Pie in the Sky: Cloud Computing Brings an End to the Professional Paradigm in the Practice of Law

Kenneth L. Bostick
University at Buffalo School of Law (Student)
Pie in the Sky: Cloud Computing Brings an End to the Professionalism Paradigm in the Practice of Law

KENNETH L. BOSTICK†

“[O]ne may critici[z]e even what one reveres.”

INTRODUCTION: A STORM ON THE HORIZON

On the heels of a swift wind, the clouds have come. To the untrained eye, these clouds appear harmless, indeed, even advantageous, especially for practicing attorneys. But these clouds carry a substantial storm to the practice of law, and although much of the threat has already been diagnosed, confronted, and moderated, the lasting effect, though subtle, deals a critical gust to a long-standing ideology.

The clouds and ensuing storm to which I allude are the influx of cloud computing, the recent trend away from personal or on-site media storage, into the legal profession.

† J.D. Candidate, Class of 2013, SUNY Buffalo Law School.

1. Oliver Wendell Holmes, Jr., The Path of the Law, 10 Harv. L. Rev. 457, 473 (1897).

2. Shellie Stephens, Going Google: Your Practice, the Cloud, and the ABA Commission on Ethics 20/20, 2011 U. Ill. J.L. Tech. & Pol'y 237, 238 (2011); Christopher Soghoian, Caught in the Cloud: Privacy, Encryption, and
Cloud computing, commonly referred to as “the cloud,” is changing the way the Internet is used, introducing an innovative approach to operating and interacting through the World Wide Web. The cloud computing model has been especially beneficial for businesses, which can increase their efficiency by outsourcing their data storage and data management to third party cloud service providers. This model allows businesses to avoid the burden of the security and management responsibilities associated with data storage, as well as the complexities of maintaining the infrastructure under which the data is held.

Some say that given the numerous advantages the cloud computing model offers, it is common sense for the legal profession to take full advantage. After all, cloud service providers now offer an array of applications designed specially to make the day-to-day functions of law practitioners much easier. Accordingly, as attorneys and law firms seek to increase the efficiency and decrease the

---

3. Hien Timothy M. Nguyen, Cloud Cover: Privacy Protections and the Stored Communications Act in the Age of Cloud Computing, 86 NOTRE DAME L. REV. 2189, 2202 (2011) (“Cloud computing has been heralded as being potentially transformative for the way individuals use and interact over the Internet.”).


7. Black, supra note 5, at 747 (arguing that “common sense prevails” when deciding whether to shift to cloud computing, and stating that “[l]awyers must resist the urge to overreact to emerging technologies”).

8. See id. at 746 (listing some of the online services available to attorneys).
overhead costs of their practices, it is no wonder that cloud computing has become a valuable and viable option.\textsuperscript{9}

But while shifting to the cloud computing model appears to be a logical measure to most, others caution that the decision requires more than a cursory review of the potential benefits.\textsuperscript{10} It is often the glaring security concern in delegating data management responsibilities to service providers that causes apprehension.\textsuperscript{11} But, as I will argue, that attorneys are even willing to consider handing over their data storage and computing responsibilities to third parties is a much more troubling concern, which may signal the beginning of the very end of professional autonomy in the practice of law.\textsuperscript{12}

To be sure, this Article does not directly confront the substantive legal issues that have developed with the emergence of the cloud computing model. There are many—far too many to consider comprehensively in one sitting.

\textsuperscript{9} Id. at 746 ("These online platforms are attractive, economical, and viable alternatives for law firms of all sizes.").

\textsuperscript{10} See David S. Barnhill, Cloud Computing and Stored Communications: Another Look at Quon v. Arch Wireless, 25 BERKELEY TECH. L.J. 621, 642 (2010) (warning about privacy implications); see also Francoise Gilbert, Cloud Service Contracts May be Fluffy: Selected Legal Issues to Consider Before Taking Off, J. INTERNET L., at 1 (Dec. 2010) ("Relinquishing control over, and custody of, one's crown jewels to one or more cloud service providers raises a plethora of legal issues."); Matthew A. Verga, Cloudburst: What Does Cloud Computing Mean to Lawyers, 5 J. LEGAL TECH. RISK MGMT. 41, 46 (2010) (noting that attorneys must keep potential issues in mind when counseling clients and the transition to or the use of cloud computing).

\textsuperscript{11} See Soghoian, supra note 2, at 361 ("Unfortunately the shift to cloud computing needlessly exposes users to privacy invasion and fraud by hackers. Cloud-based services also leave end users vulnerable to significant invasions of privacy by the government . . . ."); Stephanie L. Kimbro, Practicing Law Without an Office Address: How the Bona Fide Office Requirement Affects Virtual Law Practice, 36 U. DAYTON L. REV. 1, 19 (2010) ("[T]here are still some attorneys who debate the safety of cloud computing in law practice management.").

\textsuperscript{12} I use that phrase, "the beginning of the very end," because the collapse of professionalism in the legal profession is well documented and has been discussed at length. See discussion infra Part V.A. This scholarship suggests that the end has been near for quite a while. My suggestion is that the immersion of cloud computing into the legal profession suggests that the very end is impending.
Attorneys and scholars have already raised critical legal questions regarding how to reconcile cloud computing with the search and seizure implications of the Fourth Amendment, the USA Patriot Act of 2001, electronic discovery demands pursuant to Federal Rule of Civil Procedure 34, jurisdictional challenges, trade secret

13. Barnhill, supra note 10, at 642 (“Because of the nature of cloud computing, data must be stored with third parties. Thus, courts must consider the broad implications of Fourth Amendment doctrine that ‘a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties to the cloud.’”) (quoting Smith v. Maryland, 442 U.S. 735, 743-44 (1979)); Nguyen, supra note 3, at 2203 (“The growing trend towards cloud computing usage means that more and more people will be storing their data on remote servers (which will likely be outside Fourth Amendment protections, as currently understood.”); David A. Couillard, Note, Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing, 93 MINN. L. REV. 2205, 2206 (2009) (“The Supreme Court has not even addressed the Fourth Amendment’s application to e-mail, let alone the expanding uses of cloud-computing platforms.”).

14. Paul Lanois, Caught in the Clouds: The Web 2.0, Cloud Computing, and Privacy?, 9 NW. J. TECH. & INTELL. PROP. 29, 45 (2010) (“Outside of the United States, an often mentioned hurdle to the international adoption of cloud computing is the USA Patriot Act of 2001, which expands law enforcement’s surveillance and investigative powers and grants the U.S. government a right to demand data on the grounds of homeland security.”) (citation omitted); see also ROBERT GELLMAN, WORLD PRIVACY FORUM, PRIVACY IN THE CLOUDS: RISKS TO PRIVACY AND CONFIDENTIALITY FROM CLOUD COMPUTING 14 (2009), http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf (“Although a court order is required, the FBI’s authority under the USA PATRIOT Act is sufficient to extend to a record maintained by a cloud provider.”).


obligations,\textsuperscript{17} and especially with the Electronic Communications Privacy Act of 1986, which includes the Stored Communications Act,\textsuperscript{18} a particularly relevant piece of legislation to consider when dealing with the cloud computing model.

