
- John Simek, Vice President, Sensei Enterprises/Speaker on blockchain and cryptocurrencies
- Anette Aav, Local Coordinator, Subtech Conference Tallinn, Estonia and Director of master's program in Legal IT at the University of Tartu School of Law
- Jim Calloway, Director of the Oklahoma Bar Association's Management Assistance Program

While the Committee is dedicated to teaching lawyers how to prepare for the future, it also recognized from the outset that it should not engage in any form of protectionism. Likewise, the organized bar does not exist to regulate the market. The mission of the VSB is to regulate the legal profession of Virginia, to advance the availability and quality of legal services provided to the people of Virginia, and to assist in improving the legal profession and the judicial system.

We feel the anxiety of lawyers facing a digital world that is often foreign to them — hence our emphasis on the need to educate lawyers and identify developments so they can find their place in that world, be competitive, and provide high quality legal advice and professional services.

This report is meant to be easily read, enhance lawyers' practices and advise them of probable changes they will see in the near and long term.

TECHNOLOGY
AND THE PRACTICE OF LAW

Law practice advisor and futurist Jim Calloway has famously written an article entitled *Every Law Firm is a Technology Business*. Few would dispute the truth of that title.

As technological change comes at lawyers with ever-increasing speed, it is difficult to keep up. And yet, we have an ethical duty to be competent, which includes understanding the risks and benefits of the technology we use.

To assist in that effort, the Committee has summarized some of the major developments since we issued our 2016 report to help lawyers understand the current forces influencing technology in law firms.

2.1 CYBERSECURITY

June 27, 2017 was not a good day for DLA Piper, then the #1 law firm by revenue in the world. The apparent ransomware attack that it experienced turned out not to be about money. GoldenEye, also known as NotPetya, was designed to destroy data.

The legal world was rocked by the news that DLA Piper was down. Phones and computers were knocked out across the firm (and some shut down as a precaution) with reporters and clients unable to reach anyone at DLA Piper via email (they got a "not deliverable" message). Not a "delivery delayed" message, but a "nobody home" message.

On July 3rd, DLA Piper announced that it had its email back, but was still bringing other systems online.

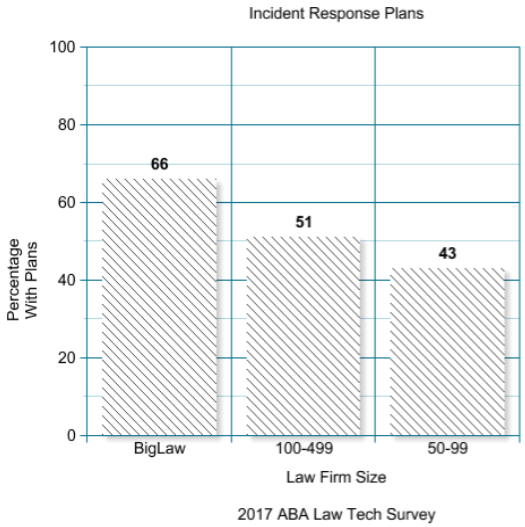
The fact that DLA Piper could be brought to its knees stimulated a lot of concern among law firms of all sizes which asked themselves, "If DLA Piper could be breached, what chance do the rest of us have?" The ultimate lesson may be that no law firm can consider itself safe, but that all law firms should take reasonable measures to secure their confidential data and to react to a data breach. Breaches come to large firms and small firms, with smaller firms often targeted because their security isn't as strong.

It is little wonder that Gartner, Inc. noted in 2017 that folks with cybersecurity skills have a zero percent unemployment rate.

2.2 CURRENT CYBERSECURITY STATISTICS

Let's look at some of the statistics which have been published since our 2016 report.

The 2017 ABA Legal Technology Survey, which had more than 4,000 respondents, yielded some interesting results. Twenty-two percent of respondents said their firms had experienced a data breach at some point, up from 14 percent in the previous year – that's a big escalation. Significantly, respondents at firms with 500 or more attorneys took the bulk of those hits.



Over one-third of law firms with 10–99 attorneys reported being compromised in 2017 alone. Some of the key consequences from breaches were downtime, loss of billable hours, destruction or loss of files — and, of course, having to pay consulting fees for remediating damages from the attacks.

One-quarter of all firms reported having no security policies, though all firms with 500+ lawyers did have such policies. Two-thirds of BigLaw firms have an incident-response plan. Of firms with 100–499 attorneys, 51 percent have an incident-response plan, as do 43 percent of firms with 50–99 attorneys. Obviously, the smaller the firm, the lower the likelihood of being well-prepared for a security incident.

That is disturbing, as is a 2018 study from CyberArk that surveyed 1,300 IT professionals and business leaders. Two of the more striking statistics are below:

- 46 percent of organizations said their cybersecurity strategy rarely changes substantially, even after suffering an attack.
- 46 percent of security professionals said that their organization can't prevent attackers from breaking into internal networks each time a hack is attempted.

While the study is not specific to the legal field, in all likelihood, the same findings would apply to law firms.

Verizon's 2018 Data Breach Investigations Report

The 2018 Verizon Data Breach Investigation Report (DBIR) includes data not only from forensic investigations conducted by Verizon, but also 67 contributing organizations. In total, the report covers analysis on over 53,000 incidents and 2,216 breaches from 65 countries. The number of incidents increased by 11,000 over the previous year.

Malware was involved in a far smaller share of breaches in 2017, compared to the previous year — 30 percent versus 51 percent, respectively — but when malware was discovered, ransomware was determined to be the cause 39 percent of the time. The frequency of ransomware attacks doubled in 2016 and again in 2017. Worse yet, Verizon noted ransomware attacks increasingly targeted critical systems and data centers, rendering entire businesses inoperable while increasing cybercriminals' leverage and escalating their ransom demands.

Mounir Hahad, head of Juniper Threat Labs at Juniper Networks, joined other experts in believing ransomware could soon take a back seat, if only temporarily. "We are likely to see a reprieve before the next storm of ransomware attacks," said Hahad. "Some threat actors are dipping their toes into the cryptocurrency pond to see if they can make a decent return on what is perceived as a lesser crime, namely cryptocurrency mining. Other threat actors will probably get pulled into the market of hacking for political actors, be it nation states or groups with political interests. This will lead to an increase in attacks like DDoS or destructors disguised as ransomware, and the targeting [of] critical infrastructure."

Outside of ransomware, other tactics used to facilitate breaches were hacking (the leading category, representing 48 percent of breaches), followed by errors (17 percent), social engineering attacks (17 percent), privilege misuse (12 percent), and physical actions (11 percent).

Verizon found users are three times more likely to be breached via social engineering tactics than through vulnerabilities. Incidents of pretexting — the act of obtaining information from someone by adopting a false identity or narrative — increased by a factor of five since the 2017 report, with 88 percent of these scams specifically targeting human resource departments in order to procure enough data to file a fraudulent tax return.

According to Verizon, in a typical organization, 78 percent of employees subjected to phishing simulations did not fail a phishing test all year, but an average of four percent of the workforce population fell for any given test. Even worse, the more phishing emails an individual clicks, the more likely he or she is to be fooled again in the future.

Based on the phishing simulation data, it takes an average of 16 minutes until someone in an organization first clicks on a phishing email and an average of about 28 minutes before an employee notes and reports the scam.

According to Verizon, 87 percent of examined breaches happened in just minutes or quicker, but only three percent were detected just as quickly. Sixty-eight percent of the breaches took months or longer to be discovered.

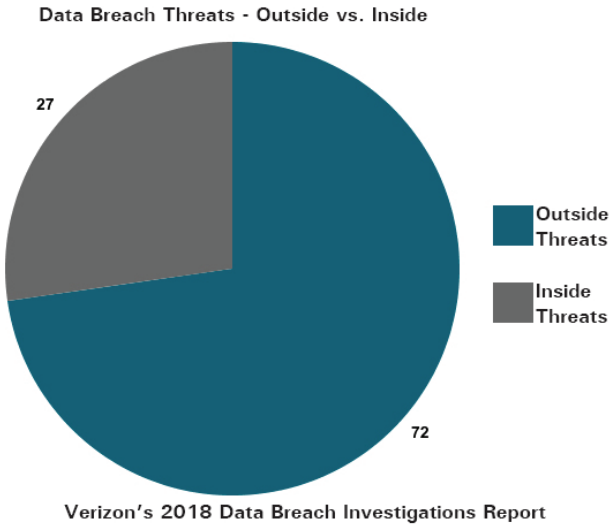
Strikingly, Verizon reported more than 43,000 breaches — over 13,000 in the U.S. — that were performed automatically by botnets that target organizations' customers by infecting their devices with malware that captures login credentials — an attack method that is so high in frequency that it was counted separately so as not to skew the report's numbers.

Other report statistics:

76 percent of breaches were financially motivated; espionage was the next most common motive.

24 percent of breaches affected health care organizations — more than any other industry, followed by hospitality and the public sector.

Most (72 percent) of the security breaches covered in the report were perpetrated by outsiders — including 50 percent representing organized criminal groups and 12 percent nation-state or state-affiliated threat actors. About 27 percent of the breaches originated from the inside — including 17 percent that were simply employee errors — as well as 2 percent that were from third-party partners.



Verizon's 2018 Data Breach Investigations Report

2.3 CYBERINSURANCE AND THE MORPHING OF THREATS

As data breaches grow in number and impact, it is clear that law firms need to consider cyberinsurance in order to manage their risk. And yet, according to a 2018 report from PricewaterhouseCoopers, only one-third of U.S. businesses have some form of cyberinsurance. Cyberinsurance, which tends to be both confusing and expensive, is nonetheless a necessity in a world where small businesses that are breached are likely to go out of business within six months, as noted by the 2017 Verizon Data Breach Investigation Report.

Virginia's endorsed insurance provider, ALPS, has a Cyber Response product which you can find more about at www.alpsnet.com/products/cyber-response.

Another worrisome trend is that cyber-attacks are increasingly complex. There are not yet simple solutions such as those that exist for ransomware. Law firms defend against ransomware by properly engineering their backups, meaning that a current backup is always available regardless of what happens to primary systems. That means they can restore their data without paying a ransom. Law firms should know that, as of 2019, less than half of those who pay a ransom actually receive a decryption key to unlock their encrypted data. It appears there is no honor among thieves.

We now face a new kind of attack. Rather than leaking a law firm's proprietary information or encrypting its systems with ransomware, attackers are beginning to manipulate the data on which the firm relies. They may also simply destroy the data, which would be a catastrophe for a law firm without a reliable backup isolated from the breached network.

Cisco researchers predicted in 2017 that more and larger cyberattacks would have the goal of destroying targeted systems of their victims, instead of financial gain or stealing information. The researchers cited the destructive nature of the Not-Petya attacks, that appeared to be traditional ransomware, but were in fact something designed to wipe a target's system, destroying its ability to operate. Cisco thinks that this model will be used more often and on a greater scale going forward, labeling this type of attack "destruction of service" (DeOS). These data manipulation or destruction attacks have the potential to be more catastrophic than ransomware or other breaches because they create uncertainty about the victim's data integrity.

2.4 CYBERSECURITY STANDARDS

In our 2016 report, we discussed the National Institute of Standards and Technology (NIST), whose Cybersecurity Framework is often used as a cybersecurity guide by solo/small/mid-sized law firms. Version 1.1, Framework for Improving Critical Infrastructure Cybersecurity, was issued April 16, 2018 and may be found at nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Since 2016, many solo/small/mid-sized firms began adhering to the Center for internet Security's (CIS) Controls. In March 2018, CIS released CIS Controls Version 7, the newest (and free) iteration of its original 20 important cybersecurity recommendations. The CIS Controls are a prioritized set of actions any organization can take to improve their cybersecurity posture. The controls are now separated into three categories: basic, foundational, and organizational:

- Basic (CIS Controls 1–6): These are key controls which should be implemented in every organization for essential cyber defense readiness.
- Foundational (CIS Controls 7–16): The next step up from basic — these technical best practices provide clear security benefits and are a smart move for any organization to implement.
- Organizational (CIS Controls 17–20): These controls are different in character from 1–16; while they have many technical elements, CIS Controls 17–20 are more focused on people and processes involved in cybersecurity.

The new CIS Controls, which may be found at www.cisecurity.org/controls/, align better with the NIST Cybersecurity Framework and map directly to it. Think of the NIST framework as the "what" and the CIS Controls as the "how." Together, these resources are concise and easily understood. Both are valuable free resources. In October 2017, CIS also published CIS Controls Implementation Guide for Small- and Medium-Sized Enterprises (SMEs) The guide should be read in conjunction with the NIST Cybersecurity Framework, which covers businesses with up to 500 users/employees.

