University of Miami Business Law Review

Volume 30 | Issue 2 Article 5

The Increased Use and Permanency of Technology: How Those Changes Impact Attorneys' Professional Responsibility and Ethical Obligations to Clients and Recommendations for Improvement

Scott B. Piekarsky

The Increased Use and Permanency of Technology: How Those Changes Impact Attorneys' Professional Responsibility and Ethical Obligations to Clients and Recommendations for Improvement

Scott B. Piekarsky

I. INTRODUCTION

We are now over one year into the COVID–19 worldwide pandemic, and it is abundantly clear that the resulting increased use of technology will be permanent.[1] With that in mind, we must consider how this will impact attorneys' professional and ethical obligations to clients moving forward. We also must understand the available and emerging technologies and their associated risks. A full and proper analysis should examine what has occurred and been experienced over the past year and how this will help us in planning and protecting for the future.

Most of us have spent all or a good part of the past year or more working from home or a second home and not from actual physical offices. Since we cannot walk out our office doors or down the hall to communicate a thought or idea to staff or a colleague, we are necessarily spending more time emailing, texting, phone calling, video calling, etc. The use of technology has greatly increased and therefore the liability and ethical risks associated with the use of technology are also greatly increased. Banter within the legal community suggests that even after the

[1] Scott B. Piekarsky, *Ethical Issues and Best Practices While Working Remotely During the COVID–19 Pandemic*, 56 RUTGERS BUS L.J. 1 (2020).

pandemic, Zoom and Teams events will continue and become a permanent part of the legal work landscape. Not only do we save time, money and energy wasted on long drives to courthouses and closings, the increased use of technology is also good for the environment where global warming may be our next environmental emergency.

There is also a certain isolation risk of remote work that does not necessarily occur in a multi–person office setting. Some have suggested that more mistakes and unethical conduct and perhaps dishonesty occurs when we are stuck at home without staff and colleagues around to assist us or interact with us.[2] Some writers feel that this calls for a heightened awareness and need to focus on attorney wellness more than ever before.[3]

This writer believes that there is going to be a greater need for physical and social support to remote workers. The use of on–site physical support and regular virtual platforms that replicate the prior office experience will be necessary if better socialization does not occur soon. In this article we will explore the technologies, challenges, risks and ways to mitigate those risks while we enter this new frontier of remote professional work like we have never seen before.

Much like everyone, tired from article after article and seminar after seminar on attorney ethics and social media, I trust readers are tiring of reading about the pandemic, how it has affected or effected remote work and remote, technological, ethical and liability risks. However, after some brief and necessary background, it would be beneficial to review the many available and evolving technologies and protective steps lawyers and professional organizations will need to take.

The American Bar Association ("ABA") has done a wonderful job detailing and cataloging the relevant legal and practice issues both before and after the start of the current COVID–19 Pandemic that started in 2020, focusing on the use of technology and remote work. Their work provides us with a helpful framework to this introductory material.

Going back about four years pre–COVID–19, the ABA gave us Formal Opinion 477R entitled "Securing Communication of Protected Client Information."[4] Its introduction section gives us a nice walk down memory lane of the onset of electronic communications, email risks, use of the internet and the "technology amendments" to the Model Rules of

---

2 Debra Cassens Weiss, *Pandemic and financial stress could push some lawyers to act unethically, experts warn*, ABA JOURNAL (February 26, 2021, 12:01 PM), https: //www.abajournal.com/news/article/pandemic–and–financial–stress–can–push–lawyers–to–act–unethically–some–experts–warn.

3 *Analysis: Lawyer Well–Being Critical During Pandemic*, BLOOMBERG LAW (Mar. 25, 2020, 03:41 PM), https://news.bloomberglaw.com/bloomberg–law–analysis/analysis–lawyer–well–being–critical–during–pandemic.

4 ABA Standing Comm. on Ethics & Pro. Resp., Formal Op. 477R (2017).

Professional Conduct. It spoke to the Duty of Competence, the Duty of Confidentiality, cyber threats, protecting clients and vetting vendors of products and services. This opinion warned of client lack of sophistication. We have made substantial advances since that time both as lawyers and clients. However, the requirements and the risks remain unchanged.