While these are complex legal issues that have been, and will continue to be, discussed as the law becomes more acquainted with cloud computing, they are beyond the scope of this Article. Instead, this Article focuses on how the decisions by attorneys and law firms, whether fully-informed or not, to shift to the cloud computing model affects the autonomy of the law profession, and the implications of incorporating new technology into legal practice. More specifically, this Article suggests that the cloud computing option presents the legal profession with an opportunity to revive its fading professional autonomy and distinguish itself from the ordinary business.\textsuperscript{19} I argue

\footnotesize

\begin{itemize}
\item effective way to require, across-the-board, that all the world's cloud services store their data in any given country . . . .
\item \textsuperscript{17} GELLMAN, supra note 14, at 7 ("Information in the cloud may have more than one legal location at the same time, with differing legal consequences.\).)
\item \textsuperscript{18} GELLMAN, supra note 14, at 16 ("[A]ccording to the Uniform Trade Secrets Act, a trade secret must be, among other things, 'the subject of efforts that are reasonable under the circumstances to maintain its secrecy.' Whether disclosure of the trade secret to a cloud provider would violate the obligation to make reasonable effort to maintain secrecy is debatable.") (quoting UNIF. TRADE SECRETS ACT § 1(4)(ii) (amended 1985), 14 U.L.A. 538).
\item \textsuperscript{19} See discussion infra Part V.B.
\end{itemize}
that the cloud’s basic structure and the celebrated advantages of that structure collaborate to breed a sense of indifference to how the cloud actually operates—an issue that should be of the utmost importance to any legal practitioner considering cloud computing.\footnote{See discussion infra Part II.B.} Moreover, the particular cloud model that is likely the most conducive to the practice of law may leave some of those celebrated advantages largely untapped.\footnote{See discussion infra Part II.B.}

Most importantly, this Article argues that the proverbial “elephant in the room”—that is, the inherent security risks associated with cloud computing\footnote{See discussion infra Part III.A.}—renders the cloud computing model fundamentally unfit for the practice of law. Although ethics committees have by and large held the use of various cloud computing models permissible in legal practice,\footnote{See discussion infra Part IV.B.} the Professionalism Paradigm, as described by Russell Pearce in the 1990s,\footnote{See discussion infra Part V.A.} should pressure the legal profession—if it is still an autonomous profession at all—to reject the cloud computing model, because it impermissibly compromises a core responsibility of attorneys.\footnote{See discussion infra Part III.A.}

It is no secret that the practice of law has slowly, but surely, developed into “the business of law,”\footnote{Chief Justice Warren Burger, The Decline of Professionalism, 63 \textit{FORDHAM L. REV.} 949, 949 (1995); see also discussion infra Part V.A.} but the influx of cloud computing signals that the very end of professional autonomy in legal practice is nearing at an alarming pace.
I. BOTTLING THE CLOUD

A. A Brief Practical Explanation of the Cloud

Defining the cloud is no simple task, and misguided attempts to explain it have often led to confusion. In truth, not many have the expertise or understanding to describe it clearly. Even scholars have struggled to develop a clear, universal definition for the cloud. Perhaps the most reliable definition is provided by the National Institute of Standards and Technology ("NIST"), which states: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." In broader and simpler terms, "cloud computing is the practice of storing and processing data apart from the local machines on which users access it." The "cloud" can be seen as a visual metaphor that conceptualizes the cloud computing model. One way to think of it is this: because there is no need to be tied down to a single computer or device to access personal files, it is as if all of our data can be accessed from an ever-present

27. Andrew Z. Adkins III, Law Firm Management in the Cloud: Leveling the Playing Field for Law Firms, LEGAL TECH. INST. 3 (Fall 2011), http://www.legal.rippe.com/LMS_Documents/cloudwp.pdf. ("There have also been several different attempts to define cloud-based computing and at times, this results in confusion in the marketplace.").

28. See David Colarusso, Note, Heads in the Cloud, a Coming Storm the Interplay of Cloud Computing, Encryption, and the Fifth Amendment’s Protection Against Self-Incrimination, 17 B.U. J. SCI. & TECH. L. 69, 80 (2011) ("[T]he precise definition of cloud computing remains somewhat fuzzy around the edges . . . .").

29. Barnhill, supra note 10, at 638 ("Many scholars’ attempts to define cloud computing have not yielded a universally agreed-upon definition.").


cloud above us. The cloud model allows access to personal data files from any device, anywhere, so long as there is a working Internet connection.\textsuperscript{33}

Joseph I. Rosenbaum created a series of practical analogies to help his readers understand cloud computing.\textsuperscript{34} For example:

You have no idea where the player that displays \textit{Gone With the Wind} is located, nor do you know where the servers are that connect you, in Minnesota, to gamers in Argentina, France, Thailand and Australia. You can watch broadcast network television, cable, or satellite, or stream music from a variety of sources and access the Internet, right from your living room - or any room. You don't worry about who owns the content or how it happens that when you want content, you can access it with the press of a button or the click of a mouse. Virtual, on-demand service: what, how, when, and wherever you want it. But you do pay a subscription fee, a license fee, or an on-demand fee, or some combination of these, to obtain and use the content.\textsuperscript{35}

In fact, most people access and utilize cloud technology without even knowing it. Services such as webmail and web-based productivity applications operate on a cloud computing model.\textsuperscript{36}

While cloud computing is a relatively new concept for most,\textsuperscript{37} it has actually been on the radar for quite some

\textsuperscript{33} Harmon, \textit{supra note} 5; Kerschberg, \textit{supra note} 18, at 2; Khan, \textit{supra note} 4, at 265 (“Using their broadband Internet connections, users will be able to access cloud services without being tied to the particular computer that holds the program or the data they want to use.”).


\textsuperscript{35} \textit{Id.}

\textsuperscript{36} Kevin Werbach, \textit{The Network Utility}, 60 \textit{DUKE L.J.} 1761, 1812-13 (2011) (“A substantial majority of Americans already use services such as webmail, online data storage, and web-based productivity applications that are considered cloud computing.”).

\textsuperscript{37} The world is becoming more familiar with cloud computing, generally because of its rapid growth in the business industry. \textit{See} Soghoian, \textit{supra note} 2, at 361 (finding “[i]ndustry analysts predicting that cloud computing related revenues will grow to somewhere between $40 and $160 billion over the next few years”); Lanois, \textit{supra note} 14, at 30 (“Information technology (IT) research and advisory company Gartner, Inc. already forecasts the market for cloud
time.38 There are calculated theories of cloud computing dating further than fifty years back,39 developed by some of the world's most computer-savvy thinkers.40 The universal shift to cloud computing was effectively facilitated by electronic mail.41 As a result, most people have been using cloud computing since e-mail became a popular form of communication, as servers such as Hotmail, AOL, and Gmail all run on cloud-based models.42 The cloud computing model has also propelled popular social networking sites like Facebook and Twitter.43 Today, as major companies such as Google offer myriad cloud-based services,44 cloud computing has become a leading model for Internet service providers and is likely to play a major role in supporting further technological advancements over the next several years.45

services to significantly expand in the coming years, from $58.6 billion in revenues in 2009 to an estimated $68.3 billion in 2010 and $148.8 billion in 2014.

38. Gellman, supra note 14, at 4 ("While the storage of user data on remote servers is not new, current emphasis on and expansion of cloud computing warrants a more careful look at its actual and potential privacy and confidentiality consequences."); Martin, supra note 6, at 285 ("As long as fifty years ago, organizations could connect widely-dispersed terminals to a mainframe computer. Cloud computing is nothing more than the application of old principles using new technology.") (citation omitted).

39. Ryan et al., supra note 16, at 7 ("[T]he debate around the theories of cloud computing have been taking place for more than 50 years.").

40. See id. ("Indeed, the world's leading thinkers within the area of cloud computing are just as old as the theories of computing themselves.").

41. Soghoian, supra note 2, at 363 ("The first application to move to the cloud was electronic mail ...").

42. See Ryan et al., supra note 16, at 8.

43. Lanois, supra note 14, at 33 ("Services such as popular social networking sites Facebook and Twitter also make use of cloud computing.").