In June 2017, NIST changed its password guidance in its Digital Identity Guidelines, which may be found at nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

The Digital Identity Guidelines provided these key recommendations:

- Requiring complex passwords is annoying — and it makes passwords harder to remember. It increases errors because artificially complex passwords are harder to type in and they don't help that much. It's better to allow people to use passphrases.
- Password expiration every 30 or 60 or 90 days makes no sense. It just makes everything harder to remember and causes security fatigue, a condition familiar to all law firm managing partners. The new thinking is that passwords should be checked against a database of known compromised passwords — no reason to change them if there is no indication of compromise. We are now seeing this recommendation implemented and expect it to accelerate in the future.
- Use password managers — they are the perfect way to keep people from reusing passwords and risking compromise in multiple places. However, the password used to gain entry to the law firm network should never be used elsewhere.

Security expert Bruce Schneier has said the old password rules were "failed attempts to fix the user. Better we fix the security systems."

2.5 DATA LOSS THROUGH EMPLOYEES

More law firms are beginning to train employees on cybersecurity from the user's point of view. Phishing is by far the most successful way to compromise law firms. A single training session can cut your risk by 20 percent. Annual training sessions (emphasizing phishing but including much more) are invaluable for creating "the culture of cybersecurity" within law firms.

Unfortunately, your greatest asset (your employees) are often your greatest source of risk. Employees should receive regular training to recognize threats such as social engineering, business email compromise scams, baited flash drives, piggybacking, tailgating, drive-by malware on websites, the dangers of sharing credentials, social media scams, wire fraud, W-2 scams, and much more. Even today, some of these terms may be unfamiliar to both lawyers and staff. **Everyone** needs training. A best practice is to make training mandatory and to demand attention by requiring everyone to turn their phones off.

A huge issue for law firms is preventing data loss when employees leave. According to Osterman Research's 2017 "Best Practices for Protecting Your Data When Employees Leave Your Company," 69 percent of organizations have experienced data loss from employee movements (departure, changing roles, relocation), and 50 percent of employees who left their jobs in the last 12 months took confidential corporate data with them.

Here are some recommendations to address these issues:

1. Give employees what they need access to — and no more. Use technology and policies to create alerts when data has been accessed inappropriately.
2. Get rid of data you don't need in accordance with your organization's data retention polices.
3. Clearly communicate policies on a regular basis.
4. Have an employee agreement that explains the duty to return data when leaving and indicate, within the bounds of state law, what action the employer may take if data is not returned. Make sure employees understand the agreement — and get a separate signature for the provision about returning data and the consequences for failing to do so. Do the same thing with an employee out-processing document. Have an exit interview — get a signature certifying that all data has been returned along with a signed acknowledgement that further access to your network would be an unauthorized criminal act. If you have any concerns about what the employee might have been doing on your network, preserve the departing employee's device and consider having a forensic image made.
5. Implementing strong passwords and using keycards to access company property is fundamental. Consider locking down USB storage devices. Use data loss prevention software to monitor data in the cloud. This software provides added security by alerting you and logging when files are moved or accessed.

Employees don't make it easy. An Insider Threat Intelligence Report from Dtex Systems found that 95 percent of enterprises surveyed had employees actively circumventing corporate security protocols, 59 percent of the organizations had experienced instances of employees accessing pornographic websites during the work day, and 43 percent had users who were engaged in online gambling activities.

2.6 WHY ARE LAW FIRMS SO FAR BEHIND IN CYBERSECURITY?

Legal-industry experts say law firms often lag behind their corporate clients in data security measures even though they are entrusted with valuable trade secrets, mergers and acquisitions data, and other sensitive information that is attractive to hackers. The reason behind the gap? Lawyers have only felt the threat recently, and law firms traditionally lag behind other industries in trying to become more efficient through technology, largely because they generally bill their services based on time.

"Law firms aren't necessarily committed to things that don't make them money per se," said Neil Watkins, the senior vice president of security, risk, compliance, and privacy at legal services company Epiq Systems. According to Mr. Watkins, law firms are at least three years behind what has become standard for data security in finance and other industries, though awareness is improving.

Marsh & McLennan Companies Inc.'s general counsel, Peter Beshar, said that in 2017 he began requiring his top 10 outside law firms to meet six cybersecurity standards, including using encrypted transmissions when sending messages externally, having detailed incident-response plans, and securing $5 million in cybersecurity insurance coverage.

Clearly, in-house counsel is requiring more of outside counsel — and not just at the big firm level. Clients of all sizes are pushing law firms harder to adopt security measures; and they often head for the exit door if they don't see improvement in a law firm's security. No law firm can expect to achieve perfect cybersecurity because it doesn't exist. However, that shouldn't stop law firms from "getting to good" and improving their cybersecurity measures year by year. Best of all, having a good cybersecurity posture has become an effective marketing tool, attracting prospective clients and retaining current clients.

2.7 ENCRYPTION

While Virginia has not tackled the issue of when, or if, encrypted communications are necessary, on May 22, 2017, the ABA Standing Committee on Ethics and Professional Responsibility ("the Committee") issued Formal Opinion 477R on lawyers' responsibility as to encryption, available at www.americanbar.org/content/dam/aba/administrative/law_national_security/ABA%20Formal%20Opinion%20477.authcheckdam.pdf.

The opinion's summary states:

A lawyer generally may transmit information relating to the representation of a client over the internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. ***However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.***

The opinion is an update to ABA Formal Opinion 99-413, Protecting the Confidentiality of Unencrypted E-mail (1999). Under Formal Opinion 477R, the Committee recognized that, unlike in 1999 when Formal Opinion 99-413 was issued, lawyers today "primarily use electronic means to communicate and exchange documents with clients, other lawyers, and even with other persons who are assisting a lawyer in delivering legal services to clients." It also recognized the explosion of varied devices and methods to create, store, and transmit confidential communications, all of which necessitated an update to the 1999 Formal Opinion.

The ABA Committee, considering all of these factors and ethical duties, concluded with the general language above. It also stated in Formal Opinion 477R that "a fact-based analysis means that particularly strong protective measures, like encryption, are warranted in some circumstances." The ABA Committee further offered considerations as guidance to lawyers

about the reasonable steps that should be taken to protect client data (these considerations, noted below, are further detailed within the Formal Opinion):

- Understand the nature of the threat
- Understand how client confidential information is transmitted and where it is stored
- Understand and use reasonable electronic security measures
- Determine how electronic communications about clients' matters should be protected
- Label client confidential information
- Train lawyers and nonlawyers assistants in technology and information security
- Conduct due diligence on vendors providing communication technology

The VSB needs to consider the issue of encryption in the context of its lawyers' obligations to safeguard client data. Virginia lawyers, having the same duties to safeguard client data as outlined in the ABA Model Rules, should become familiar with and include encryption available in their practices. This would include the encryption of objects, such as network and personal hard drives, as well as documents, whether stored locally or on the cloud. This also includes encryption of emails, which was once a difficult, expensive, time-consuming process; however, it is now easy, inexpensive and fast.

There are many reputable third-party solutions for lawyers to explore. These offerings generally work by filtering sent emails (from whatever email platform used) through a secure server/system or hardware device to encrypt them, and then the recipient gets an email with a hyperlink to retrieve the sent email. The user will need to create an account the first time, but then every email sent will be received in this manner, ensuring 100 percent encryption, every time. These companies usually offer bundled protection services, with encryption being just one, which can have an added benefit of increased protection of lawyers' client data once they explore their options.

2.8 CLOUD COMPUTING AS A SOLUTION TO DATA SECURITY CONCERNS

Law firms are searching for cybersecurity solutions as major data breaches have made them more aware of growing cyber threats. Firms have a 27.7 percent chance of experiencing one or more data breaches in the next 24 months according to IBM Security and the Ponemon Institute's 2017 Cost of Data Breach Study. The unfortunate victims will have to deal with the effects of lost or damaged data, repairing brand image, and securing their information technology (IT) infrastructure following a breach.

These factors have forced firm leaders to search for cybersecurity solutions that are cost efficient and that will provide the business resiliency needed to face the current cyber threats. Many firms are turning to cloud computing as the solution to their cybersecurity problems. The cloud offers many security benefits. However, it is important to remember that the cloud presents its own set of data security issues. This section will briefly discuss the pros and one critical con associated with cloud security.

2.8.1 CLOUD COMPUTING BENEFITS

One of the major benefits of cloud computing is transferring some of the cybersecurity responsibility from the law firm to the firm's cloud service provider. Tom Ruff, Vice President of Public Sector Americas at Akami Technologies, calls this "shifting the point of mitigation." This transfer of responsibility can do several things for a firm.

First, it allows firms to eliminate some of the complexity and cost associated with hardware replacement and securing their

IT infrastructure. Firms can trim their hardware replacement budgets because some of the expenses associated with replacing, operating, and maintaining internal servers have been transferred to the cloud service provider. Additionally, some of the costs and physical and technical issues associated with securing IT hardware and data have also been passed on to the cloud service provider. Firms can now exchange capital IT expenditures for a lower recurring operational expense since the cloud provider is securing their hardware, applications, and data. Depending on the size of the firm, this can equate to considerable savings. Do the math, though – cloud providers often overstate the savings.

Cloud computing allows firms to leverage the security infrastructure of bigger and more secure data organizations. Major cloud vendors usually have larger, more complex, and more secure cybersecurity infrastructures than a firm can build on its own. This provides a safer computing environment according to Philippe Very, professor of strategic management at EDHEC Business School. Major cloud vendors are some of the world's most secure cloud computing platforms because they cannot afford to be breached due to the nature of their business. This larger security infrastructure comes with more advanced application patching, threat detection, and better internal threat response-processes than the average law firm IT department could ever produce.

Reputable cloud vendors may also solve the problem of compliance with certain industry specific cybersecurity regulatory requirements. Law firms are now subject to the industry specific cybersecurity requirements of their clients and must be able to comply with HIPPA, Sarbanes-Oxley, Graham-Leach-Bliley, as well as many other federal and state laws and regulations. Cloud vendors that comply with these security frameworks provide firms with an easier way to secure themselves and comply with additional regulatory requirements necessary to secure client data.

2.8.2 CLOUD COMPUTING DATA SECURITY ISSUES

The cloud allows a firm to shift the point of mitigation and transfer some of the technology and security responsibilities to a cloud vendor, but it is not a cybersecurity silver bullet. As noted by Bob Violino of CSO Online, there are too many data security issues associated with migrating to the cloud to discuss in this section, such as vulnerabilities in the vendors' security protocols, accidental deletion of data by the cloud vendor, performing due diligence when selecting a cloud provider, or the shared technology vulnerabilities that are created when vendors co-locate or host multiple clients on one server. However, the most important factor, and the one that we can influence the most, is the compromise of cloud access credentials.

The Achilles' heel of the cloud is compromised credentials. Credentials can be easily compromised by using weak passwords, lax authentication processes, and poor credential management as employees' roles change or they leave the organization. Credentials are also easily compromised by phishing schemes. According to Cloud Pages, the most common type of phishing scheme involves a malicious actor who impersonates a legitimate company or individual to steal an employee's login credentials. Usually, the scheme involves an email that is sent with a sense of urgency to encourage an employee to click on a link or transfer funds.

An authorized user's credentials being compromised is like leaving the key in the front door of your house. A malicious actor can come and go as they please and appear to be an authorized user. Once malicious actors get access to a legitimate system user's credentials, they can eavesdrop on transactions, manipulate data, redirect clients, access critical areas of your computing system, and compromise the confidentiality, integrity and availability of client data and firm services according to the Cloud Security Alliance. For lawyers, unauthorized access to client data by a malicious actor may trigger violation of Virginia Rules of Professional Conduct 1.1 (Competence), 1.6 (Confidentiality), and 5.1 or 5.3 (if the incident involves the supervision of firm staff), if the lawyer fails to take reasonable steps to protect client data.

Firms can shift some of the responsibility for cybersecurity to their cloud providers, but Jay Heiser, vice president and cloud security lead at Gartner, Inc. reminds us that "the main responsibility for protecting corporate data in the cloud lies not with the service provider but with the cloud customer." It is not a problem for firms to share the responsibility for data security with a cloud vendor, but it is important not to abdicate totally that responsibility. Firms must recognize the weak points in any system they deploy and then structure policies and training to mitigate those vulnerabilities.

2.9 THE EUROPEAN UNION'S GENERAL DATA PROTECTION ACT

The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU, including in the U.S. The GDPR became effective on May 25, 2018. GDPR aims primarily to give control to individuals over their personal data.