In the Fall of 2018 came Formal Opinion 482 on Ethical Obligations Related to Disasters.[5] While our then experience with hurricanes, floods, tornados and fires certainly prompted the opinion, we still were not prescient as lawyers of a possible pandemic. Nonetheless, many of the issues necessary for physical natural disaster discussions are relevant to a pandemic. Seems like the difference is that the pandemic is much longer and perhaps not as physically devastating to files, computer systems, data and the like. They all keep us remote, but it appears that the ethical and liability risks and lessons are the same. The opinion spoke to communications, dealing with the physical impediments, withdrawal as counsel, lawyers displaced to other jurisdictions, loss of files and client property, and solicitation and advertisement.

The next relevant Formal Opinion is Formal Opinion 483 entitled "Lawyer's Obligations After an Electronic Data Breach or Cyber Attack," also released in the Fall of 2018.[6] While there was a clear risk in 2018, it now seems to still be present and perhaps at an increased level which will be discussed. Such breaches involve the most important and coveted duties for attorney, such as the duty of confidentiality and the duty to safeguard client property. Overarching this and other duties that counsel may have is the Duty of Competence which appears to be quickly increasing in scope and has been perhaps accelerated by the current pandemic and our changed and still changing world.

The next timely and important ABA Formal Opinion issued in December of 2020 was Formal Opinion Number 495 entitled Lawyers Working Remotely.[7] In an already mobile world with laptops, tablets and smart phones, even pre–pandemic, it seemed totally appropriate to give our local clients advice while we were travelling, on vacation or at a second home. Whether it is arcane or outdated laws or the risk of lawyers spreading their advice at a distant place where not licensed, it was determined that a related opinion was necessary. In essence, the opinion says that it is okay to do your work while at a different jurisdictional location so long as not prohibited by local law and not hanging out a local shingle, so to speak. Some jurisdictions might consider such a practice the

---

5 ABA Standing Comm. on Ethics & Pro. Resp., Formal Op. 482 (2018).

6 ABA Standing Comm. on Ethics & Prof'l Resp., Formal Op. 483 (2018).

7 ABA Standing Comm. on Ethics & Pro. Resp., Formal Op. 495 (2020).

unauthorized practice of law, which no lawyer wants to be charged with, as it is essentially a criminal or quasi criminal offense.

This now brings us to the most recent and comprehensive of the ABA opinions, Formal Opinion 498 entitled Virtual Practice issued on March 10, 2021.[8] The ABA defines virtual practice as a "technologically enabled law practice beyond the traditional brick and mortar law firm". To first summarize the opinion, the ABA speaks to competence, diligence, communication, confidentiality, inadvertent disclosures and supervision of others. The opinion notes that the comments suggest best practices and certainly we must all look to local laws, and local rules of Professional Conduct as they can vary from state to state.

The beauty of the rules of professional conduct is that they can be applied to many new and changing factual and technological issues as we saw years ago with the commencement of the use of social media. While Rules of Professional Conduct and Formal Opinions are not necessarily standards of practice for liability reasons, they give us a framework, a focus, and bases upon which standards of practice will likely form.

Continuing through Formal Opinion 498 is a good discussion guide for this article. Probably use of the key Rule of Professional Conduct getting the most attention and rightly so is MRPC 1.1 on Competence. In 2012, the ABA's House of Delegates voted to amend comment 8 to Model Rule 1.1 to include a technology requirement which reads as follows:

II. MAINTAINING COMPETENCE

"To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, <u>including the benefits and risks associated with relevant technology</u>, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.[9]" Interestingly, not every state has adopted this requirement. On March 24, 2021, Bob Ambrogi reported that California became the 39th state to adopt the duty of technology competence.[10] Such lawyer saturated and sophisticated jurisdictions like New Jersey and the District of Columbia have not yet adopted this requirement but this writer expects that should soon change. The ABA advises that "lawyers should have plans in place to ensure responsibilities

---

8 ABA Standing Comm. on Ethics & Pro. Resp., Formal Op. 498 (2021).

9 MODEL RULES OF PRO. CONDUCT r. 1.1 cmt. 8 (AM. BAR ASS'N 2020) (emphasis added).

10 Bob Ambrogi, *California Becomes 39th State to Adopt Duty of Technology Competence*, LAWSITES (Mar. 24, 2021), https://www.lawsitesblog.com/2021/03/california–becomes–39th–state–to–adopt–duty–of–technology–competence.html.

regarding competence, diligence and communication are being fulfilled when practicing virtually."[11] It is further suggested that if these responsibilities cannot be met, the lawyer must withdraw.[12] We will examine a whole host of technologies and the challenges they present.