44. Colarusso, supra note 28, at 83.

45. William Jeremy Robison, Note, Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act, 98 Geo. L.J. 1195, 1203 (2010) ("Widespread consumer embrace of early cloud computing offerings suggests that a meaningful shift is underway, rather than a passing fad."); Kerschberg, supra note 18, at 5 ("Cloud computing here is here to stay.").
B. A Brief Technical Explanation of the Cloud

There are three basic cloud service models: Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS). For those without much computer knowledge, this may look terrifying, but it is not so bad. In fact, one of the celebrated benefits of the cloud model is that the consumer does not necessarily need to understand anything about the cloud structure to use it because the cloud service provider takes care of its management. Moreover, the majority of cloud computing services involve some element of each of the three models, making the distinctions among them rather irrelevant. However, while the distinctions may be irrelevant as a practical matter, cloud computing in the aggregate is a bit easier to grasp with the understanding that there are multiple models that provide similar, but distinct, services. So at the risk of making irrelevant distinctions, an abbreviated explanation of the three models is in order.

Infrastructure as a Service, or “IaaS,” refers to the capability that allows consumers to install and run software from various devices, such as personal computers and cellular phones. IaaS provides the servers and storage space on which consumers can run their applications. Essentially, IaaS creates a virtual data center that allows the consumer to choose the specific operating systems, database systems, and web servers that best fit their needs, offered on a pay-as-you-go basis.

46. Barnhill, supra note 10, at 639.
47. MELL & GRANCE, supra note 30, at 2 (“The consumer does not manage or control the underlying cloud infrastructure.”).
49. MELL & GRANCE, supra note 30, at 3.
50. Barnhill, supra note 10, at 640.
51. Martin, supra note 6, at 292.
Software as a Service, or “SaaS,” offers applications that can be easily accessed by any device with a working Internet connection. For example, a SaaS that most people are familiar with is Google Apps. Google Apps is a free service that allows customers to perform almost any computing task (write documents, e-mail, build spreadsheets, create websites, instant message, and more) under a personalized domain name, using Google servers for storage. With Google Apps, it may be unnecessary for consumers to purchase expensive office applications like Microsoft Office for their personal computers or other computing devices. Instead, customers enjoy the freedom to perform all of their essential computing tasks (as well as those less essential tasks), while Google takes care of any necessary maintenance of the infrastructure. Because the data is stored on the service provider’s server, and not on any particular computer or device, the user’s personal computer is essentially useless in the process. Some other notable SaaS service providers include GMail, Yahoo! Mail, and Mint.

Lastly, Platform as a Service, or “PaaS,” is a “platform for application development that gives customers tools and a computing environment to develop and run their own applications.” Thus, PaaS allows users to develop their own applications and deploy them on servers in the cloud.

52. Gilbert, supra note 10, at 19 (“SaaS services are usually easy to access and easy to use . . . .”).
53. See Barnhill, supra note 10, at 639; Kerschberg, supra note 18, at 3.
54. Kerschberg, supra note 18, at 3 (“Google Apps (Gmail, Calendar, Docs, etc.) for business is a quintessential example of SaaS.”).
55. See Christopher Negus, Foreword to Scott Granneman, Google™ Apps Deciphered: Compute in the Cloud to Streamline Your Desktop, at xxv (2009).
56. See id.
57. See id.
58. Robison, supra note 45, at 1200.
59. Gilbert, supra note 10, at 19.
60. Barnhill, supra note 10, at 639.
61. Martin, supra note 6, at 291.
The PaaS provider takes care of maintaining the underlying software infrastructure that allows the applications to function.\textsuperscript{62}

Cloud based services can be delivered and used in multiple forms to fit the organization or community that purports to use those services. \textsuperscript{63} The NIST explains four different deployment models—private clouds, public clouds, community clouds, and hybrid clouds—that can be chosen accordingly to fit a particular customer’s needs.\textsuperscript{64}

In a private cloud, the entire cloud infrastructure is provided to a single customer, often an organization.\textsuperscript{65} Management of a private cloud may be controlled by the organization, a third party, or both may hold management responsibilities.\textsuperscript{66}

Community clouds are offered to communities of consumers or organizations that share the same concerns.\textsuperscript{67} Like private clouds, community clouds may be managed by the organizations themselves, third parties, or a combination of both.\textsuperscript{68}

Public clouds are open for public use.\textsuperscript{69} Many of the cloud-based services that most people can readily identify are public clouds. Google Apps is an example of a public cloud.\textsuperscript{70}

Lastly, hybrid clouds are combinations of private and public cloud infrastructures “that remain unique entities,
but are bound together by standardized or proprietary technology that enables data and application portability.\footnote{MELL & GRANCE, supra note 30, at 3; Barnhill, supra note 10, at 640.}

While there is “a general recognition that cloud computing is the practice of storing and processing data apart from the local machines on which users access it,”\footnote{Colarusso, supra note 28, at 81.} it is important to note for the purpose of clarity that cloud computing and cloud storage are not synonymous terms.\footnote{Harmon, supra note 5.} Cloud computing generally refers to the use of online software applications controlled by third party service providers,\footnote{Id. (“Cloud computing is the use of software applications online—applications that don’t reside on the computer with which you’re working.”).} while cloud storage refers to “the depositing of your data online, at a place from where you can access the information as needed, from wherever you are, using any mobile computing device at your disposal.”\footnote{Id.} Most cloud service providers offer both applications and data storage.\footnote{Id.} Although a closer understanding reveals that cloud computing and cloud storage refer to slightly different actions, for the purposes of this Article it makes more sense to refer to the two terms as one in the same. As such, all further references to cloud computing in this Article should be taken to include both cloud storage and cloud-based applications.

II. CAUTION ON CLOUD NINE

A. The Cloud in All Its Glory: Cloud Computing Offers Vast Benefits to the Practice of Law

So what makes the switch from personal computing to cloud computing desirable for attorneys and law firms? Perhaps the prime advantage of the cloud computing model is that it minimizes the customer’s technology investment.\footnote{Id. (“The underlying reason, proponents explain, is that you can minimize your firm’s technology investment.”).}
Cloud computing allows the customer to pay only for the services that it wishes to access. Under the personal computing model, businesses are often obligated to buy more computing capacity than necessary for essential tasks. This includes not only the software programs themselves, but also the corresponding security, technical, and support requirements necessary to run the software effectively. In addition, businesses may be forced to either buy multiple copies of necessary software or to purchase upgrades or other programs that allow the software to run at multiple workstations. Then, after those significant expenses, many of the purchased capabilities are often either severely underutilized or completely unwanted by the customer.

The cloud computing model vastly reduces these unnecessary expenditures, leading to an overall reduction in overhead costs. Using a third-party cloud service provider would allow a law firm to buy and support only the programs and services that it truly needs. Moreover, because cloud-based applications are run from a host computer, all of the firm's computers are kept up to date with the most recent versions of the applications without having to upgrade each computer one by one, as the service

78. Kimberly L. Rhodes & Brian Kunis, Walking the Wire in the Wireless World: Legal and Policy Implications of Mobile Computing, 16 J. TECH. L. & POL'Y 25, 31 (2011); see also Martin, supra note 6, at 285 (“Cloud computing allows individuals and businesses to purchase and use sophisticated technology services over the Internet on an as-needed basis.”).

79. DeVore, supra note 5, at 367.

80. See id.

81. Harmon, supra note 5.

82. DeVore, supra note 5, at 367; Martin, supra note 6, at 285 (“Cloud computing is a cost-effective alternative to buying and maintaining expensive and complicated computer hardware and software, but it is not really new.”).

83. Black, supra note 5, at 746.

84. DeVore, supra note 5, at 367; Rhodes & Kunis, supra note 78, at 31 (“In a cloud computing environment, a company only pays for the services that it wishes to access or workers it chooses to enable.”).
provider upgrades the software continuously. In fact, the customer does not even need to own a copy or license of the software applications. This makes cloud computing both a desirable and economically efficient model.