Law firms which store, collect, or process the personal data of EU residents must now put in place appropriate technical and organizational measures to implement the data protection principles. Compliance with GDPR will require applicable US firms to meet some or all of these requirements:

- Adoption of the data protection principles
- Oversight of vendors and modification of contracts
- Specific disclosures in published privacy statements/policies
- Data protection impact assessments of certain kinds of technologies
- Appointment of a Data Protection Officer
- Breach notification to EU data protection authorities within 72 hours
- Opt-in only for direct marketing (including cookies)
- Right to be forgotten for data subjects
- Safeguards for international data transfers

Effective January 1, 2020, firms that do business in California or collect or process personal data of California citizens or consumers may be subject to the California Consumer Protection Act of 2018 (CalCPA). Key provisions of the CalCPA include:

- Right to know what is collected, sold or disclosed and to whom
- Right to opt-out or "Say No" to sale of private information
- Right to opt-in (affirmative authorization needed for sale of private information of a consumer under 16 years old)
- Right to request deletion of private information
- No discrimination: Equal service and price, even if privacy rights were exercised
- Data breach private right of action (not the act as a whole)

2.10 ABA ISSUES NEW ETHICS OPINION ON THE DUTIES OF LAWYERS FOLLOWING A DISASTER

Disaster recovery does have a legal technology component, and we have seen many disasters since our 2016 report was issued. The ABA released ABA Formal Ethics Opinion 482 on September 19, 2018. The opinion may be found at www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_482.authcheckdam.pdf.

In the opinion, the Standing Committee on Ethics and Professional Responsibility clarifies the ethical obligations attorneys face when disaster strikes.

Lawyers must follow the duty of communication required by Rule 1.4 of the ABA Model Rules of Professional Conduct, requiring lawyers to communicate regularly with clients and to keep clients reasonably apprised of their cases. Following a disaster, a lawyer must evaluate available methods to maintain communication with clients. The opinion instructs that lawyers should keep electronic lists of current clients in a manner that is "easily accessible."

Lawyers should pay attention to the duty of competency, Rule 1.1, which includes a technology clause that requires lawyers to consider the benefits and risks of relevant technology. Because a disaster can destroy lawyers' paper files, lawyers "must evaluate in advance storing files electronically" so that they can access those files after a disaster. Storing client files through cloud technology requires lawyers to consider confidentially obligations.

With due diligence, this should not present much of a problem. We constantly encourage lawyers to keep backups in the cloud. It is prudent to have a local backup, but the cloud provides additional security. As we learned from Katrina, having a backup at the office and one at home a mile away is not sufficiently protecting confidential data.

If a disaster causes the loss of client files, lawyers must also consider their ethical obligations under Rule 1.15, which requires lawyers to safeguard client property. For current clients, lawyers can attempt first to reconstruct files by obtaining documents from other sources. If they cannot, lawyers must notify the clients of the loss of files or property. To prevent such losses, "lawyers should maintain an electronic copy of important documents in an off-site location that is updated regularly." Yes, we're back to the cloud again.

A disaster could impact financial institutions and, therefore, client funds. Thus, lawyers "must take reasonable steps in the event of a disaster to ensure access to funds the lawyer is holding in trust." This could be highly problematic in some circumstances, but of course it is wise to do whatever one can.

A disaster may cause an attorney to have to withdraw from a client's case under Rule 1.16. "In determining whether withdrawal is required, lawyers must assess whether the client needs immediate legal services that the lawyer will be unable to timely provide," the opinion notes. We certainly saw a lot of withdrawals after Katrina. Entire law practices closed their doors, some forever.

The opinion also warns lawyers that they should not take advantage of disaster victims for personal gain: "Of particular concern is the possibility of improper solicitation in the wake of a disaster." Ambulance chasers, hurricane and flooding chasers — all distasteful, but they've been with us for a long time.

On balance, the opinion provides some good guidance and may help lawyers to form an incident response plan that complies with the guidance of this opinion. It's worth taking a look at your incident response plan to see if modifications are warranted. And if you don't have a formal incident response plan, this is a good time to formulate one! At a recent CLE with some 40 attendees, only a single attendee had a written incident response plan. We need to do better than that — put that high on your agenda.

2.11 ABA ISSUES NEW ETHICS OPINION ON ETHICAL DUTIES FOLLOWING A DATA BREACH OR CYBERATTACK

On October 17, 2018, the ABA issued Formal Opinion 483, Lawyers' Obligations After an Electronic Data Breach or Cyberattack, which may be found at www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_op_483.pdf.

This opinion builds on the standing committee's Formal Opinion 477R, released in May 2017, which set forth a lawyer's ethical obligation to secure protected client information when communicating digitally.

The new opinion states: "When a breach of protected client information is either suspected or detected, Rule 1.1 requires that the lawyer act reasonably and promptly to stop the breach and mitigate damage resulting from the breach."

The ethics opinion implicates Model Rule 1.1 (competence), Model Rule 1.4 (communications), Model Rule 1.6 (confidentiality of information), Model Rule 1.15 (safekeeping property), Model Rule 5.1 (responsibilities of a partner or supervisory lawyer), and Model Rule 5.3 (responsibilities regarding nonlawyers assistance).

There is a "rule of reason" overtone to the opinion, which states, "[a]s a matter of preparation and best practices, however, lawyers should consider proactively developing an incident response plan with specific plans and procedures for responding to a data breach. […] The decision whether to adopt a plan, the content of any plan and actions taken to train and prepare for implementation of the plan should be made before a lawyer is swept up in an actual breach."

This is, of course, what cybersecurity experts have said for a very long time — and, in our experience, all large firms tend to have an incident response plan. The smaller firms? Not so much.

The opinion also recommends, in a footnote, that firms should have data retention policies that limit their possession of personally identifiable information. We certainly agree with that. Many firms have "zombie" data — data they don't know they have until there is a data breach.

Since data breaches cannot entirely be avoided, the opinion says, "[w]hen they do [have a breach], they have a duty to notify clients of the data breach under Model Rule 1.4 in sufficient detail to keep clients 'reasonably informed' and with an explanation 'to the extent necessary to permit the client to make informed decisions regarding the representation.'"

The law firm should also advise clients of the actions the firm is taking to remediate the breach. This communication duty extends to current clients only, not former clients; however, state or federal laws may require data breach notification to former clients if personal identifiable information (PII) or other protected data has been lost, accessed or compromised.

2.12 MICROSOFT INTRODUCES SECURE SCORE

Microsoft has introduced a scoring system called Secure Score for the configuration and setup of its customers' Office 365 accounts. This scoring system is a metric that is intended to be used by clients to determine how secure their configuration is, allowing Microsoft to provide recommendations for its customers to improve their security posture.

Neither Office 365 nor Windows itself is secure "out of the box." Secure Score lets you track and plan incremental improvements over a longer period of time. The number one recommendation is to enable multi-factor authentication, but there are many steps lawyers can take to make Windows and Office 365 more secure.

More information is available at securescore.microsoft.com/.

2.13 ARTIFICIAL INTELLIGENCE COMES OF AGE

If you pit AI against experienced lawyers, who will win? In February of 2018, we saw perhaps one of the most evenly matched contests in a study by LawGeex.

The accuracy score was AI 95 percent and humans 85 percent when AI went up against 20 experienced lawyers. Participants were given four hours to identify and highlight 30 legal issues in five standard nondisclosure agreements (NDAs).

It took the humans between 51 minutes to more than 2.5 hours to complete the review of the five NDAs. It took the AI engine 26 seconds. Yes, that's pretty much a smackdown.

This wasn't the first such contest, but it appears to have been the most evenly matched.

But lest you feel too badly for the humans, LawGeex noted that this technology would allow lawyers to focus only on the relevant sections of a contract pre-validated by AI. It is more efficient, no doubt of that — but the fact that it requires less lawyer time no doubt fosters some degree of apprehension.

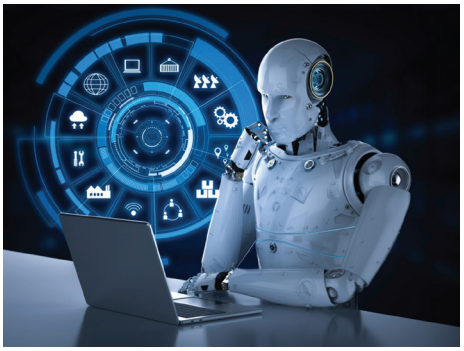
So, who do we believe? Consider these two quotes about AI:

> ***"It's the most exciting thing going on . . . It's the big dream that anybody who's ever been in computer science has been thinking about."***
> ***-Bill Gates***

> ***"I think we should be very careful about artificial intelligence. If I had to guess at what our biggest existential threat is, it's probably that . . . With artificial intelligence, we're summoning the demon."***
> ***-Elon Musk***

Starkly different views. And there is evidence that supports both views. Already, using chatbots, we have seen great progress in providing access to justice. And while chatbots are not true AI (they tend to follow decision trees), it is certain that AI can enhance access to justice as it matures.

2.13.1 AI AND HUMAN BIAS



And yet, we have seen evidence of darker aspects of AI. In particular, we have seen AI influenced by human bias — it is humans who teach/program the machines. And all too often, AI operates as a proprietary black box — no one is allowed to know how it really works.

In October 2017, *The New York Times* reported on a fascinating and disturbing story. In 2013, police officers in Wisconsin arrested Eric Loomis, who was driving a car that had been used in a recent shooting. He pleaded guilty to attempting to flee an officer, and no contest to operating a vehicle without the owner's consent. Those crimes did not mandate prison time.

But at Mr. Loomis's sentencing, the judge focused on Mr. Loomis's high risk of recidivism as predicted by a computer program called COMPAS, a risk-assessment algorithm employed in Wisconsin. The judge refused probation and handed down an 11-year sentence — six years in prison and five years of extended supervision.

COMPAS is a classic "black box" — no one knows how it works and its manufacturer won't be transparent about the proprietary algorithm. What do we know? Simply the final risk assessment score, which judges can consider at sentencing.

As the article notes, "Mr. Loomis challenged the use of an algorithm as a violation of his due process rights to be sentenced individually, and without consideration of impermissible factors like gender or race. The Wisconsin Supreme Court rejected his challenge. In June, the United States Supreme Court declined to hear his case, meaning a majority of justices effectively condoned the algorithm's use."

This may have far-reaching effects. Wisconsin is not alone in using algorithms in connection with sentencing decisions. How can we permit an algorithm, about which we know nothing, to have a major part in sending someone to prison?

Sure, judges do have sentencing guidelines. And within those guidelines, it is certainly true that a judge may have bias, based on color, ethnicity, gender, etc. So, it is easy to understand why states might employ technology to be part of the process, theoretically making it more neutral. Many people are probably unaware that the use of computerized risk assessment tools is quite widespread.

The author of *The New York Times* article argues that "shifting the sentencing responsibility to a computer does not necessarily eliminate bias; it delegates and often compounds it."

The architects of COMPAS probably fed historical recidivism data into the algorithm. From that, the program came to its own conclusions about things that might make a defendant a higher risk. And this is undoubtedly what happened in the case of Mr. Loomis.

Unfortunately, the historical data would necessarily reflect our biases. A ProPublica study found that COMPAS projects that black men will have higher risks of recidivism than they really do, but it forecasts lower rates for white men than they really have.

Besides receiving input that may be flawed, algorithms lack the human ability to see things on an individual basis. A computer cannot look into the eyes of a human, consider a difficult childhood or disability, and recommend, in light of the circumstances, a sentence that would help rehabilitate someone. This sounds very much like the argument against mandatory minimum sentences, which are seen as depriving judges of the ability to administer individualized justice. The argument seems equally compelling against machine sentencing.

Transparent algorithms in the criminal justice system can really make a positive difference. New Jersey used a risk assessment program known as the Public Safety Assessment to reform its bail system. This led to a 16 percent decrease in its pre-trial jail population. The same algorithm aided Lucas County, Ohio in doubling the number of pretrial releases without bail and cut pretrial crime in half. The difference here was that a published report explaining exactly how the system worked, which permitted experts to affirm that race and gender, among other constitutionally impermissible factors, were not a part of the decision process.

The only people who understand how COMPAS works are its programmers — certainly not trained in the administration of justice. Judges have legal education, must adhere to ethical standards, and are accountable not only for their decisions but also their reasoning which they must include in published opinions.

As the author of the article notes:

> "Computers may be intelligent, but they are not wise. Everything they know, we taught them, and we taught them our biases. They are not going to un-learn them without transparency and corrective action by humans."