Confidentiality, a hallmark of the attorney client relationship is then focused upon by the ABA. This key responsibility becomes so challenging when we are 1) not working in our office and 2) relying significantly on remote technology. We cannot be having confidential client discussions while at a remote location with other people present. In participating in scores of virtual remote matters, it is obvious that many lawyers do not have private remote workspaces. This will be an ever–increasing challenge that will need to be addressed by firms and entities and that should be documented in remote work policies and procedures.

Next is the topic of supervision. This is an incredibly difficult requirement to meet in light of the new normal. Many lawyers are working remotely and so are their subordinate lawyers and non–lawyer assistants. How do you effectively and efficiently supervise when you cannot see what your subordinates are doing? Yes, you can have weekly or daily zoom calls but how do you know they are working and doing so in a confidential setting? This is an area sorely in need of improvement, perhaps through the use of remote work software where one can actually have a virtual office to stop in on a subordinate unannounced at any time. Isn't that something we were doing in early 2020 when we were working in our physical offices? Some non–lawyers report that employers are requiring them to be present 09:00 A.M. to 05:00 P.M. on a virtual platform like Zoom or Teams.

Let's now address the core of this article, which are the technologies and the challenges they pose. Formal Opinion 498 speaks to "Particular Virtual Practice Technologies and Considerations".[13] This can be overwhelming to the solo practitioner, the novice, or the long–term practitioner who did not grow up using these technologies. We know we must use the internet. That brings with it a host of not–so–new challenges. For example, secure internet portals like Citrix, Virtual Private Networks (VPN's), complex and regular changing passwords, use of double authentication modes like DUO, firewalls, anti–malware/spyware/virus software, use of patches and updates, back up storage of data and keeping Alexa out of the room which this author has written about recently at length.[14]

---

11 *See* ABA STANDING COMM. ON ETHICS & PRO. RESP., *supra* note 8, at 2.

12 *Id.*

13 *See* ABA STANDING COMM. ON ETHICS & PRO. RESP., *supra* note 8, at 4.

14 *See* Piekarsky, *supra* note 1, at 4 (citing PA. BAR ASS'N COMM. ON LEGAL ETHICS AND PRO. RESP., Formal Op. 2020–300 (2020)).

Next, as to Hardware and Software systems, have you reviewed the terms of service, and will they maintain and protect confidentiality? As the Formal Opinion notes, "some terms and conditions of service may include provisions for data–soaking software systems that collect, track and use information."[15] They may also purport to own the information and reserve the right to sell or transfer it to third parties or otherwise use it contrary to a lawyer's duty of confidentiality. This is obviously problematic and unacceptable. Someone on the team or staff must vet this issue.

Next is access to client files and data. A reliable cloud service should be acceptable so long as steps are taken to ensure confidentiality and ready accessibility. But backing up data and securing it are necessary steps in case of data loss. Also, with a loss or hacking, lawyers must have a data breach policy and a plan and protocol for communicating the same to clients. Some states also have adopted comprehensive data privacy and security programs to protect personal information.

Virtual meeting platforms and video conferencing are the biggest and newest change for remote lawyering. Again, reviewing terms of service to ensure ethical obligations are met is critical. Strong passwords and tight security are essential. Clients also need to know if and when such sessions will be recorded. Also, warning staff and clients about prohibitions by courts on private recording is essential. The Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility on the forefront once again promulgated Formal Opinion 2020–300 (2020), setting forth many best practices for videoconferencing security including not making meetings public, requiring a meeting password, not sharing links publicly, providing links directly to specific people, managing screensharing and other options and using updated versions.[16] Perhaps needless to say to those with lots of regular use, be prepared for power outages, internet outages and potential sources of inside and outside noise and interference. This writer was compelled to purchase a jet–pack (i.e., portable independent internet server) and luckily had an emergency backup generator for the hurricane season strike in the midst of a remote hearing during 2020.