Additionally, “most cloud computing services are either free or significantly cheaper than more traditional desktop offerings.” Thus, shifting to cloud computing can reduce technology expenditures considerably. In light of the fact that most law firms spend on average somewhere between 3.5 and 6% of their gross revenue on technology expenditures, cutting extra costs can have a sizeable impact on the bottom line. Furthermore, with business clients becoming keener to the business practices of the law firms they employ as counsel, firms are feeling pressure from their major clients to cut down on the overhead and technology costs that drive up the bill. Accordingly, law firms may choose cloud computing to appeal to large organizational clients that place structural demands on their counsel.

Another major advantage of cloud computing is that because a service provider provides the infrastructure and platform for the services, the firm or organization is not charged with the responsibility of system maintenance and troubleshooting. In addition, “[t]he large, up-front capital expenditures necessary for an IT security overhaul are not required in the cloud.” Thus, the cloud computing model is

85. Adkins, supra note 27, at 5; Harmon, supra note 5 (“You don’t have to think about software upgrades, for example; your cloud service, presumably, will keep things upgraded for you.”).

86. Verga, supra note 10, at 42-43.

87. See Rhodes & Kunis, supra note 78, at 31.

88. Soghoian, supra note 2, at 366.

89. Adkins, supra note 27, at 9.

90. Kimbro, supra note 11, at 25.

91. See id. at 24-25.

92. Black, supra note 5, at 746 (finding that with cloud computing there is “less hassle related to maintaining and upgrading the case management system . . . .”); see Kerschberg, supra note 18, at 2.

93. Rhodes & Kunis, supra note 78, at 31.
particularly desirable among smaller law firms and solo practitioners who do not have the resources for a full-time information technology support staff.94

Moreover, as cloud computing is becoming more mainstream, a variety of services offered by companies that provide Software as a Service are becoming available to attorneys.95 These SaaS applications are accessible from all devices connected to the Internet96 and are designed to make the everyday tasks of the attorney easier, all while the service “provider operates, updates, and maintains the software.”97 There is now an array of useful applications available to attorneys—from online timekeeping and billing, to client, case, document, or project management.98 Unquestionably, the list of available applications will continue to grow as the cloud model gains traction. Because cloud computing is a service industry, cloud service providers will be under constant pressure to meet the needs of their market.99 As a result, attorneys can count on seeing new and enticing applications and services tailored to the demands of legal practice.100 As word of these new applications spreads, more and more attorneys will inevitably join their colleagues in the shift to the cloud.101

Cloud computing has been particularly convenient for attorneys with virtual law practices102 and other attorneys who practice from their computers at home (or anywhere

---

94. See Adkins, supra note 27, at 11.
95. See Black, supra note 5, at 746.
96. See Kerschberg, supra note 18, at 2.
97. Black, supra note 5, at 746.
100. See Kimbro, supra note 11, at 4 (noting that at the rate at which technology is evolving, there will be applications to “create additional secure methods that will provide more complex and richer forms of communicating with clients and other professionals online”).
101. See id. at 2.
102. See id.
they are connected to the Internet). Virtual law practices benefit from the cost effective and time saving applications offered by service providers as well as from having an infrastructure that they do not need to upkeep personally.\(^\text{103}\)

As Randal Picker put it, one of the major difficulties with owning and operating a personal computer is that “you are your own tech support, and most of us are getting lousy service.”\(^\text{104}\) With cloud computing, virtual law practitioners do not need to be fluent in computer technology to run an effective law practice from their personal computers. The cloud service essentially comes with its own information technology service, so attorneys can focus on their clients’ matters.\(^\text{105}\)

B. Checking the Weather: Law Practitioners Should Avoid Throwing Caution to the Wind When Considering Cloud Computing

Another benefit of the cloud computing model lies in its versatility, as attorneys and law firms can select the deployment model most favorable for their practice. A main variation in the deployment models is the degree to which the cloud is accessible to others.\(^\text{106}\) In the cloud, there is an indirect relationship between accessibility and control.\(^\text{107}\) As the number of people that have access to a particular cloud increases, the amount of control each user has over the data decreases.\(^\text{108}\) Accordingly, due to the highly confidential nature of the data stored by attorneys, private clouds, which limit the amount of users, appear to be the optimum choice.

---

103. See id.


105. See Black, supra note 5, at 746.

106. See discussion supra Part I.B, pp. 1383-84, for a description of deployment models.

107. See id.

108. See, e.g., Barnhill, supra note 10, at 644.
for legal practice. 109 Private clouds have been widely accepted as the ideal deployment model for businesses because their access restrictions create a much more secure computing environment. 110 Private clouds have been characterized as “best-of-both-worlds” models, because they allow for a more closely managed data center with the typical cloud infrastructure. 111

But although the private cloud may appear acceptable for legal practice, its structure may ultimately suppress its potential benefit. Because private clouds are more closely managed, information technology departments typically have to buy, build, manage, and control their data centers. 112 Thus, data storage on a private cloud actually may not yield the benefit of reduced data management responsibility and downsized information technology departments. 113 If information technology departments are still required to manage the data and its storage, a crucial benefit of cloud computing is essentially equalized. Consequently, attorneys who shift to cloud computing are likely to abandon some of its benefits as they square their ethical responsibilities with technological opportunities.

Furthermore, the structure of the cloud, although convenient for most users, brings about an additional concern that may be overlooked by legal practitioners considering cloud computing. While the cloud’s three-tiered structure may not be too difficult to understand, there is no incentive to inquire about the cloud’s basic infrastructure because consumers often have limited or no control over IaaS, PaaS, or SaaS. 114 Again, one of the main selling points of cloud computing is that the customer need not maintain

110. Id. at 199.
111. See John Foley, Private Clouds (Can We Say That?) Begin to Take Shape, INFO. WEEK, Aug. 11, 2008, at 25.
112. Id.
113. See id.
114. See discussion supra Part I.B.
or manage the infrastructure. In other words, the customer is encouraged to leave important questions, like where and how information will be stored, largely to the discretion of the third-party storage provider. As convenient as that may be, it shocks a basic instinct essential to legal practice—to know or to inquire until you know. Furthermore, the general attitude that the distinctions among the models are "essentially irrelevant" breeds an indifference to knowledge of particulars, an indifference that may ultimately lead to an uninformed decision. Such uninformed decision making is unacceptable when the decision has the potential to affect legal and ethical duties to clients, however indirectly.

In today's technological society, it is easy for both individual and organizational consumers to take routine computing tasks like web browsing and data storage for granted. To make matters worse, many consumers lack the patience or the incentive to research and discover the inner workings of these processes. This is especially the case with cloud computing. Also, with the cloud adding further complexities to personal computing as we know it (or as we think we know it), it is increasingly dangerous for consumers to take it for granted—especially law practitioners—who work with highly confidential information. That is why even the basic structure of the cloud should raise a red flag as to its place in the practice of law. As it is, the cloud computing structure offers an entirely unsuitable stance on data security: Don't worry,

115. See Black, supra note 5, at 746 ("Taking advantage of SaaS law practice software allows you to focus on the ever-important task of practicing law while the SaaS provider operates, updates, and maintains the software for you.").


117. See MODEL RULES OF PROF'L CONDUCT R. 1.6 (2012). Here, the duty most affected is the duty of confidentiality. Because cloud computing has the potential to affect confidentiality, legal practitioners must be fully aware of how it works before choosing to employ it.

118. Robison, supra note 45, at 1199 ("Many Internet users have experienced cloud computing, but fail to recognize or understand the technology making it possible.").