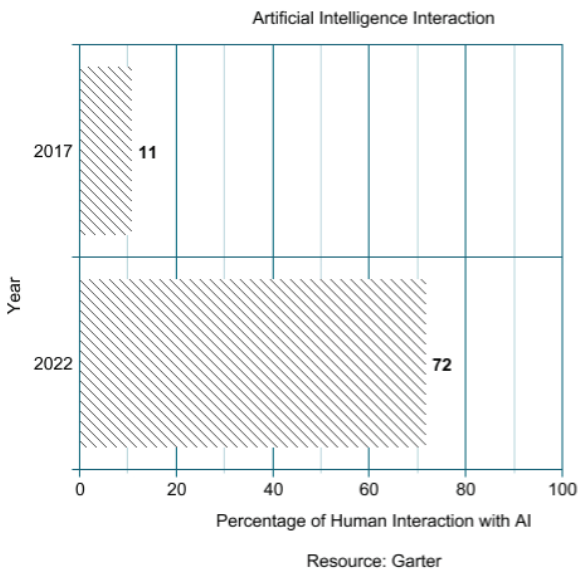
2.13.2 THE LEGAL SECTOR'S ROLE IN ARTIFICIAL INTELLIGENCE

It was notable to the Committee that one of our guest presenters, Brian Kuhn (co-founder of IBM Watson Legal) was sensitive to the ethical concerns surrounding AI. He specifically asked the Committee to give input to those in the AI industry about "what not to build." There is growing concern within the AI community about ethics, transparency, and guiding principles during AI development.

In March of 2018, Brad Smith, Microsoft's president and chief legal officer spoke at Princeton University and prophesized that AI will become an integral part of our lives in 20 years, influencing every part of our society, including the practice of law. He emphasized the need to ensure AI has accountability, as we reference above.

AI is now out of its infancy in law practice — we have seen significant implementations by a handful of AI companies in larger law firms. IBM Watson Legal, Kira Systems, and Neota Logic are perhaps seen the most often. Fastcase, which provides free legal research for Virginia lawyers, now has an AI sandbox where law firms can analyze their own data or Fastcase data, but it requires a one-year subscription with pricing beginning at $6,000 a month. Even with a discount for Fastcase subscribers, that is clearly outside the reach of most attorneys.

The large firms are generally pleased with their AI investments, and as we conclude the drafting of this report, AI is on solid ground with major achievements in contract analytics, e-discovery, legal research, predictive analysis and expertise automation. Research firm Gartner has predicted that 72 percent of people are expected to interact with AI by 2022 — the percentage in 2017 was only 11 percent. So, this trend is moving quickly. Though there is an enormous amount of hype in AI served up by vendors, AI has, since our last report, found solid footing and proven itself useful both in making the practice of law more efficient and in aiding access to justice.



Resource: Garter

Is AI ready for the small firm market? It's certainly getting there. IBM's legal AI, ROSS, now has a little sister designed for smaller firms: EVA. Completely free to use, EVA uses a stripped-down version of ROSS to analyze uploaded briefs and other legal documents. It checks whether cited cases remain good law, provides links to view cited cases, and even allows users to find cases using similar language to selected text in the uploaded document. By using AI to streamline tasks that are ordinarily time-consuming with traditional legal databases, EVA is paving the way for AI to become a standard part of solo and small-firm lawyer workflows.

We expect that pricing will drift downward as AI permeates our lives — and smart companies learn how to make a profit serving smaller firms. In the meantime, prudent lawyers will keep an eye on AI developments and what they may mean to their practices.

"Where the technology is going to be in three to five years is the really interesting question," said Ben Allgrove, a partner at Baker McKenzie, a firm with 4,600 lawyers. "And the honest answer is we don't know." March 19, 2017.

2.14 BLOCKCHAIN: POWERING MORE THAN CRYPTOCURRENCIES

Bitcoin became a household name over the last year as front-page news reports tracked its meteoric rise and analysts speculated whether the "Bitcoin bubble" was about to burst. The recent roller-coaster ride in bitcoin value, peaking at an all-time high of just under $20,000 per bitcoin, demonstrates that digital currencies have real-world value. Unsurprisingly, the financial and legal sectors are paying close attention.

The advent of Bitcoin and the blockchain technology that powers it heralds a new period of disruption — and opportunity — for the legal profession. Lawyers will need to become familiar with how these technologies work in order to remain competitive as the practice of law continues to evolve.

2.14.1 THE ADVENT OF CRYPTOCURRENCIES

Despite being the most familiar name, Bitcoin is but one of many "cryptocurrencies." 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.

Cryptocurrency is serious business. The major cryptocurrencies have a combined market capitalization well into the billions. The explosion in cryptocurrencies is due in large part to the unique value they have compared to any other medium of exchange: they are decentralized.

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.

The benefits of cryptocurrencies over other currencies means that many people want to purchase goods and services with cryptocurrency. Unsurprisingly, many lawyers are under pressure from their clients to accept cryptocurrencies as payment for legal services, and some are already doing so.

To date, Nebraska is the only state that has issued a legal ethics opinion (No. 17-03) specifically addressing a lawyer's duties when receiving cryptocurrency as payment for legal services. That opinion states that Nebraska lawyers may accept cryptocurrencies, but only if they immediately convert them into U.S. dollars. Any refunds relating to the transaction must also be made in U.S. dollars.

The ruling is rooted in the traditional rule that lawyers cannot access client funds until earned, and the fee earned must be reasonable. Lawyers may accept money or property in exchange for services, but the property must have a valuation — otherwise, it would be impossible to determine if the fee is reasonable.

Cryptocurrencies currently rest in the grey area between money and property. The Nebraska ruling dodges the fluctuations in cryptocurrency values by forcing lawyers to convert cryptocurrencies into U.S. dollars immediately, functionally assigning a value to the cryptocurrency. But in doing so, the opinion forces lawyers to bear the transaction costs of converting cryptocurrency into U.S. dollars.

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.

2.14.2 BLOCKCHAIN AND DISTRIBUTED LEDGER TECHNOLOGY

The technology that makes cryptocurrencies possible and allows for a decentralized market is called "blockchain." Think of blockchain as, fundamentally, a digital transaction ledger. Blockchain technology is the latest stage in the evolution of the paper transaction register every old-time general store used to track sales.

A blockchain is a decentralized, purely digital ledger that encrypts every transaction and distributes it throughout a network. For this reason, blockchain is also called distributed ledger technology. The distribution of transactions across a network is what makes blockchain technology decentralized — rather than a single central computer that hosts the blockchain, there are multiple identical copies of the whole blockchain across the network.

Because each transaction recorded on the blockchain is encrypted, the blockchain takes the form of a public record that is nearly impossible to hack or alter. The blockchain keeps a complete record of every transaction from its inception forward, validated and confirmed by cryptographic calculations performed by the distributed computers. Each transaction is recorded as a new "block" on the blockchain, preserving an indelible record that a transaction occurred. The result is a reliable digital system that permits transactions to occur securely and without a need for third-party facilitation.

Blockchain thus allows for automatic, decentralized proof of trust. The participants in a blockchain transaction do not necessarily know one another, but because of the secure and reliable nature of blockchain technology, they can exchange value with certainty despite the lack of a central validating authority.

To illustrate in more concrete terms how blockchain technology works, consider the following analogy for a cryptocurrency blockchain. Imagine a public space filled with countless safes. Each safe has a unique identification number, a lock requiring a key, a glass window revealing its contents, and a one-way slot for sliding in money. Only one key exists for each safe, which is delivered once someone claims that safe. There is no limit to how many safes a person can claim. No one owns the safes; possessing a key merely gives that person the power to access the contents of that safe when he or she wishes. It is a public space, so anyone can view the contents of any of the safes at any time. Because no information connects the key owner to the identification number on the safe, there is no way to tell who has the key to which safe.

In this analogy, the group of safes is the blockchain, and the contents of each safe are the units of cryptocurrency. The identification number of each safe would be a particular address on the blockchain, and the key is the private key that unlocks that address. Even though cryptocurrency is digital, it cannot be "copied and pasted." Just as making a duplicate key to a safe does not double the amount of money in the safe, copying the private key to a blockchain address does not double the amount of cryptocurrency stored on that blockchain address.

This limited analogy applies primarily to the sort of blockchain used with Bitcoin: a completely public blockchain designed to be transparent to anyone who cares to look. Anyone who has a hard drive with a few hundred gigabytes of free storage space could download the entire Bitcoin blockchain to their own computer and view it at their leisure.

Other cryptocurrencies use a similar model but with an added layer of privacy. Whereas every single transaction on a public blockchain like Bitcoin is visible to anyone looking, other blockchains are visible only to a permissioned group of known participants.

2.14.3 ARE BLOCKCHAINS REALLY HACK-PROOF?

Many people respond to claims that blockchains are "nearly impossible to hack or alter" with skepticism, often pointing to high profile attacks resulting in the loss of millions of dollars in cryptocurrencies. These highly publicized incidents generally involve breaches of cryptocurrency exchanges, not the blockchains themselves. The distinction is subtle, but important.

A cryptocurrency exchange is an online marketplace where cryptocurrency investors can trade out their cryptocurrencies for traditional currencies, like U.S. dollars or Euros, for a fee. Many of these exchanges allow users to store the private keys for their cryptocurrency wallets on the exchange website itself, similar to clicking "remember me" when a website asks for your username and password. And just like a saved username and password, if a malicious third-party gains access to your private key, it gains access to your wallet and can swipe all of your cryptocurrency. Because cryptocurrencies are decentralized by design, no authority can reset your private key or restore your cryptocurrency — when your crypto is gone, it's gone for good.

For this reason, cryptocurrency exchanges are particularly vulnerable to attacks. Since 2011, at least 56 cyberattacks have been directed against exchanges and other digital currency platforms, resulting in a cumulative hacking-related loss of over $1.6 billion. Most recently, in July 2018, the cryptocurrency exchange Bancor lost $23.5 million in cryptocurrency after one of its virtual wallets was compromised. January 2018 saw perhaps the largest single breach, with the Japanese platform Coincheck losing $535 million in cryptocurrency following a breach.

Despite all these attacks on exchanges and similar platforms, the blockchains making each cryptocurrency possible have remained largely unscathed. Blockchains are incredibly difficult to breach, but there have already been a few isolated instances of successful attacks on the blockchains themselves. These attacks all involve a subset of blockchains that permit storage of executable computer code in the blocks themselves. Storing code within a blockchain goes beyond simple transaction recordation and has a wealth of potential applications (discussed further in the next section).

The ability to store code within these blockchains makes them both rife with possibilities for innovation and vulnerable to exploits. The most notorious blockchain breach occurred in 2016 when an unknown assailant exploited a series of vulnerabilities in code stored on the Ethereum blockchain to steal $55 million in Ether, the cryptocurrency associated with that blockchain. This attack was eye-opening because Ethereum is a major blockchain, widely perceived as second only to the Bitcoin blockchain in popularity and usage.

In September 2018, a company known as DEOS Games fell victim to a similar exploit. DEOS Games used the EOS blockchain's ability to store code in order to run an online gambling business processing bets made in the EOS cryptocurrency. A hacker known as "Runningsnail" used his own malicious code stored on the same blockchain to interact with the code behind DEOS Games, causing DEOS Games to send Runningsnail a total of 4,728 EOS — or $24,250 given the EOS exchange rate at the time of the attack.

The main takeaway is that blockchains are, on the whole, far more secure than traditional websites secured only by a username and password combination. That's why most breaches associated with blockchains and cryptocurrencies take place on exchanges or similar platforms. The only known blockchain breaches are those that permit executable code storage within the blocks. Even among these blockchains, breaches are all but nonexistent.

As discussed further in the next section, the same code-storage ability that makes these blockchains vulnerable also gives them the greatest potential for significant innovations that could change the legal profession as we know it. That means that as we see a proliferation of blockchain applications, there will in all likelihood be a corresponding uptick in attempts to breach these blockchains.

2.14.4 APPLICATIONS AND IMPLICATIONS FOR LAWYERS

The essential attraction of blockchain technology is that it allows for trusted, secure transactions without recourse to a central authority, such as a bank. With that in mind, it may come as a surprise to learn that financial institutions are leading the charge in blockchain technological development.

But it makes sense for big banks to take a keen interest in blockchain's disruptive potential. After all, if banks make much of their profits from transaction costs, then they stand to lose out if decentralized transactions become the norm.

The financial sector is not alone in investigating blockchain's potential to revolutionize the marketplace. Other industries and even governments recognize the need to prepare for blockchain. In January 2018, Virginia lawmakers introduced a resolution to establish a joint subcommittee "to study the potential implementation of blockchain technology in state recordkeeping, information storage, and service delivery." Although the resolution failed in committee, its introduction demonstrates an awareness that blockchain technology could alter even governmental services.

Likewise, the legal field will not be immune from blockchain-driven changes. Lawyers must take notice of blockchain or risk being left behind. Just as nonlawyers entrepreneurs are leveraging technology to provide legal services more efficiently than traditional law practice models can, the legal industry will be unable to adopt blockchain technology independently of other market constituencies.