As to virtual document and data exchange platforms, again reviewing terms of service is critical to make sure you are complying with ethical mandates and requirements. Is the platform secure, and is it storing for later retrieval securely? Is encryption being utilized, and is it necessary or required?

---

15 *See* ABA STANDING COMM. ON ETHICS & PRO. RESP., *supra* note 8, at 4 n.17.

16 PA BAR ASS'N COMM. ON LEGAL ETHICS AND PROF. RESP., Formal Op. 2020–300 (2020).

What emerges from this review and analysis is an absolute need to educate and communicate to lawyers and non–lawyer assistants and create policies and procedures within your firm or legal department. This will also help protect you and your firm in the event of a liability suit, ethics grievance or governmental action.

This is a good point to examine some newer and emerging technologies and some ways to ensure that you are satisfying your legal and ethical duties.

III. ARTIFICIAL INTELLIGENCE (AI)

Let's examine the ever evolving and wide–spread use of AI or Artificial Intelligence. This refers to any human–like intelligence exhibited by a computer, robot or other machine.[17] It often refers to the ability of a computer or machine to mimic the capabilities of the human mind, learning from examples and experience, recognizing objects, understanding and responding to language, making decisions, solving problems and combining these and other capabilities to perform functions a human might perform. So what part is AI playing in the practice of law? Well, it is being used in the areas of e–discovery, legal research, document management, contract and litigation analytics, predictive analytics, etc.[18]

E–discovery was the first use of AI in the practice of law, and it is well grounded.[19] It allows software to review voluminous documents relevant to a search criteria in rapid time at minimal expense. It is also quite accurate. In legal research, large well–known companies utilize large databases allowing attorneys to do rapid searches relatively inexpensively and accurately. Some platforms allow for the answering of questions versus just utilizing search terms.[20] With document management, special software allows for the management of voluminous like documents for consistency and enforcement.[21] In the area of contract and litigation analytics, it allows attorneys to draft consistent, current documents for transactions and litigation by utilizing large databases of historical documents.[22]

---

17 B.J. Copeland, *Artificial Intelligence*, ENCYC. BRITANNICA, https://www.britannica.com/technology/artificial–intelligence (last visited Aug. 11, 2020).

18 Anthony E. Davis, *The Future of Law Firms (and Lawyers) in the Age of Artificial Intelligence*, ABA (Oct. 2, 2020), https://www.americanbar.org/groups/professionalresponsibility/publications/professionallawyer/27/1/the–future–law–firms–and–lawyers–the–age–artificial–intelligence/.

19 *Id.*

20 *Id.*

21 *Id.*

22 *Id.*

With predictive analytics, decisions can be analyzed by plugging in the legal issues and factors like the judge handling the mater to elicit a prediction of likely outcomes.[23] Other analytics can review an item of legal research or a legal submission to a court to identify precedents missing from the research or submission. Unfortunately, AI has posed many potential biases and vulnerability to manipulation. At a very basic level, the same can lead to wrongful arrests or qualified applicants being rejected for jobs or loans. Because of its growth, wide use and inherent risks, The National Institute of Standards and Technology (NIST) is advancing an approach for identifying and managing biases on a national level.[24] One area of law related to AI that is receiving widespread media and legislative attention is the area of facial recognition software. In 2020, there was a widely reported case in New Jersey about a man who spent ten (10) days in jail after facial recognition software led to the arrest of the wrong man.[25] The New Jersey attorney general announced a moratorium on the use of facial recognition products in law enforcement until the Division of Criminal Justice evaluated them and developed a policy governing their use.[26] On the national level, the NIST periodically tests the accuracy of facial recognition algorithms voluntarily submitted by vendors.[27]

Just published in 2021 is a very informative book for lawyers in this realm entitled *AI For Lawyers* by Noah Weisberg and Dr. Alexander Hudek.[28] The authors take a deep dive into this discipline and the related ethical challenges. Head on, they discuss the issue of bias and solutions to the same.[29] They say the first step is to test for bias.[30] As one example, they use the rate of recidivism and testing it by changing the skin color or gender of an individual and then looking at whether the prediction changes.[31] Much has been written about the known bias with AI algorithms

---

23 *Id.*

24 *See* Nat'l Institute of Standards and Technology ("NIST*"), NIST Proposes Approach for Reducing Risk of Bias in Artificial Intelligence*, NIST, June 22, 2021, https://www.nist.gov/news–events/news/2021/06/nist–proposes–approach–reducing–risk–bias–artificial–intelligence.