119. See Kimbro, supra note 11, at 1.
your information will be safe. Nevermind how. We will take care of it.

III: THE ELEPHANT IN THE CLOUD

A. The Insecure Web: The Cloud Computing Model Presents an Inherent Security Risk

While there are certainly plenty of legal issues concerning the cloud that have not yet been revealed, the security concern posed by cloud computing has not evaded the radars. "[S]ecurity in the cloud inherently raises even greater concerns than traditional desktop-based computing due to the intangible and ‘less visible’ nature of the Internet." The American Bar Association has acknowledged that "cloud computing raises ‘specific issues and possible concerns relating to the potential theft, loss, or disclosure of confidential information.’" The cloud computing model changes the “default assumption” that protected data “will be within the control of the user.” This shift is particularly troublesome for attorneys. The cloud computing model forces the consumer, in this case the attorney, to relinquish nearly all computing control, including the storage of data, which

120. See Nguyen, supra note 3, at 2190 (noting that law is slow to catch up with technology).

121. Kimbro, supra note 11, at 19 (“[T]here are still some attorneys who debate the safety of cloud computing in law practice management.”).

122. Lanois, supra note 14, at 43.

123. Kerschberg, supra note 18 at 3 (referring to the American Bar Association’s Request for Comments on “Issues Concerning Client Confidentiality and Lawyers’ Use of Technology”).

124. Werbach, supra note 36, at 1820.

125. Timothy Martin writes, “[t]he complex web of relationships [sic] cloud computing creates can compound the difficulty of contractual compliance. At the core of these issues are concerns over security, confidentiality, and ownership of electronic data as well as liability for system breakdowns.” Martin, supra note 6, at 295. The maintenance of “security, confidentiality, and ownership of electronic data” are all vital to the practice of law. Id.
inevitably includes confidential client information. As a result, the attorney becomes dependent on the performance of the cloud service provider. But the performance of Internet service providers and attorneys is (at least hypothetically) regulated by different forces. The incentive for successful management by the service provider is largely driven by the free market, the service contract, and the general policies of good business. This differs significantly from the attorney, whose actions are additionally governed by a professional code of ethics.

Furthermore, it is unclear what role this new default assumption takes on from a client's perspective. Clients expect confidentiality, regardless of who controls the information. So what happens when the entity that controls the information is not governed by a code of ethics? If the default assumption of control has changed, will lawyers and law firms now have to highlight confidentiality as part of their legal services?

In a discussion on how cloud computing will affect government data processing and storage, Christopher Soghoian writes that “unfortunately the shift to cloud computing needlessly exposes users to privacy invasion and fraud by hackers.” He explains:

The vast majority of cloud computing services are, by default, insecure. Often, usernames and passwords are transmitted to remote servers via unencrypted network connections. In cases

126. Harmon, supra note 5 (“You are, literally, surrendering much of your computing control—some of which involves sensitive personal and client data. You’re losing some real freedom, making yourself dependent on the performance (and sense of ethics) of your cloud service provider.”).

127. Id.

128. For a discussion of service contracts, see discussion infra Part III.B.

129. Harmon, supra note 5 (explaining that attorneys that employ cloud computing relinquish their control, and become dependent on the third party and consequently that third party's sense of ethics).

130. Soghoian, supra note 2, at 361. Soghoian recognizes that the government can also gain access to private information stored in the cloud. Id. (“Cloud-based services also leave end users vulnerable to significant invasions of privacy by the government, resulting in the evisceration of traditional Fourth Amendment protections of a person’s private files and documents.”).
where encryption is used, it is typically only used to transmit the initial login information, while all subsequent data is sent in the clear. This data can easily be snooped on by hackers. This exposes users to significant risks when they connect to the services using public wireless networks. These flaws are rarely, if ever, disclosed to end-users.\textsuperscript{131}

Soghoian’s observation is critical, and it exposes a major dilemma that practitioners considering the cloud must meet head-on. It is important to remember that in legal practice, it is not the end user that is ultimately owed the protection. Typically, individual consumers or businesses select particular cloud models to meet their specific needs. Here, however, the data theoretically belongs to the client, a third party to the transaction. There is no communication between the party owed the protection and the party purporting to provide the protection. Therefore, attorneys should be able to interpret the workings of the cloud and relay that information to the client to ensure a mutual understanding of the security risks for all parties involved.

But wait, I thought an advantage of cloud computing was that the consumer does not really have to understand it, right?\textsuperscript{132} Perhaps the bar exam should include a computer science section.

B. The Mighty Pen: Contracting in the Clouds

Because security incidents are “bound to occur”\textsuperscript{133} in the cloud, it is vitally important that attorneys know exactly what services they are getting and providing for their clients.\textsuperscript{134} The risk of privacy and confidentiality breaches can be reduced through finely tuned negotiations between the customer and the cloud service provider.\textsuperscript{135} Before finalizing a contract with a service provider, attorneys should perform due diligence on the cloud provider to make

\begin{itemize}
\item \textsuperscript{131} Id. at 372-73 (citations omitted).
\item \textsuperscript{132} See discussion supra Part II.A.
\item \textsuperscript{133} Gilbert, supra note 10, at 28.
\item \textsuperscript{134} Id. at 20-21 (noting that “[p]articular attention should be given to allocation of responsibilities and liabilities . . .”).
\item \textsuperscript{135} See GELLMAN, supra note 14, at 6.
\end{itemize}
certain that the services offered correspond to the unique demands of legal practice, especially the obligation of confidentiality. Simple clickwrap agreements are often insufficient; agreements should be complete with comprehensive provisions detailing how the service provider will meet those demands in a cloud environment. The service agreement effectively defines the professional obligations of each party. Thus, when negotiating a service agreement, "[p]articular attention should be given to allocation of responsibilities and liabilities among the different service providers in order to avoid finger pointing in the event of an incident." Because technology continues to change, it is important that attorneys consider both present and future implications of the agreement.

When confidential information is stored and managed by a third party, "the typical expectations of preservation take on new and challenging dimensions." For instance, one of the many concerns about cloud service agreements is what happens when the length of the agreement has run its course. If an attorney decides to part ways with the

136. Gilbert, supra note 10, at 20 ("The company should conduct due diligence of the proposed cloud service provider in order to determine whether the services offered correspond to the needs of the company and whether they will allow the company to fulfill its computing needs, access needs, as well as its continued obligation to protect its assets.").


138. Id. ("Detailed, comprehensive provisions tailored to the unique risks of operating in a cloud environment should be negotiated.").

139. See Stephens, supra note 2, at 243.

140. For a detailed survey and analysis of the terms and conditions offered in standard cloud computing service contracts, see Simon Bradshaw et al., Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services, 19 INT'L J. L. & INFO. TECH. 187 (2011).


143. See Gilbert, supra note 10, at 21.
provider, there must be detailed protocol regarding how data will be transferred and/or preserved. The agreement must lay out "whether and how the data will be returned to the customer or destroyed, the cost associated with this return, and the procedures to be used in the event of termination." This point becomes a serious issue when the stored data is summoned as an electronic discovery request in litigation. Without a particular contractual obligation to preserve the information in dispute, the service provider is not likely to be held liable for its destruction, leaving the attorney on the hook for ethical reprimand and likely even malpractice. While the practitioner may certainly pay extra for additional security, the service provider is ultimately responsible only for what it has contracted and received compensation for.

For practitioners who negotiate service agreements, the specter of a security breach in the cloud may leave them at a serious disadvantage. Consider that the service provider may outsource or subcontract some of its data management responsibilities to another service provider. After all, the service industry values efficiency, and thus service providers will inevitably take measures to increase the efficiency and decrease the costs of their own operation. It is clear from such scenarios that the business instinct of

144. Id. ("It is therefore even more important for the parties to ensure the proper and secure winding down of the relationship in order to ensure business continuity and to limit the risk of loss or alteration of the data.").