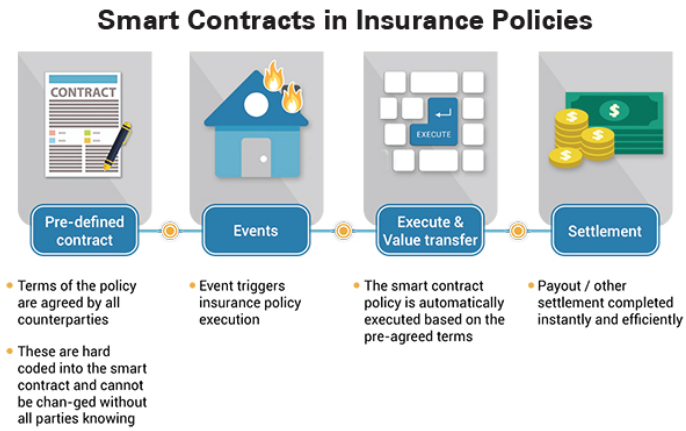
Robert Craig, chief information officer at Baker Hostetler and a leader in legal applications for blockchain, has noted that four key entities will be involved as the legal ecosystem begins to embrace blockchain: in addition to law firms and the law schools, clients — especially corporate clients leveraging blockchain in their own business — and competing technology startups focused on legal services will drive how the legal industry will adopt blockchain technology.

> "It is a matter of when, not if, blockchain will affect ordinary law practice,"
> - Robert Craig

Potential legal applications for blockchain technology are already becoming apparent, including some that will affect even the smallest law practices:

- Smart Contracts — Smart contracts are perhaps the most commonly cited legal application for blockchain. As alluded to in the discussion of blockchain breaches above, the same distributed ledger infrastructure that permits blockchains to track cryptocurrency transactions can be used to store executable computer code. Using "if this, then that" logic, entire contracts can be coded into an immutable, self-executing blockchain. This ability has major implications for transactional lawyers.

Smart Logistics Contracts in the Internet of Things



For instance, a complex logistics contract could be coded into a blockchain along with contingent triggers. One term might provide that if delivery occurs before a certain date, then the seller receives a monetary bonus. internet of things tracking devices would automatically detect arrival of the shipping container at the port, triggering the relevant smart contract provision. With this technology, deliveries could be tracked and payments sent without the need for manual verification or paperwork filing. In ordinary logistics contracts, these provisions are often the subject of litigation, and even if all goes as planned, payouts can take months to verify and process. Smart contract applications could dramatically streamline the logistics industry, and major companies, such as Maersk, are already investing heavily in the technology.

What if there's noncompliance with the contract? The same "if this, then that" logic coded into the blockchain smart contract would apply. For instance, if delivery occurs after a certain date, then the shipment is rejected. If the particular exigency is not contemplated by the smart contract, ordinary principles of contract law would apply, with the smart contract being construed against the drafter — the party who coded the agreement terms into the blockchain.

Logistics contracts are just one illustration of smart contract potential. As the illustration above indicates, even ordinary insurance contracts could become more efficient using the blockchain smart contract model.

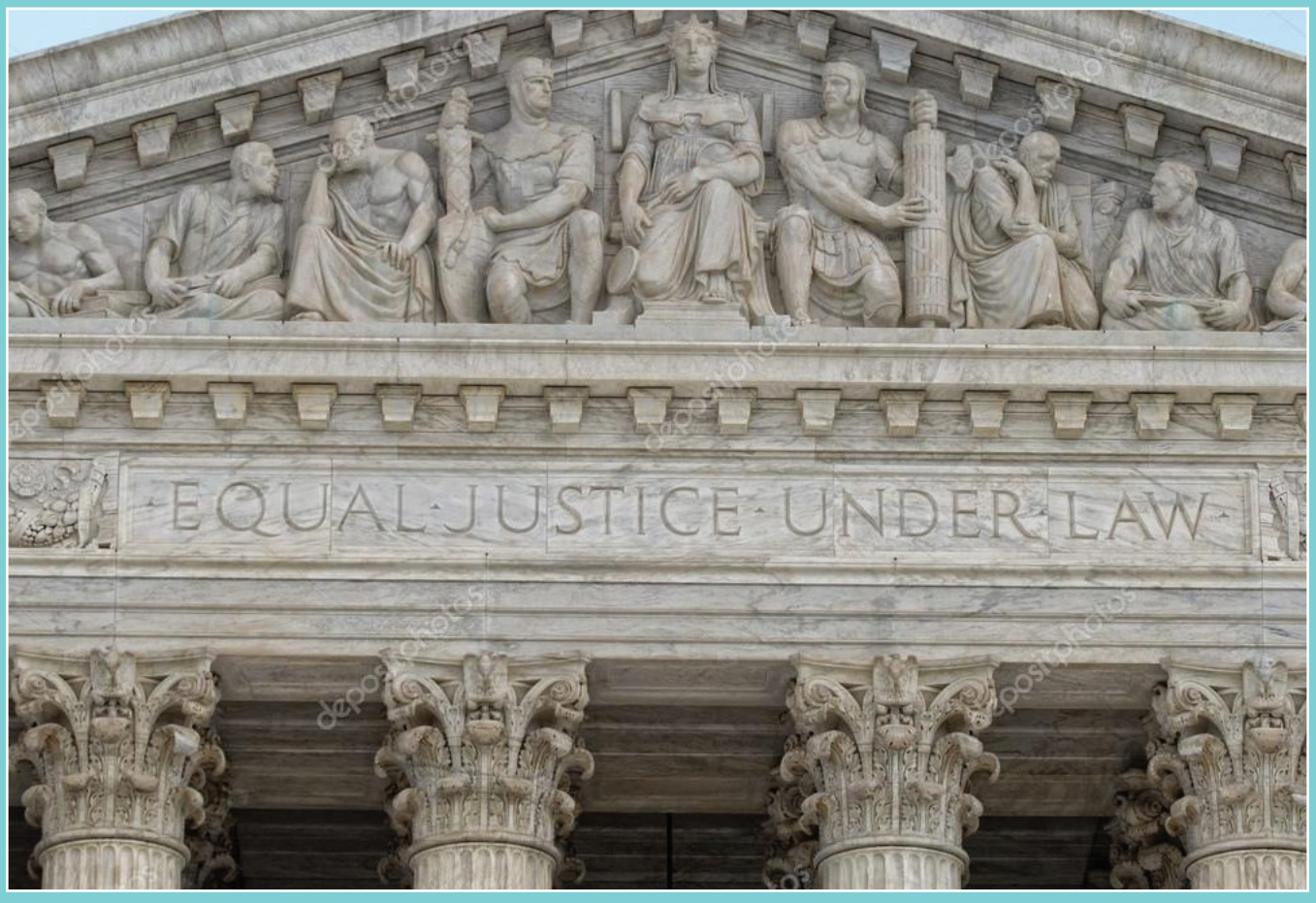
- **Corporate Filings** — Because blockchain provides an unalterable record of transactions, it naturally lends itself to record management. Delaware launched the Delaware Blockchain Initiative in May 2016 seeking to leverage blockchain technology to overhaul the laborious, paper-based filing system in the Delaware Division of Corporations. The blockchain technology promises to automate record retention, release, and renewal, as well as streamline UCC record searches. When fully implemented, the system should reduce errors and operational costs when compared to a manual filing process.
- **Land Records** — For many of the same reasons, blockchains could be the deed books of the future. Rather than a dedicated room in a courthouse filled with massive volumes, land records recorded on a blockchain ledger would be easily searchable and immutable. All transactions are recorded on a blockchain for all time, meaning land record blockchains have the potential to eliminate broken chains of title caused by sloppy recordkeeping and permit instant recording. Further, because of the distributed nature of blockchain technology, banks, real estate offices, insurance companies, and property lawyers could all have access to the entire chain from their own computer — no need for a trip to the courthouse.
- **Notarization** — Blockchain is, at its core, a technology designed to provide trust. Just as signet rings, wax seals, or diplomatic apostilles are designed to authenticate documents and prevent fraud, blockchain has the ability to serve as an authentication technology that could ultimately replace inefficient notarization. Several start-ups employ blockchain technology to offer online notary services, and Microsoft Office has already announced integration with some of these authentication technologies. This vote of confidence suggests the market for blockchain-based notarization services is on the rise.

These examples illustrate just how versatile distributed ledger blockchain technology is. Given the myriad applications for blockchain in the legal world, now is the time for lawyers to become familiar with the technology. A lawyer does not have to be a programmer or computer scientist to be effective — but he or she does need to cultivate a general understanding of blockchain and its related technologies in order to be prepared for life in tomorrow's law office.

ACCESS TO JUSTICE

"Equal justice under law is not merely a caption on the façade of the Supreme Court building, it is perhaps the most inspiring ideal of our society. It is one of the ends for which our entire legal system exists . . . it is fundamental that justice should be the same, in substance and availability, without regard to economic status."

- **Lewis Powell Jr., former Associate Justice of the United States Supreme Court.**



This Committee's 2016 report ably articulated the evidence of an access to justice gap throughout the United States and in the Commonwealth of Virginia. One of the key observations in the report states:

Research shows that legal services in civil matters for low and moderate-income persons or families are an unmet need. One study reports that 80 percent of civil legal needs of the poor and up to 60 percent of the needs of middle-income persons remain unmet.

* * *

There is no question that the need to increase legal services to these groups exists now and will continue to exist in the future.

More recently, the Legal Services Corporation (LSC) issued its 2017 Justice Gap Report, *Measuring the Civil Legal Needs of Low-income Americans*, available at www.lsc.gov/media-center/publications/2017-justice-gap-report. The report "explores the 'justice gap,' the difference between the civil legal needs of low-income Americans and the resources available to meet those needs in 2017," and includes these sobering statistics:

- In the past year, 86 percent of the civil legal problems reported by low-income Americans received inadequate or no legal help.
- 71 percent of low-income households experienced at least one civil legal problem in the last year, including problems with health care, housing conditions, disability access, veterans' benefits, and domestic violence.
- In 2017, low-income Americans will approach LSC-funded legal aid organizations for support with an estimated 1.7 million problems. They will receive only limited or no legal help for more than half of these problems due to a lack of resources.

The Commonwealth of Virginia has a total population of approximately 8.5 million people and, according to the LSC Report, approximately 15 percent of that 8.5 million — or nearly 1.3 million Virginians — are at or below 125 percent of the federal poverty level. Of these nearly 1.3 million Virginians, approximately 1.118 million receive inadequate or no help with their civil legal matters.

To date, the highest courts of 40 states and territories throughout the United States have established Access to Justice Commissions. The Conference of Chief Justices and Conference of State Court Administrators adopted a number of resolutions over the years beginning in 2004 supporting the establishment of such commissions. These commissions serve an umbrella function, involving an expanded range of key justice system stakeholders from both the public and private sectors working together to develop meaningful systemic solutions to the chronic lack of access for disadvantaged members of society.

In August 2018, the American Bar Association released a report titled *Access to Justice Commissions: Increasing Effectiveness Through Adequate Staffing and Funding*, available at www.americanbar.org/content/dam/aba/administrative/legal_aid_indigent_defendants/ls_sclaid_atj_commission_report.authcheckdam.pdf. The report's major findings and recommendations included:

- Expand the stakeholders in the A2J effort beyond the judicial and legal community to include participants from business, civic, social services, and community groups;
- Adequate and effective staffing is necessary to provide A2J Commissions with support, continuity, communications, and continued momentum;
- Leadership provided by the Conference of Chief Justices and individual Chief Justices in expanding access to justice cannot be overstated; and
- Private philanthropy through contributions from private foundations have played a key role in expanding A2J and accessing such financial support should be continued and encouraged.

In addition to these commissions, the efforts of individual lawyers are essential to closing the justice gap. Rule 6.1 of the Virginia Rules of Professional Conduct sets an aspirational goal that a minimum of two percent per year of a lawyer's professional time for pro bono work should be performed by all active members of the Virginia State Bar. The rule establishes the principle that ensuring access to justice is a key responsibility of the organized bar. Despite the urgings of Rule 6.1, it is overwhelmingly clear that Virginia lawyers as a whole are failing to close the justice gap.

In an October 2015 presentation to the VSB Council, the Virginia Access to Justice Commission reported that if all active members of the VSB met the aspirational goal of Rule 6.1, approximately 940,000 hours of legal services would be devoted to pro bono services annually. This Committee's 2016 Report, however, stated that "the best estimate based upon the data available is that Virginia lawyers are providing 80,000 hours annually." Assuming this data is close to being accurate, only 8.51 percent of the Rule 6.1 aspirational goal is being met by the active members of the Virginia State Bar.

The problem is clear, but the movement toward solutions has been difficult, and some would argue, too slow. We now turn to some of the tangible steps taken since the 2016 report was issued to begin to close the justice gap in the commonwealth.

3.1 ATTORNEY-ASSISTED PRO SE LITIGATION AND UNBUNDLED SERVICES

Recommendation 6 of the 2016 Report urged:

> "That the VSB focus on broadening access to justice through traditional programs of legal aid and pro bono work, as well as efforts to make legal services more affordable and attainable through limited-scope representation and programs to enhance assistance to pro se litigants."