25 *See* Anthony G. Attrino, *He spent ten (10) days in Jail After Facial Recognition Software Led to the Arrest of the Wrong Man, Lawsuit Says*, NJ.com, Dec. 29, 2020, https://www.nj.com/middlesex/2020/12/he–spent–10–days–in–jail–after–facial–recognition–software–led–to–the–arrest–of–the–wrong–man–lawsuit–says.html.

26 *Id.*

27 Kashmir Hill, *Your Face Is Not Your Own*, N.Y. TIMES MAGAZINE, Mar. 21, 2021, at Page 8. https://www.nytimes.com/interactive/2021/03/18/magazine/facial–recognition–clearview–ai.html.

28 *See* Noah Waisberg and Dr. Alexander Hudek, *AI For Lawyers*, Wiley (2021).

29 *Id.* at 89.

30 *Id.*

31 *Id.*

when dealing with race. The authors claim by doing this on a large enough number of individuals will determine if the model is biased.[32]

They speak to another common technique of modifying training data. Like with recidivism rates, you can make sure people of all skin colors are equally represented.[33]

Finally, they cite to Norm Judah, a former chief technology officer at Microsoft. His idea was to simply make sure your data science team is diverse.[34] Such a team will be more likely to think about and locate bias issues. Diverse teams often generate better solutions. What a great endorsement and compelling example as to why in 2021 we must finally promote and insure Diversity, Equity and Inclusion. As officers of the court and society members who swear to defend the Constitution, there is good reason why diversity, equity and inclusion are sorely needed. The following is one great example.

We now must face the new or existential reality that it is a changed world forever, technology will advance geometrically, and we must face the challenge. We need to understand new technologies, make sure they fit the attorney/client model, and legally and ethically are compliant to well–established legal and ethical norms. In addition, but not to be trite, we need to think outside the box. Meaning, how will bad actors use the new technologies in bad and nefarious ways? It reminds this author of a prior CLE course he has given about dealing with the Rambo or Scorched earth litigator. This is coursework for litigators designed to make ethical litigators to think like non–ethical litigators to cut them off at the pass. The same is true here in that we have wonderful new technologies which when put in the wrong hands can wreak havoc. For example, in the area of real estate transactions for many years now we have dealt with bad actors coopting wire information and having parties to transactions send the wires to the wrong recipients (i.e., criminals, often continents away and usually never reachable).[35] That is an old and elementary criminal concept. Now, with developments such as deepfakes, one can imitate voices and likenesses to make you believe you are dealing with the actual person versus their clone or fake. Apparently, the term "deepfake" was first used in late 2017 when someone on the online forum Reddit started posting

---

32 *Id.*

33 *Id.*

34 *Id.*

35 *See* Michael Lerner, *Take These Steps to Prevent Wire Fraud During a Real Estate Transaction*, THE WASHINGTON POST, Jan. 5, 2021, https://www.washingtonpost.com/business/2021/01/05/take–these–steps–prevent–wire–fraud–during–real–estate–transaction/.

doctored celebrity videos utilizing that label.[36] "Deep" refers to deep learning, an AI method that involves training a neural network to create fabrications based on existing recordings and images of a person.[37] Websites and apps now exist that allow anyone to make use of this emerging abuse of technology. For example, ZAO is one of the newest apps that allows you to create a deepfake video within seconds.[38] It has a library of video clips where one can be plugged into a Hollywood movie or popular television program within a few seconds. A little bit more sophisticated and challenging is DeepFaceLab, which can replace faces in videos.[39] An earlier spoof telephone misuse of phone and cellular technology has allowed bad actors or jokesters to spoof who they are when calling someone else and having the caller appear to be anyone they want.[40] Having a hard time getting someone to pick up their phone may be much easier if it appears that the caller is, for example, "The White House."