145. Id. at 30.

146. See Nicholson, supra note 15, at 191-93.

147. Id. at 193 ("Unless cloud service providers accept a particular contractual obligation to preserve information in dispute, they are likely to escape repercussions from the destruction of the crucial data even when they are the key player in its loss.").

148. See id. at 206. ("[A] party can pay for additional storage or other services, but it cannot expect the third-party vendor to assume any preservation responsibilities, apart from those to which it has contractually obligated itself, without additional compensation.").

149. Gilbert, supra note 10, at 24 ("The cloud service provider may also need to have the ability to subcontract some of the services to third parties. This flexibility might be necessary in order to limit financial exposures and ensure the ability to reconfigure a cloud network as needed.").
service providers shifts most, if not all of the bargaining power in their favor. Additionally, the service provider’s focus on efficiency puts a serious strain on the practitioner, who is responsible for creating a mutual understanding of the duties among all parties involved.150 In other words, the service provider’s concern is managing the data most efficiently—however that may be—while practitioners must be concerned with exactly how the data is managed, in order to ensure its security.151 Because of the disparity in bargaining power, “service providers are in a position to dictate terms that are favorable to themselves, but risky for consumers.”152 Naturally, the service provider will want to “limit the extent to which the customer can retain control over its data in order to keep all of its customers aligned within the same structure or business model.”153 Thus, a direct clash of interests ensues as parties with diverging concerns seek to maximize control over the data.

With cloud service providers operating under this business model, there should be more concern that those whose information is put at risk—the clients—have no say in the negotiation. It is important to keep in mind that a legal practitioner using a cloud computing model to manage data is not like the everyday Internet user of Google Apps, Facebook, Twitter, and other cloud-based services. Although consumers of these services use them willingly, they may not fully understand that there are associated security risks.154 Nevertheless, it is their own information that they put at risk. Conversely, when an attorney uses a cloud-based service, there is a conscious choice (as evidenced by the service contract) to deposit confidential client data in a hub susceptible to security breaches. It is this particular choice that fuels my pessimism toward the suitability of cloud computing in legal practice.

150. See Nicholson, supra note 15, at 211.
151. See id. at 211-13 (explaining that many service providers explicitly disclaim liability for lost data and provide no warranty "as to the quality or fitness of their service for any particular purpose").
152. Soma et al., supra note 109, at 211.
154. See discussion supra Part III.
To clarify, when I say security breach, I mean any situation where a client's confidential file ends up in the hands of a person or entity other than the attorney, client, or otherwise contracted-for service provider. That is not to suggest that all security breaches will be of malicious intent, or that they all will be detrimental to the client's case or the attorney-client relationship. But any security breach in this sense inherently means that client confidentiality has been violated. Although reasonable precautions may have been taken to minimize the risk of security breach, it is alarming that lawyers can take such considerable risks with confidential client information.

Presumably, the attorney fully understands the associated security risks, because he would have contracted to minimize them. If this presumption is correct, attorneys that use cloud-based services in their law practice put the highly confidential information and property of their clients at risk with full knowledge of the potential consequences. It is in this context that we see the business aspect of legal practice overshadow professional ethics. Is it not fitting that this shadow has formed with a development we call "the cloud"?

The charge is blunt: that legal practitioners are willing to compromise confidentiality by exposing client files to potential security risks, no matter how unlikely those risks are to materialize, is an unmistakable illustration of the demise of professionalism in the practice of law. Moreover, as ethics committees continue to approve of the use of cloud-based services in legal practice, the demise has transpired much too quickly for a simple resolve.

155. See Model Rules of Prof'L Conduct R. 1.6 (2012).
IV: ETHICS COMMITTEES FORECAST MOSTLY CLEAR SKIES AHEAD

A. Chasing the Clouds: The American Bar Association Tries to Keep Pace with the Changing Technology

With the shift to cloud computing and other technological advances in society, attorneys are forced time and again to address a question that never seems to have a simple answer: "How do we resolve our ethical duties to our clients and the system, our need to be economically efficient, and our duty to be competent in this swiftly changing world?"\(^{156}\) Roberta Cooper Ramo elaborated on that question:

To be an accomplished American lawyer has always meant more than simply following the legal dots (which can now be done by anyone for some issues on the web, for little to no charge without us). It has meant to be an advocate and a counselor, a definer of the dreams or hopes of clients into legal reality. Among the very best lawyers are the imaginative partners and the moral conscience in complicated situations. Most basically, being an American lawyer is to be a defender of the Constitution and the Bill of Rights. What if anything about these obligations has changed because of technology?\(^{157}\)

Theoretically, the obligations of the legal profession should remain the same. Thus, perhaps a more fitting question would be whether the means to satisfy those obligations are in accordance with the obligations of the profession.

Naturally, the American Bar Association Model Rules of Professional Conduct are probably the best starting point. But the nature of cloud computing just seems to add confusion to a body of rules that already generates ambiguity. Nevertheless, to ensure ethics keep pace with the changing technology, attorneys must remind themselves of the rules with a careful eye on how those rules are affected by the changes.

---

156. Roberta Cooper Ramo, Ethics for American Lawyers in the Age of Twitter and the Cloud, 72 Mont. L. Rev. 227, 230 (2011).

157. Id. at 231.
New age technology has already caused ethics committees to contemplate a significant change in Model Rule 1.1, which addresses the requisite competence to represent a client. The contemplated change would add the phrase: "including the benefits from technology and the risks associated with that technology." Accordingly, Rule 1.1 would read:

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation, including the benefits from technology and the risks associated with that technology.

Adding the proposed phrase to Rule 1.1 may well be necessary to ensure that attorneys keep technology in mind as they "keep abreast of changes in the law and its practice." But adding language about risk exacerbates an apprehension I will discuss at length in Part V.

Namely, when attorneys are asked to weigh risk and reward in the performance of their duties as a professional, it diminishes the idea that the practice of law amounts to something more than the ordinary business. The embodiment of "risk" in the Model Rules of "Professional" Conduct therefore seems quite ironic. If the idea behind the rules is to protect not only the client, but also the profession, we do the profession a disservice by suggesting a risk-versus-reward analysis.

I do not mean to say that no professional should ever engage in a risk-versus-reward analysis. Indeed, such analysis is often required for professionals. For instance, a doctor or surgeon must continually balance risks and

158. Id. at 230-31 ("The ABA Commission on which I sit[] is now debating whether we should ask the Ethics committee of the ABA and then the ABA's deliberative body, the House of Delegates, to add the following phrase to Rule 1.1: 'including the benefits from technology and the risks associated with that technology'.")

159. Id.


161. MODEL RULES OF PROF'L CONDUCT R. 1.1 cmt. 6 (2012).

162. See discussion infra Part V.
rewards in difficult and often life-altering situations. Similarly, attorneys must engage in some risk-versus-reward analysis when making tactical decisions about a case (e.g., whether to file in state or federal court, whether to put a particular witness on the stand, etc.). But whether to shift to cloud computing is a business decision, not a tactical decision about a file. In reality, most clients would never even consider where their file is located, and the possibility that someone other than the attorney may have access to that file is a distant concern. But if the code of ethics is worth the paper it is written on, that distance cannot diminish its influence. At its core, the critical concern is whether, when making a purely business decision that affects clients collaterally, attorneys are held to the standard of an ordinary businessman or to the heightened standards of the legal profession.

B. All Clear: Ethics Committees Generally Approve of the Cloud Computing Model in Legal Practice

A number of states have already addressed some of the more pressing concerns posed by the cloud. Thus far, the trend indicates that a relaxed standard applies (which, I would argue, implies that a general business standard, rather than a heightened professional standard, governs).