The findings of the recent, groundbreaking Blue Ridge Legal Services self-represented litigants study reveal the frequency of pro se litigation in Virginia. That study of Virginia civil caseloads revealed three headline statistics: both parties have legal representation in only one percent of general district court cases, six percent of adult juvenile and domestic relations district court cases, and 38 percent of circuit court cases. The study is available at brls.org/wp-content/uploads/2018/03/Outcome-Report.pdf.

3.1.1 LIMITED SCOPE REPRESENTATION

Rule 1.2(b) of the Rules of Professional Conduct authorizes a lawyer to limit the objectives of his or her representation if the client consents after consultation. Currently, once an attorney undertakes to represent a client in a civil case, he or she is generally obligated to see the matter through to conclusion, unless allowed to withdraw by the court. One potential solution to the access to justice problem is allowing attorneys to assist pro se litigants on limited matters instead of in an entire legal case. The Supreme Court of Virginia recently amended Rule 1:5 to expressly allow limited-scope representation by legal aid attorneys by filing a notice of limited scope representation. The new rule will also permit any attorney to seek leave to provide limited representation by filing a notice identifying the particular issues or proceedings on which the attorney would provide representation.

The amended rule took effect January 1, 2019, as a "Pilot Project" until December 31, 2021, unless the court ends, modifies or extends these amended rules. It is hoped that by limiting the scope of an attorney's representation to specific issues or proceedings, there will be an increase in the number of attorneys willing to undertake representation on limited issues pending before the court in pro bono matters, and there will be a reduction in the number of pro se litigants at least with respect to certain significant issues relevant to the civil case.

3.1.2 GHOSTWRITING

Another form of limited scope representation is the preparation of motions and pleadings for a person to file as a pro se litigant. Different states have divided on whether an attorney may "ghostwrite" a pleading for a pro se litigant — specifically over whether an attorney must disclose his/her identify and the fact of their legal assistance to the court. Virginia's LEO

1874 makes plain that it is not unethical for an attorney to provide assistance to pro se litigants, and also that there is no duty to disclose this assistance to the court. As Virginia's legal opinion explains, some case decisions and ethics opinions in other states have required disclosure of the lawyer's assistance on the basis that pro se litigants may be treated more leniently and held to less stringent standards than represented parties. However, in Virginia, pro se litigants do not receive any liberal-construction benefit.

3.2 PRO BONO SERVICE REPORTING

U.S. Supreme Court Justice Sonia Sotomayor said at the 93rd annual meeting of the American Law Institute in Washington, D.C. that all lawyers should be required to provide pro bono legal representation to low income clients, insisting that law schools "don't do enough" to show young lawyers the importance of serving the needy.

In October 2016, the VSB Council narrowly opposed a proposed amendment to Rule 6.1 of the Rules of Professional Conduct offered by the Supreme Court's Access to Justice Commission mandating that every active member of the VSB report the number of hours and/or the amount of financial contributions made to legal aid societies annually. The intent of the commission's proposal "is to promote awareness of and compliance with the existing goal in Rule 6.1, improve the profession's self-governance, and minimize any calls for mandated pro bono service due to the existing lack of complete and accurate pro bono data." The proposed amendment was forwarded to the Supreme Court by the commission for its consideration.

On February 27, 2018 the Supreme Court of Virginia issued an order establishing voluntary pro bono public legal services reporting effective December 1, 2018. The court's order notes that:

> **Providing an opportunity for lawyers to voluntarily report their pro bono service on an annual basis will: (1) heighten awareness of this ethical responsibility among the bar membership by serving as an annual reminder; (2) provide a comprehensive mechanism for the bar to report and measure its collective performance vis-à-vis the aspirational goal set by Rule 6.1; (3) provide comprehensive data for the judiciary to support its efforts to promote and recognize pro bono work on a local, regional and statewide basis; (4) provide crucial benchmark data to the Virginia Access to Justice Commission to support its work promoting equal access to justice for Virginia residents; and (5) enable the bar to educate the public regarding the amount of pro bono public legal services provided by its membership to the community, thereby improving the image and standing of the profession and its membership.**

The voluntary reporting will commence with the annual renewal application process for the previous bar year running from July 1, 2018, through June 30, 2019. On the license renewal application, lawyer will have five options:

1. Note the approximate number of pro bono services hours rendered by the lawyer in the prior year;
2. Note the amount of money contributed to legal aid and similar societies as an alternative method for fulfilling the lawyer's personal Rule 6.1 responsibility;
3. State that the 2 percent goal is not applicable because the lawyer is a member of the judiciary, or a government lawyer prohibited by statute, rule, regulation, or agency policy from providing legal services outside of the lawyer's employment, or the lawyer is retired, disabled, or has an "associate" status with the VSB; or
4. State that the lawyer does not wish to report the hours of pro bono services performed nor report any financial contributions made in lieu of performing such services.

5. Lawyers can choose to associate the data they report in this section with their name and bar number so that they can be eligible for awards and recognition.

As this data is compiled, the VSB and the Access to Justice Commission will have a much clearer understanding of the contributions of Virginia lawyers to meet the aspirational goal of Rule 6.1, and, as a result, be in a better position to advise the Supreme Court on how to promote equal access to justice for Virginia residents.

3.3 AMENDMENTS TO EMERITUS RULE TO PROMOTE PRO BONO SERVICES

Effective March 1, 2018, the Supreme Court of Virginia approved changes to the rules governing emeritus membership status in the Virginia State Bar. Among other things, the amendments to Paragraph 3(e) of Part 6, Section IV of the Rules of the Supreme Court of Virginia alter the number of years an attorney must have been engaged in active practice before becoming an emeritus member, and they abolish the requirement to practice under the direct supervision of legal aid attorneys. The new amendments have already encouraged more experienced members to elect this membership status to provide pro bono legal services.

3.4 LAW FIRM ROLE IN CLOSING THE ACCESS TO JUSTICE GAP

Rule 6.1(b) of the Rules of Professional Conduct notes that a law firm or other group of lawyers may satisfy their responsibility collectively under this rule. Comment 7 of the rule specifically states:

> **Although every lawyer has an individual responsibility to provide pro bono publico services, some legal matters require the application of considerably greater effort and resources than a lawyer, acting alone, could reasonably provide on a pro bono basis. In fulfilling their obligation under this Rule, a group of two or more lawyers may pool their resources to ensure that individuals in need of such assistance, who would otherwise be unable to afford to compensate counsel, receive needed legal services. The designation of one or more lawyers to work on pro bono publico matters may be attributed to other lawyers within the firm or group who support the representation.**

Several law firms in our commonwealth have established pro bono practices as a means of providing such legal services in the name of the firm. Indeed, such pro bono practice groups within law firms provide a great service as supplemental legal aid societies. Additional law firms should be encouraged to follow the example of these trailblazing firms as an institutional contribution to closing the access to justice gap.

3.5 UTAH TO LICENSE NONLAWYERS TO PRACTICE LAW IN LIMITED CIRCUMSTANCES

Utah will become the second state to license nonlawyers to practice law in limited circumstances, similar to the limited license legal technician (LLLT) program in the state of Washington.

The Utah Supreme Court has approved a new class of legal professional called the licensed paralegal practitioner. New rules governing LPPs took effect on November 1, 2018. Court officials expect the first licensing examinations to be conducted in the spring of 2019 and the first licenses to be issued later in 2019.

In approving LPPs, the Supreme Court adopted amendments to Utah's Rule 14-802, which defines who is authorized to practice law in the state. Under the rule, LPPs will be limited to practicing in three areas of law:

- Cases involving temporary separation, divorce, parentage, cohabitant abuse, civil stalking, custody and support, and name change
- Cases involving forcible entry and detainer
- Debt collection matters in which the dollar amount in issue does not exceed the statutory limit for small claims cases

ALTERNATIVE BUSINESS STRUCTURES

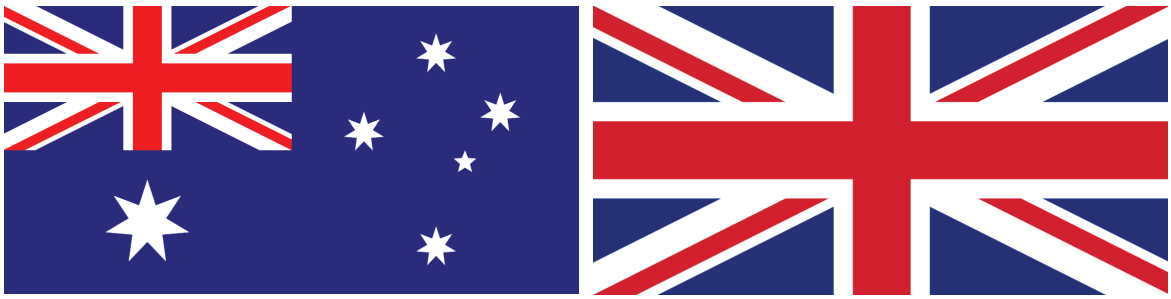
Since the issuance of its initial report in 2016, the Committee has continued to monitor activities related to and the evolving issues surrounding alternative business structures (ABS) within the United States. To date there has been no expansion beyond the adoption of Limited Licensed Legal Technicians or licensed paralegal practitioners addressed earlier.

An alternative business structure (ABS) is an entity that, while providing regulated reserved legal activities, allows nonlawyers to own or invest in law firms for the first time, opening up what has been a closed profession.

The Committee also continues to monitor activity concerning the existing programs in the United Kingdom and Australia. Proponents assert that ABS will allow nonlawyer investment in law firms enabling investment of more capital or innovation to develop software applications and new delivery systems for legal services. However, in order to significantly affect practitioners in the Commonwealth, this capital investment would need to make its way to solo practitioners and small law firms. According to a 2017 UK study, solos and small law firms do not have the same levels of access to capital. In contrast, nonlawyers legal service providers like LegalZoom and Rocket Lawyer have access to venture capital to market their services, optimize their delivery platforms, and leverage technology.

4.1 ALTERNATIVE LEGAL SERVICE PROVIDERS

Much scholarship has already been written on the innovative legal services delivery models that have emerged in this decade and how they have transformed the legal services market. In its 2016 report, the Committee identified some of the forces that have contributed to this transformation. Some commentators think the Great Recession contributed to changes in the way business looks for legal help. The rise and influence of in-house counsel is certainly another factor. And of course, technology has changed the way people and corporations seek legal help and talent. Gone are the days when businesses turned over all their legal work to a single private law firm. Commentators predict that the next decade will bring even more rapid innovation in the delivery of legal services and changes in traditional law firm structures and other law-related service delivery models.



Thus far, the subcommittee has been following the development of alternative business structures in the UK and Australia in which the service provider is a law firm but allows nonlawyer ownership and is regulated by a separate governmental authority in addition to the traditional self-regulation by the organized bar, such as the Law Society. International corporations that once turned solely to U.S. law firms now have a diverse array of professional service firms in Europe to choose from for legal and other professional services. But there are other forms of alternative legal service providers in the U.S. and around the world that bear little semblance to the traditional law firm.

A study published by ThomsonReuters and Georgetown University in 2017 reports that alternative legal service providers (ALSPs) are gaining market share in the legal services sector, while revenue and market share growth for traditional law firms have been flat now for several years in spite of the economic recovery from the Great Recession. More than 800 firms were surveyed regarding their use of ALSPs in lieu of traditional law firms. A majority of them, the report found, were using ALSPs. Initially, the use of ALSPs was predominantly for document review and discovery, but that is changing. Law firms are likely to use ALSPs for eDiscovery support services and litigation and investigation support, while corporate legal departments are using ALSPs most commonly for regulatory risk and compliance services and specialized legal services, such as requiring lawyers with expertise in a particular area.

Big accounting firms have been providing these services for decades, transforming themselves from audit firms to globally integrated business solution providers, including legal services as a component. PriceWaterhouseCoopers has launched its own law firm (ILC Legal) in Washington, D.C. to provide lawyers on demand to the accounting firm's clients. In addition to its alliance with U.S. immigration law firm Berry Appleman & Leiden, Deloitte UK will acquire the law firm's eight offices overseas, serving multinational corporations facing immigration legal issues. KPMG's Wolfers plans for its law firms to expand their foothold in Asia: "We're a specialist firm in the areas that are directly complementary with KPMG's businesses and services." Axiom provides teams of professionals including lawyers to service corporations and their law departments on discrete projects. Axiom is not a law firm. Smaller businesses are looking to ALSPs as well since they cannot maintain a corporate legal department but need legal expertise on specific matters and projects and can afford to hire a legal team on an ad hoc basis.

In a 1937 case, 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 do that. But that is exactly what is happening in the rapidly evolving legal services market. While the case is good law, market forces are running roughshod over UPL rules and doctrine.