Let's now examine and address the elephant in the room – breaches of our electronic data storage systems that can wreak utter havoc for our organizations, as everything today runs on electronic databases and cloud– and internet–based systems. We have vulnerability from anywhere, everywhere, abroad, and from unknown and nefarious sources. These problems existed before but seemed to have only been magnified perhaps geometrically during the pandemic, a time where we have been isolated and feel even more vulnerable and at risk as professionals who follow and cherish the law, that other outside parties disdain.

We have seen during the pandemic the Seyfarth Shaw cyberattack,[41] the Colonial Pipeline cyberattack,[42] a Florida water system almost

---

[36] *See* Ben Zimmer, *'Deepfake': A Piece of Thieves' Slang Gets a Digital Twist*, WALL STREET JOURNAL, Jul. 23, 2021, https://www.wsj.com/articles/deepfake–a–piece–of–thieves–slang–gets–a–digital–twist–11626983869.

[37] *Id.*

[38] *10 Best Deepfake Apps and Websites You Can Try for Fun*, BEEBOM, Jan 7, 2022, https://beebom.com/best–deepfake–apps–websites/.

[39] *Id*.

[40] *Understanding Spam Calls / Caller ID Spoofing*, VERIZON, https://www.verizon.com/support/knowledge–base–218765/.

[41] AJ Shankar, *Ransomware Attackers Take Aim at Law Firms*, FORBES (March 12, 2021), https://www.forbes.com/sites/forbestechcouncil/2021/03/12/ransomware–attackers–take–aim–at–law–firms/?sh=25d9c8d3a13e.

[42] William Turton & Karti Kay Mehrotra, *Hackers Breached Colonial Pipeline Using Compromised Password*, BLOOMBERG (June 4, 2021), https://bloomberg.com/news/articles/2021–06–04/hackers–breached–colonial–pipeline–using–compromised–password.

poisoned by cybercriminals,[43] hysteria and a more concentrated effort by government to combat the same.[44]

Electronic service vendors have publicized the risks, and many have commissioned studies and investigations to demonstrate those risks and perhaps to help sell products and services. For example, Arlington Research was commissioned to do a survey and study on outbound email security risks for the company Egress.[45] Their recent findings are both enlightening and concerning. Ninety three percent (93%) of organizations have suffered email data breaches in the last twelve (12) months. Ninety four percent (94%) of organizations are sending more emails due to the COVID–19 pandemic.[46] Thirty five percent (35%) of organizations most serious breaches were caused by remote working.[47] Thirty seven percent (37%) of breaches are due to stressed out and tired employees.[48] Sixty two percent (62%) of organizations rely on people to report email data breaches.[49] Forty six percent (46%) of employees were disciplined and twenty seven percent (27%) were fired.[50] Sensitive data has been put at risk in ninety three percent (93%) of organizations due to outbound email.[51] This author does not see a week go by without at least one or more suspicious email. The disruptive at–home, on–the–go pandemic model puts us and our organizations at great risk due to bad actors domestically and internationally with an opportunity to make money whether through stealing a wire, stealing data, or coercing a ransom to unlock a frozen system. One can imagine the more devastating consequences for a hospital, for example, versus a law firm. Nonetheless, for both liability and ethical reasons, we must meet and confront this overwhelming challenge to our proper, ethical and legal operations. Hopefully more similar initiatives will be forthcoming.

The Association of Corporate Counsel (ACC) is undertaking a valuable initiative through their ACC Data Steward Program to deal with client data security.[52] The legal profession does not have a set of rules for

---

43 Philip J. Bezanson, et. al., *Florida Water System Hack Highlights Challenges for Public Utility Cybersecurity*, 11 NAT'L LAW REV. 55 (2021).

44 Press Release, U.S. Dep't of Treasury, Treasury Takes Robust Actions to Counter Ransomware (Sept. 21, 2021), (on file with author).

45 2020 Outbound Email Security Report, EGRESS (2020), https://www.egress.com/media/zm5harrd/egress–2020–outbound–email–security–report–uk.pdf.

46 *Id.* at 3.