For instance, the Oregon Ethics Committee recently released a formal opinion on the legality of third-party service contracts for storing client files.\textsuperscript{163} The committee held that storing confidential client information on third-party servers is permissible “so long as [the lawyer] complies with the duties of competence and confidentiality to reasonably keep the client’s information secure within a given situation.”\textsuperscript{164} The opinion further states that “[t]o do so, the lawyer must take reasonable steps to ensure that the storage company will reliably secure client data and keep


\textsuperscript{164} Id.
information confidential." The Oregon Ethics Committee explained that reasonable steps would include performing due diligence on the service provider and ensuring that the terms of the service agreements require the provider to preserve confidentiality.

The New York State Bar Association Committee on Professional Ethics released a similar opinion, stating that lawyers may use online data storage systems to store and backup confidential client information “provided that the lawyer takes reasonable care to ensure . . . confidentiality.” The committee noted that even after due diligence and other affirmative steps to satisfy the reasonable care standard, the lawyer “should periodically reconfirm that the provider’s security measures remain effective in light of advances in technology.” That requirement is significant because lawyers would be required to “keep abreast” not only of changes in the law, but also of the changes in technology specific to the services they employ. So, if a cloud service provider makes changes to its infrastructure, the lawyer should be required to understand them, as well as how these changes affect the quality of service. As a result, due diligence cannot be viewed as a one-and-done deal. Rather, it must be performed as often as the technology changes to ensure full compliance.

The Iowa State Bar Association Committee on Ethics and Practice Guidelines addressed due diligence in an

165. Id.

166. Id. (“Under certain circumstances, this may be satisfied through a third-party vendor’s compliance with industry standards relating to confidentiality and security . . . ”).


168. Id.

169. MODEL RULES OF PROF’L CONDUCT R. 1.1 cmt. 6 (2012).

170. Perhaps another reason why bar exams should include a computer science section.
opinion on whether lawyers can ethically use Software as a Service applications in their practice. The committee opined that rules should take a “reasonable and flexible approach to guide a lawyer’s use of ever-changing technology.” The committee concluded that lawyers must “perform due diligence to assess the degree of protection that will be needed,” but it also recognized that lawyers may not have the requisite information technology knowledge and skill to perform the appropriate due diligence. To lessen the burden of due diligence, the committee yielded that lawyers may rely on the “due diligence services of independent companies, bar associations . . . or through its own qualified employees.”

The North Carolina State Ethics Committee has addressed SaaS services as well, proposing a formal opinion that lawyers may contract with SaaS services, provided that the lawyer “uses reasonable care to safeguard confidential client information.” The opinion recommends several security measures that lawyers should take before signing any contracts and encourages law firms “to consult periodically with professionals competent in the area of online security.” Among those recommendations are inclusion of “how the vendor will handle confidential client information in keeping with the lawyer’s professional responsibilities” in the service agreement; contractually requiring the SaaS vendor to return or destroy data on request; carefully reviewing the license agreement; and

172. Id.
173. Id.
174. Id.
175. Id.
177. Id.
evaluating the extent to which the vendor backs up the information that they store. 178 However, the opinion stops short of making any of the recommended security measures mandatory. 179 Making specific security measures mandatory would create a "false sense of security in an environment where the risks are continually changing." 180 This approach, of course, circles back to the requirement that lawyers must do what is reasonable under the circumstances to ensure security and confidentiality.

But as technology changes, what is reasonable under the circumstances also changes. For instance, in 2009, Arizona's Ethics Committee addressed a more novel question, distinct from the basic inquiry of whether cloud computing violates any rules of ethics. The issue was whether a lawyer could offer a cloud-based service that would allow clients to use personal computing devices to view and retrieve their own files. 181 The inquiring attorney had developed a multilevel security system, so that clients would only have access to their own files. 182 The Arizona Ethics Committee found that the heavily encrypted security system was a reasonable precaution to secure client files

178. Id.

179. Id. ("This opinion does not set forth specific security requirements . . . ").

180. Id.; see also Kimbro, supra note 11, at 7 ("T]his approach provides the necessary guidance requested by attorneys to help them in doing their due diligence to research a prospective software provider without placing restrictions on the use of the technology, which would quickly become obsolete.").


182. Id. ("First, the client files would be accessible only though a Secure Socket Layer (SSL) server, which encodes documents, making it difficult for third parties to accept or read them. Second, the lawyer would assign unique randomly generated alpha-numeric names and passwords to each online client folder. The folder names contain no information that could identify the client to which it belongs. The password would not be the same as the client folder name. Third, all online client files would be converted to Adobe PDF (Portable Document Format) files and protected with another randomly generated unique alpha-numeric password.").
and protect confidentiality and therefore did not violate any rules of ethics.\textsuperscript{183}

This proposed service is an illustration of how the cloud computing model can inspire creative changes to the practice of law. But once again, what appears to be a convenient development in cloud computing may bring with it a flood of issues that could seriously undermine professional autonomy. In a model where security incidents are already “bound to occur,”\textsuperscript{184} allowing clients to access their own files anytime and anywhere can make matters much worse. Indeed, documents in the cloud would be password protected,\textsuperscript{185} meaning that clients would have access to their password. Clients would obviously be responsible for the protection of that password. Accordingly, a reasonable step to safeguard confidentiality under those circumstances would be to ensure that the client knows the consequences of sharing the password. Perhaps a confirmation in writing would solidify the discharge of that duty.

So the lawyer is off the hook, right? Not so fast. If a security breach were to occur,\textsuperscript{186} would we be able to determine if either the lawyer or client was responsible? If it were the client’s fault, can we be sure he or she would own up to it? Vice versa? Would there need to be a hearing to determine who the guilty party is? Of course, these questions are purely hypothetical and may not arise at all. Regardless, a security breach under this model, whether the fault of the lawyer, the client, or neither, would likely cause permanent damage to the attorney-client relationship.

The encrypted system proposed by the inquiring Arizona attorney reveals an interesting, yet somewhat troubling, correlation. As technology visibly advances at a rapid pace, our society, including attorneys, develops a dangerous trust. That is, the better technology gets, the

\begin{itemize}
  \item \textsuperscript{183.} \textit{Id.}
  \item \textsuperscript{184.} Gilbert, supra note 10, at 28.
  \item \textsuperscript{185.} ST. OF ARIZ. ETHICS COMM., supra note 181.
  \item \textsuperscript{186.} Again, I mean any situation where the client’s file ends up in the hands of someone other than his attorney or the client himself.
\end{itemize}
more attorneys trust the technology to work as expected, and the more they trust third parties to maintain it. Moreover, the inquiry to the Arizona Ethics Committee suggests that technology has even convinced some attorneys to put more trust in their clients, as the proposed system would allow clients nearly unconditional access to their own files. For now, it is unclear what effect this expanded trust will have on the practice of law. Only time will tell, as technology continues to advance, and trust continues to build.