To compete with ALSPs, traditional law firms have begun to change their partner, associate, and employee compensation schemes and client billing practices as well as acquire ownership of or form alliances with nonlawyer consulting firms and ancillary businesses that provide complementary law-related services to clients.

4.2 ETHICAL IMPLICATIONS OF NONLAWYER LEGAL SERVICE PROVIDERS

Since the 2016 report, attorney-client matching services (ACMS), Avvo, Rocket Lawyer, and LegalZoom, have continued to be embroiled in battles with various state bars and certain law firms. Despite those challenges, these ACMSs do not seem to be going away any time soon and are far from shrinking violets. Legal Zoom is a registered legal service provider in the UK and subject to considerable regulation ushered in by the Legal Services Act of 2007. In 2018, Avvo was acquired by internet Brands, a vertically focused internet company that owns, in addition to Avvo, several other legal service providers including Martindale-Hubble, Nolo.com, Total Attorneys, Ngage Live Chat, Lawyers.com and AllLaw.com.

The VSB Council approved Legal Ethics Opinion 1885, entitled "Ethical Considerations Regarding A Lawyer's Participation in An Online Attorney-Client Matching Service" by a vote of 59–6 on October 27, 2017. During its consideration of LEO 1885, VSB's Legal Ethics Committee heard from Avvo's former chief legal officer, Josh King, who also met with this Committee. The Legal Ethics Committee also considered anticompetitive and free speech implications of LEO 1885, which were ultimately found to be subordinate to the regulatory objective of preventing interference with a lawyer's independent professional judgment. Ultimately, LEO 1885 determined that a lawyer cannot participate in an attorney-client matching service under the facts presented in the opinion because such participation would violate the Rules of Professional Conduct governing fee sharing with nonlawyers, paying for referrals, and safeguarding client funds. The VSB petitioned the Supreme Court of Virginia to approve proposed LEO 1885 on November 17, 2017. On November 8, 2018, the Court approved the opinion effective immediately.

In August 2017, the New York State Bar Commission on Professional Ethics issued Ethics Opinions 1131 and 1132. In Ethics Opinion 1131, the Commission found that a lawyer could pay a for-profit service for leads to potential clients obtained via a website where the website was deemed to be an advertisement and the accompanying fee constituted a marketing fee. The Commission noted that the website provided a list of all lawyers meeting the geographic and practice area criteria based on neutral (mechanical) criteria and that the fee did not vary depending on whether the lawyer was retained or the amount the lawyer charged. The Commission also found that the website would not be "recommending" a lawyer if it made clear that (i) being included on the list only required payment and that the website did not vet the qualifications of the lawyers, (ii) the website's selection of a participating lawyer from the list was the result of a neutral process that involved no evaluative judgment, and (iii) when a lawyer was chosen by the website, it did not mean the lawyer was being referred or selected over other lawyers based on quality.

Other state bars have issued ethics opinions in agreement with Virginia. Ethics Opinion 1132 concluded that a lawyer who pays Avvo's "marketing fee" to participate violates New York's ethics rules by making an improper payment. Focusing on whether Avvo was "recommending" a lawyer on its website, the Commission noted that although a marketing fee is not per se prohibited and that a lawyer can permissibly pay a reasonable fee for advertising, Avvo's rating system and "satisfaction guaranteed" promise suggests that the marketing fee is not a mere advertisement but a payment for recommendation. The

Commission distinguished Avvo from an internet-based directory (citing Virginia Advertising Op. A-0117 (2006)) and found that "Avvo's advertising of its ratings, in combination with its statements about the high qualifications of lawyers who participate in Avvo Legal Services (ALS), constitutes a recommendation of all of the participating lawyers."

New York State Bar President Sharon Stern Gerstman commented that "those lawyers who continue to participate in Avvo's program do so at their own peril." Josh King defiantly encouraged lawyers in New York to continue to utilize Avvo's service and stated that Avvo would support any lawyer who faced disciplinary action for participating.

New York's decisions followed on the heels of New Jersey's June 21, 2017 decision to blacklist Rocket Lawyer, Avvo, and LegalZoom. Three New Jersey State Bar committees jointly considered the issue of whether it was ethical for New Jersey lawyers to participate in "certain online, nonlawyer, corporately owned services that offer legal services to the public," namely, Avvo, LegalZoom and Rocket Lawyer. The three committees answered in the negative. The committees considered the websites of the three companies in addition to their written responses. Avvo's website was found to be an impermissible referral service that violated Rules of Professional Conduct 7.2(c) and 7.3(d) as well as violated Rule 5.4(a)'s prohibition on fee sharing with nonlawyers through its use of the "marketing fee." LegalZoom and Rocket Lawyer did not suffer from those infirmities but were found to be legal service plans that were not registered with the New Jersey Supreme Court. As a result, the committees prohibited New Jersey lawyers from participating in all three services. An appeal of the three-committee opinion followed, but the New Jersey Supreme Court denied the petition.

In reaching its decision, the New Jersey State bar committees cited decisions of Ohio, South Carolina, and Pennsylvania. Ohio concluded that the "marketing fee" did not amount to a payment for advertising as Avvo suggested; instead, it was a referral fee dependent on the percentage age of the fee for providing the legal services. *See* Supreme Court of Ohio, Board of Professional Conduct, Opinion 2016-03 (June 3, 2016). The Ethics Advisory Committee of the South Carolina Bar also concluded that Avvo's per service "marketing fee" amounted to sharing legal fees with a nonlawyer that did not fall within permissible exceptions. *See* South Carolina Ethics Advisory Opinion 16-06 (July 14, 2016). The South Carolina Advisory Opinion also concluded that the lawyer's payment to the company was not payment for the cost of advertisement, but a referral fee. The Pennsylvania Bar Association, Legal Ethics and Professional Responsibility Committee Formal Opinion 2016-200 (September 2016), likewise, found that Avvo's "marketing fee" was not for the usual cost of advertising but impermissible fee sharing. In so finding, Pennsylvania noted that "[t]he cost of advertising does not vary depending on whether the advertising succeeded in bringing in business, or on the amount of revenue generated on a matter."

In California, an intellectual property firm filed an 81-page, $60 million-dollar lawsuit against LegalZoom and the bars of Texas, California, and Arizona, alleging that LegalZoom engages in the unauthorized practice of trademark law, violates California's Rules of Professional Conduct, and other state and federal anti-trust and anti-competition laws. The complaint in *LegalForce RAPC Worldwide, P.C. v. LegalZoom.Com, Inc.*, 5:17-cv-07194-NC (N.D. Cal. Dec. 19, 2017), alleges among other things, that LegalZoom has an unfair advantage over Legal Force because the latter as a law firm must abide by the various ethics rules and client protections necessitated by being a law firm employing lawyers, while LegalZoom claims it is not a law firm nor does it provide legal services.

Amidst this opposition against the likes of Avvo, LegalZoom, and Rocket Lawyer, some insist that such efforts to resist change are pointless or counterproductive, and that if state bars are really concerned with issues related to public protection, and access to justice, they will ultimately need to relax restrictions. For instance, in its June 2017 report entitled, *The Future of Legal Services in Oregon, Executive Summary* and available at www.osbar.org/_docs/resources/taskforces/futures/futurestf_summary.pdf, the Oregon State Bar Futures Task Force listed certain recommendations to revise the rules of professional conduct to remove barriers to innovation. Among the task force's recommendations were one to "amend

current fee-sharing rules to allow fee sharing between lawyers and lawyer referral services, with appropriate disclosure to clients." Contrary to the current practice of limiting market competition by for-profit players, the Oregon Futures Task Force proposes amending Oregon's rules to allow fee sharing between any referral service and lawyers, so long as there is adequate price disclosure to the client and the clients are not charged a clearly excessive fee.

Similarly, on May 30, 2018, the Illinois Attorney Registration and Disciplinary Commission issued a report for public comment recommending rule changes that would allow lawyers in Illinois to participate in and share legal fees with for-profit lawyer referral services and ACMSs subject to certain client protection requirements and registration with that lawyer regulatory agency. The Commission revised this report on June 25, 2018, and the 126-page report may be found at www.iardc.org/Matching_Services_Study_Release_for_Comments.pdf. The report covers extensively all the issues that have been discussed concerning lawyer participation in ACMS and criticizes the organized bar's resistance to change. What is remarkable about the report is that its call for change comes from a lawyer regulatory agency. In its report, the IARDC states: "Prohibiting lawyers from participating in or sharing fees with for-profit services that refer clients to or match clients with participating lawyers is not a viable approach, because the prohibition would perpetuate the lack of access to the legal marketplace." At this point the report is merely a proposal, and public comment is invited.

Following litigation between the North Carolina Bar and LegalZoom, which resulted in a settlement and an October 25, 2015 consent order that allowed LegalZoom to operate in the state under certain conditions, the North Carolina State Bar Council issued Proposed 2017 Formal Ethics Opinion 6, entitled Participation in Online Platform Finding and Employing a Lawyer (July 27, 2017). Proposed Formal Ethics Opinion 6 would allow lawyers to participate in Avvo Legal Services as well as similar online platforms marketing legal services under a number of conditions. The Ethics Committee of the North Carolina Bar voted at its January 2018 meeting to return the proposed ethics opinion to a subcommittee for additional study.

On June 6, 2018, after facing extensive opposition expressed in state bar ethics opinions, the general counsel for internet Brands, the parent company that now owns Avvo, informed the North Carolina State Bar's Unauthorized Practice of Law Committee that Avvo Legal Services would be discontinued by the end of July 2018. In that letter, General Counsel Lynn Walsh told the UPL Committee that it would not be necessary to issue a UPL opinion, but also explained that Avvo Legal Services was never engaged in UPL because a licensed attorney selected by the client worked independently with the client in performing the fixed fee limited scope services.

In July 2018, the California State Bar approved the creation of a task force to consider whether regulatory changes should be made to support online legal service delivery models including nonlawyer ownership of entities delivering legal services with a special focus on enhancing access to justice. The bar commissioned Law Professor William D. Henderson, well-known legal industry expert and surveyor of innovation in the delivery of legal services. In his July 2018 *Legal Market Landscape Report*, Henderson writes:

> **The legal profession is at an inflection point. Solving the problem of lagging legal productivity requires lawyers to work closely with professionals from other disciplines. Unfortunately, the ethics rules hinder this type of collaboration. To the extent these rules promote consumer protection, they do so only for the minority of citizens who can afford legal services.**

Professor Henderson further notes:

> **The law should not be regulated to protect the 10 percent of consumers who can afford legal services while ignoring the 90 percent who lack the ability to pay. This is too big a gap to fill through a renewed commitment to pro bono. This is a structural problem rooted in lagging legal productivity that requires changes in how the market is regulated.**

Dr. Henderson asserts that "modifying the ethics rules to facilitate greater collaboration across law and other disciplines will (1) drive down costs; (2) improve access; (3) increase predictability and transparency of legal services; (4) aid the growth of new businesses; and (5) elevate the reputation of the legal profession." However, he provides no empirical evidence to substantiate this assertion. And that lack of evidence is what results in the hesitancy of lawyers and bar associations to support the changes he recommends.

The landscape of ACMS is thus currently uncertain and varied. The American Bar Association Commission on the Future of Legal Services issued a *Report on the Future of Legal Services in the United States* in August 2016. The Commission encouraged states to be circumspect in issuing new regulations and rules to Legal Service Providers (LSPs), acknowledging that regulation can often dissuade LSPs from using technology to provide greater access to legal services. Instead, the Commission suggested that states study the LSPs operating in their jurisdictions, collect data on their benefits and harm and determine whether current law provides adequate safeguards against harm before adopting new rules and procedures for LSPs.

ATTORNEY WELL-BEING

In 2016, the American Bar Association (ABA) Commission on Lawyer Assistance Programs and the Hazelden Betty Ford Foundation published a study of nearly 13,000 currently-practicing lawyers. That study found that between 21 percent and 36 percent qualify as problem drinkers, and that approximately 28 percent, 19 percent, and 23 percent are struggling with some level of depression, anxiety, and stress, respectively. This study, and others like it, sent shock waves through the American legal community. As a result, numerous initiatives addressing attorney well-being sprang to life.