47 *Id.*

48 *Id.*

49 *Id.*

50 *Id.*

51 *Id.*

52 ACC DATA STEWARD PROGRAM, https://accdatasteward.com (last visited Oct. 18, 2021).

information security and gathering. ACC has created an accreditation program drawing upon expertise from NIST and ISO.[53]

We need to utilize organizations and systems to insure data security and safety. But we also need to work on our human capital, our many workers who are human and capable of mistakes and error, whether due to being tired or burnt out by COVID work life.

IV. LAWYER WELL–BEING

We have seen an increased emphasis on lawyer mental health and well–being.[54] We have all been party to the mistaken "reply all" email or a sloppy and mistaken reply from our smart phones. No matter how robust and intelligent our software and systems are, nothing will stop a tired, burnt out, depressed, or poorly motived individual. This highlights the continuing need for policies and procedures and in–house training and oversight. Simple physical and mental exercises, fun events and the like should be more widely utilized by law firms and organizations. Larger firms do this better but smaller ones often overlook this.[55] Mistakes and accidents will happen but when defending the lawsuit or ethics complaint, nothing is better than offering documented policies and procedures, training programs and solid attempts to avoid mistakes.

V. CRYPTOCURRENCY

Just when you thought it could not get any more challenging in navigating business and practice electronically and remotely, in comes cryptocurrency.[56] A couple of months ago, this author was home working remotely when a regular law firm client sent an email inquiring as follows: "Do you see it as a problem receiving Bitcoin as payment for legal services for a client's brother with appropriate third party payment waivers?" Well, after frantically researching this somewhat novel inquiry and a dearth of authority to follow, I devised the following response to this legal research/legal opinion inquiry:

"I'm glad you are familiar with cryptocurrency. There are lots of obvious risks and no concrete specific rules in this context. First, it's not currency but it's property. Jurisdictions are allowing its use in this context. One rule seems to be that you must convert it to US currency immediately

---

53 *Id.*

54 *See supra* note 3.

55 *Id*.

56 *See generally* Jake Frankenfield, *Cryptocurrency*, INVESTOPEDIA (Aug. 9, 2021), https://www.investopedia.com/terms/c/cryptocurrency.asp.

upon receipt. The client must be contemporaneously notified. Most importantly, we cannot overcharge or charge unreasonable fees. You obviously need an electronic wallet and must use a bitcoin exchange to value it at market rates. Many suggest using the NY Stock Exchange Bitcoin Index. You also need to use a N.J. licensed payment processor. Since you have a third party paying you know that you need to use due diligence. You need to maintain independence and impartiality and want to make sure that no one is seeking to launder money through this novel process. Any processing costs need to be discussed and agreed upon. It is also critical to disclose all of these steps described in your engagement letter. I hope this assists you. Unfortunately New Jersey has not provided direct guidance here so we need to look to out of state and national authorities. This is obviously a transaction fraught with risk where you also probably will have no liability insurance overage if things go badly. Good Luck!"

A few jurisdictions have issued ethical or practice guidance here, but most have not. Apparently, four jurisdictions are allowing cryptocurrency to be used as a form of payment.[57] Just like lawyers being stiffed with international payments and email closing/wire scams, here too are dangerous waters. Cryptocurrency is also being widely used in ransomware cases. There is little, if any, governmental regulation, as intended. If things go badly, there is probably no recourse. We are dealing with a digital asset, not currency. Much like a new client brings you his supposed solid gold Rolex versus cash, should we lawyers really be getting into the business of bartering or swapping? Until such time as there is real recognition, regulation and accountability, this is an area best left to risk–taking business folks, not purveyors of the law.

VI. CONCLUSION

Well, it seems that in a period of a few years, perhaps accelerated by a pandemic, we are confronted and immersed head–on into various modes of full–time technology. Due to its newness and vulnerability, the liability–ridden practice of law seems to be amplified. We need to learn, study, educate and regulate to protect us and to protect the public at large. Most importantly, we should rely upon professionals and create policies, procedures and practices and oversight so these technologies are followed, and vulnerabilities are sought to be avoided and minimized.

---

[57] Melissa Heelan Stanzione, *Washington D.C. Lawyers Can Accept Cryptocurrency as Payment*, BLOOMBERG LAW, (June 30, 2020), https://news.bloomberglaw.com/us–law–week/washington–d–c–lawyers–can–accept–cryptocurrency–as–payment.