5.1 REPORT OF THE NATIONAL TASK FORCE ON LAWYER WELL-BEING

Studies of lawyer well-being were the impetus for the creation of a 17-member National Task Force by the ABA, the Conference of Chief Justices, and other entities. Virginia's chief justice, Donald Lemons, was one of two judges selected to serve on the task force. In August 2017, the task force published its report entitled *The Path to Lawyer Well-being: Practical Recommendations for Positive Change*, which can be found at www.americanbar.org/content/dam/aba/images/abanews/ThePathToLawyerWellBeingReportRevFINAL.pdf ("National Task Force Report"). The report identified seven different stake holders: judges, regulators, legal employers, law schools, bar associations, professional liability carriers, and lawyer assistance programs. The report further identified various ideas which each of those stakeholders should consider adopting to address lawyer well-being. In all, the report offers at least 44 different recommendations. Among the recommendations are the following:

1. Acknowledge the problems that exist and take responsibility;
2. Use the Report as a launch pad for a profession-wide action plan;
3. Encourage leaders to demonstrate a personal commitment to well-being;
4. Facilitate, destigmatize, and encourage help-seeking behaviors;
5. Build relationships with lawyer well-being experts;
6. Foster collegiality and respectful engagement throughout the profession;
7. Enhance lawyers' sense of control;
8. Provide high-quality educational programs about lawyer distress and well-being;
9. Guide and support the transition of older lawyers;
10. De-emphasize alcohol at social events;
11. Utilize monitoring to support recovery from substance use disorders;
12. Begin a dialogue about suicide prevention; and
13. Support a lawyer well-being index to measure the profession's progress.

In summary, the report was a clarion call to the profession for critical self-examination. Because of the importance of the topic, and the fact that our own chief justice was a co-author of the report, Virginia has already initiated numerous changes to help promote attorney well-being.

5.2 REPORT OF THE COMMITTEE ON LAWYER WELL-BEING OF THE SUPREME COURT OF VIRGINIA

Motivated by the National Task Force Report, Chief Justice Lemons appointed a group of judges, bar leaders, prominent attorneys, and law school deans to study attorney wellness issues in the Commonwealth of Virginia. Chaired by Justice William Mims, the committee published its own report entitled *A Profession at Risk: Report of the Committee on Lawyer Well-Being of the Supreme Court of Virginia*, which is available at www.vsb.org/docs/A_Profession_At_Risk_Report.pdf. At the heart of this report was a recommendation that Virginia's lawyer assistance program, Lawyers Helping Lawyers (LHL), have a permanent, reliable, and adequate funding source paid from bar dues of Virginia's lawyers. The report further recommended that LHL serve as the state's designated judge/lawyer assistance program (JLAP). Further, the JLAP should serve not only the needs of Virginia's judges and lawyers, but also Virginia's law students, particularly given the fact that recent studies revealed that wellness issues arise as early as the second year of law school.

The increased dues expense will be offset by an additional recommendation that the Educational Services Department of the Office of the Executive Secretary (OES), in conjunction with Virginia CLE and other state agencies, develop online professional health initiative programs in 30-minute and one-hour modules that will qualify for MCLE credit and be available to Virginia lawyers free of charge. In effect, multiple MCLE opportunities addressing health and well-being will be made available for the relatively low increase in annual dues.

Two additional recommendations from the report are noteworthy. First, the committee recommended the appointment of an advisory board to advise OES regarding all aspects of the comprehensive well-being initiatives in Virginia. This will be a multi-disciplinary advisory board composed of volunteer members, including representatives from LHL. Moreover, the MCLE Rule of Court will soon be amended to require lawyers to disclose on their MCLE forms whether they have taken at least one hour of professional health initiatives education or training within the past three years. This is a voluntary reporting requirement for now. However, the message is clear: lawyers must seek education on lawyer well-being issues in order for our profession to address the wellness crisis.

5.3 VSB PRESIDENT'S SPECIAL COMMITTEE ON LAWYER WELL-BEING

Also, in response to the National Task Force Report, VSB President Leonard C. Heath Jr. convened the President's Special Committee on Lawyer Well-Being, which is currently examining the specific risks that can adversely affect lawyer well-being. The committee plans to issue its report in Spring 2019. The report will identify each individual risk, describe the nature of the risk, provide resource links so others can become educated on each specific risk, and provide practice pointers for individuals and law firms. At this point, no other organization has commissioned a similar report. The goal of the president's Special Committee is twofold. First, the committee's report will provide a resource for judges, lawyers, and law students on the specific risks involved in the practice of law. The second goal is to prompt further discussion and study by others on the specific risks in the profession.

5.4 OTHER CHANGES WITHIN THE VIRGINIA STATE BAR

The Virginia State Bar has initiated a number of changes in response to the attorney well-being initiative. The following are just a few examples. First, Rule 1.1 of Virginia's Rules of Professional Conduct has been amended, adding a new comment 7, which calls attention to the fact that maintaining well-being is an aspect of maintaining competence to represent clients. Second, Virginia's disciplinary process has been modified to facilitate retirement for a lawyer suffering from a permanent impairment, such as an irreversible cognitive decline, by allowing retirement with dignity instead of having the lawyer's license suspended on impairment grounds. Third, the disciplinary process has also been modified so that when information of possible mental health or substance abuse issues is discovered during investigation or prosecution of lawyer regulation matters, confidentiality rules will now allow sharing of such information with lawyer assistance programs.

Referencing the National Task Force Report, Virginia's Mandatory Continuing Legal Education Board has modified and expanded its Opinion 19 dealing with attorney well-being issues. While the opinion only reinforces past practices of the board, the opinion is now designed to make it abundantly clear that attorney well-being topics will be granted CLE credit, so long as other requirements of the MCLE process are satisfied.

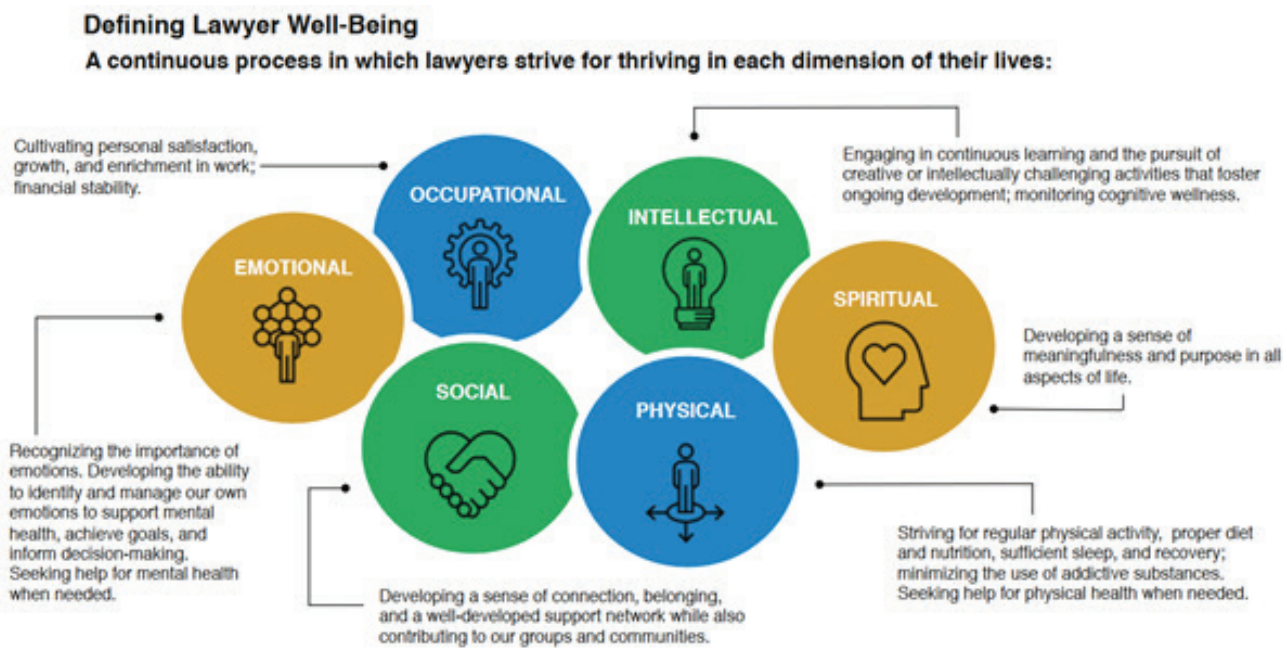
Predating the National Task Force Report, in April 2017, the Virginia State Bar Young Lawyers Conference (YLC) established its Wellness Initiative, which focuses on raising awareness of lawyer well-being, compiling and providing related resources to its members, and working to eliminate the stigma associated with mental health and substance abuse. The YLC was already working on wellness issues because previous literature noted that substance abuse and untreated mental health issues were more significant with law students and lawyers in their first years of practice.

Finally, members of the Supreme Court of Virginia, the Virginia State Bar president, and numerous members of the Virginia State Bar Council have spoken both locally and nationally on attorney well-being issues. Uniformly, the leadership of our legal community believes that education and understanding is a major component of addressing the wellness crises.

The wellness initiative can best be summarized by the first two paragraphs of the Supreme Court Committee Report:

> **The well-being of lawyers, judges and law students in Virginia is integral to professional competence. A competent bench and bar in Virginia is essential to ensuring the protection of the public we serve.**
>
> **As members of a self-regulated profession, we are devoted to client protection as a fundamental duty. To achieve this, the legal profession must support education and training that will ensure professional competency. Further, the legal profession as a whole must provide the resources necessary to ensure intervention, assessment, and referral services for at-risk and impaired lawyers, judges, and law students.**

The leadership of the Virginia State Bar stands in full support of the wellness initiative.



From the Path to Lawyer Well-Being Report, Page 9. The graphic looks at all aspects of a human being's needs in order to feel healthy and fulfilled.

RECOMMENDATIONS

The Committee makes the following recommendations:

1. That the Virginia State Bar Standing Committee on Legal Ethics further study Rules 5.4(a) and 7.3(d) of the Virginia Rules of Professional Conduct, as applied to Attorney Client Matching Services (ACMS), for-profit lawyer referral services, and other arrangements online where legal fees may be shared with nonlawyers; consider whether to recommend any relaxation of the prohibition on lawyers paying a fee to a nonlawyer company for client referrals or development; and provide further guidance to lawyers regarding participating in for-profit lead generation, client-matching, and lawyer referral services.

2. That the Virginia State Bar promote the availability of legal technology education, especially focusing on cybersecurity and data privacy, striving to ensure that such education is available to Virginia lawyers through the Solo and Small Firm Conference, events such as the TECHSHOW and the VSB annual meeting, and conferences/seminars developed by VSB committees and VACLE. Further, that the VSB explore presenting webinars on this topic, enabling those who live in all regions of the state to attend quality programming.

3. That the *Virginia Lawyer* and other VSB publications regularly feature articles on the changing future of law practice.

4. That the VSB's Mandatory Continuing Legal Education Board consider exercising its discretion in favor of approving CLE courses that focus on law practice management topics and firm management, and CLE courses that focus on lawyer well-being, provided their primary objective is to increase the attendee's professional competence and skills as an attorney and improve the quality of legal services rendered to the public, and promote the attendee's compliance with the Virginia Rules of Professional Conduct. Appropriate practice management promotes the efficient, ethical and competent practice of law. This includes subjects such as technology, case management, ethical marketing, and accounting. See MCLE Regulation 103(b) and MCLE Op. 17.

5. That Virginia's law schools comprehensively teach legal technology. Such teaching should encompass case management, time and billing, collaboration, document assembly, and artificial intelligence to speed the lawyer's ability to perform routine and complex tasks and make legal services more accessible. The teaching should also include cybersecurity, including the use of cloud computing, encryption, multi-factor authentication, the secure use of wireless networks, the proper configuration of backups and disaster recovery. The teaching should also include laws governing the privacy of personal data. The Virginia Rules of Professional Conduct impose an ethical duty that lawyers understand and are competent with law office technology including securing confidential data. This ethical duty, and how to abide by it, should be an integral part of law school education.

6. That the profession should support and take advantage of the actions taken by the Supreme Court of Virginia allowing lawyers to enter limited appearances in civil proceedings. This rule change should make legal services more affordable and attainable through limited-scope representation and programs to enhance assistance to pro se litigants. Bar associations and attorneys should create programs with legal aid and pro bono programs to broaden access to justice.

7. That this Committee continue to study the evolving issues surrounding alternative business structures.

8. That all entities incorporate wellness initiatives into their workplace, membership, and/or court policies.

9. That the profession creates and fosters a culture that promotes well-being of judges, lawyers, and their staffs.

10. That all entities support Lawyers Helping Lawyers.

SUBMITTED BY

Respectfully submitted,

The Special Committee on the Future of Law Practice
March 13, 2019

Sharon D. Nelson, Chair
Kellam T. Parks, Vice-Chair
Graham K. Bryant
Brian L. Buniva
Marni E. Byrum
Doris H. Causey
Darius K. A. Davenport, Sr.
Karl A. Doss
Teirra M. Everette
Christopher R. Fortier
Jonathan Vincent Gallo
Leonard C. Heath, Jr.
Christy E. Kiely
Lisa Marie Lorish
Jamie Baskerville Martin
Kevin E. Martingayle
David B. Neumeyer
Mary C. Zinsner

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