V: PIE IN THE SKY

A. In the Rearview Mirror: A Look Back at the Traditional Professionalism Paradigm

The 1980s and 1990s brought a surge of concern about the decline of professionalism in the practice of law. During that period, scholars such as Mary Ann Glendon, Sol Linowitz, and Anthony Kronman released important works arguing that lawyers and the legal profession had "lost their way, largely through becoming more elitist, selfish, separated from society, and greedy." Perhaps the greatest criticism of the legal profession came from Chief Justice Warren E. Burger, who expressed a profound concern about the shift in the professional ideal:

The bedrock of our profession from Blackstone's day has been the professional ideal: the lawyer as an officer of the court, compelled as such to maintain a standard of conduct that rises above the standard we would expect from a tradesman engaged in what many now call "the business of law." The law is not and never has


been a “business.” But we are well on the way to making it less than a profession.\textsuperscript{189}

Chief Justice Burger cautioned that lawyers must remember that they have a monopoly on legal services, and that “[l]awyers, like doctors, must be more than just skilled technicians.”\textsuperscript{190} Furthermore, he emphasized an old sentiment that “if lawyers are to be an educational and professional elite, they should not stoop to common commercialization.”\textsuperscript{191}

Yet another influential piece documenting the decline of legal professionalism was written by Russell Pearce, who examined the crisis through Thomas S. Kuhn’s theory of paradigms.\textsuperscript{192} The Professionalism Paradigm, Pearce explained, “rests on a purported bargain between the [legal] profession and society in which the profession agreed to act for the good of clients and society in exchange for autonomy.”\textsuperscript{193} That autonomy exempted the legal profession from external regulation, and distinguished the profession from the ordinary business, who, by nature, maximized self-interest.\textsuperscript{194} The distinction relied on the idea that lawyers “possess esoteric knowledge inaccessible to lay persons.”\textsuperscript{195} And because lay persons were detached from that esoteric knowledge, professional autonomy allowed for consumers to rely on the reputation and ethical character of lawyers.\textsuperscript{196} Thus, under the Professionalism Paradigm, the market for legal services was governed by “the invisible hand of reputation,” not business principles.\textsuperscript{197}

\begin{flushleft}
\textsuperscript{189} Burger, \textit{supra} note 26, at 949
\textsuperscript{190} \textit{Id.} at 954.
\textsuperscript{191} \textit{Id.}
\textsuperscript{193} \textit{Id.} at 1231.
\textsuperscript{194} \textit{See id.}
\textsuperscript{195} \textit{Id.}
\textsuperscript{196} \textit{Id.} at 1232.
\textsuperscript{197} \textit{Id.}
\end{flushleft}
The Business Paradigm, on the other hand, does not assume that lawyers place the interests of society above their own self-interest. Rather, it views lawyers as profit-maximizers who structure their practices and deliver their services as businessmen would. In the Business Paradigm, the legal profession is not entitled to autonomy at all.

Seventeen years after Chief Justice Burger's criticisms of the legal profession, there is little doubt that the practice of law has indeed become "the business of law." Despite the American Bar Association's recent attempts to stress professionalism and high morality, the practice of law has become a predominantly commercial activity whose primary purpose is to render services to the client. Knowledge of the business aspect of the legal profession is more or less mandatory for the newly admitted attorney, and a growing number of law schools now offer courses in law firm or practice management. Such courses are designed to expose law students to how law firms operate and how to effectively deliver legal services. Students who do not learn how to manage their practice are behind the curve, especially those who aspire to practice on their own or to

198. Id. at 1268.
199. See id.
200. Id.
201. Burger, supra note 26, at 949.
202. Benjamin H. Barton, The ABA, the Rules, and Professionalism: The Mechanics of Self-Defeat and a Call for a Return to the Ethical, Moral, and Practical Approach of the Canons, 83 N.C. L. Rev. 411, 443 (2005) ("[T]he ABA trumpeted the announcement of the Ethics 2000 campaign (which focused mainly on reformulations of the minimum rules) as a crucial move towards 'taking professionalism seriously' and the 'advancement of the legal profession to a higher moral ground.'").
204. See Gary A. Munneke, Managing a Law Practice: What You Need to Learn in Law School, 30 PACE L. Rev. 1207, 1217-18 (2010) ("Although the numbers are not large, an identifiable number of law schools offer courses in the discrete subject area called law practice management.").
205. Id. at 1222.
become partners with significant management responsibilities.

The shift from a professionalism to a business paradigm is largely evidenced by the inability of scholars and bar officials to describe exactly what professionalism is. Benjamin H. Barton wrote that:

[The term "professionalism" itself has proven abstruse. Most agree that professionalism implies something above and beyond the minimum behavior required under state rules of professional conduct (often referred to as rules of "ethics"). It has proven notoriously difficult to define what professionalism offers beyond the minimums of legal ethics, and most scholars and bar officials have abandoned efforts at a specific definition.]

Notwithstanding the difficulty in providing a clear description, it is clear from the Professionalism Paradigm that legal professionalism centers on the lawyer as a fiduciary who resolves conflicts of interest between the lawyer and the client in favor of the client. Clients enter into agreements with lawyers assuming that they will take a client-oriented approach, and that they are not profit-maximizing businessmen. As the practice of law has become more business based, that assumption is no longer safe.

B. Caught Under the Cloud: Cloud Computing Marks the End of the Professionalism Paradigm in the Practice of Law

Because of the significant security risks inherent in the cloud computing model, it has been suggested that law firms and attorneys considering cloud computing should balance the potential financial benefits against the costs of

206. Barton, supra note 202, at 415 (citation omitted).

207. See Pearce, supra note 192, at 1231; see also Eli Wald, Lawyer Mobility and Legal Ethics: Resolving the Tension Between Confidentiality Requirements and Contemporary Lawyers' Career Paths, 31 J. LEGAL PROF. 199, 240-42 (2007).


209. See id.
data security. But because lawyers have an absolute duty to protect the confidential information they store in the cloud, this analysis should also balance the potential financial benefits against the risk of a security breach. In essence, modern attorneys have had to value decreased overhead expenses and ease of practice against data security and confidentiality. The Professionalism Paradigm and the notion of autonomy imply that adequate security for the purposes of ensuring confidentiality carries far more weight in running an efficient practice.

After noting that professionalism has been increasingly difficult to define, Benjamin H. Barton suggested that "professionalism has come to embody what a lawyer 'should' do, i.e., professionalism has come to cover a lawyer's ethical duties." But what a lawyer should do and what he or she is required by ethics to do are not the same. As discussed, ethics committees around the country have mainly approved and applauded the use of cloud computing in legal practice, so long as reasonable precautions are taken to ensure confidentiality. Taking those ethics determinations at face value, lawyers are clearly not restricted from shifting to cloud computing.

But whether they should is an entirely different question. The migration to the cloud has made it clearer than ever that the practice of law has become separated from what Chief Justice Burger called the "bedrock" of the profession—that the conduct of a legal professional must rise above the standard we would expect from an ordinary tradesman. In this regard, the profession has fallen short, not for its openness to explore new ideas that may ultimately benefit clients, but for its failure to go beyond the minimums of legal ethics in evaluating these new ideas.

210. Couillard, supra note 13, at 2217.
211. See MODEL RULES OF PROF'L CONDUCT R. 1.6 (2012).
212. See Pearce, supra note 192, at 1231.
213. Barton, supra note 202, at 441.
214. See discussion supra Part IV.B.
Because confidentiality is so central to the practice of law, no prospect of efficiency should prompt lawyers to put it at risk, no matter how small that risk is.

It is clear that the benefits of cloud computing are many. But these benefits come at the high price of control. Undoubtedly, measures will be taken to ensure that the possibility of a security breach is de minimis. But does the role of attorneys as fiduciaries allow them to take that chance? Thus far, the repeated answer from ethics officers has been that it does. As such, I question whether there is any point that attorneys, as professionals, separate themselves from the ordinary businessman. Or is the Professionalism Paradigm, and the autonomy that comes with it, gone forever?

I ask these questions not to chastise practitioners that have already or will soon shift to cloud computing, but simply to suggest that in a world where the advancement of technology is conceptually limitless, the practice of law must have a limit. That attorneys are governed by a code of ethics makes clear that attorneys are, and should be held to a higher standard of accountability than those in other careers, business based or otherwise. So how should that higher standard translate when an attorney makes a business decision?

One last time, consider the cloud computing model. When contemplating cloud computing, attorneys have adopted the enduring formula of balancing the risk against the reward. Undoubtedly, market pressures will force cloud service providers to minimize the associated security risks of operating on a cloud-based model. Yet, a purely professional analysis—taking into account the importance of confidentiality to legal practice—should find that even

---

216. See Model Rules of Prof'l Conduct R. 1.6 (2012).
217. See Martin, supra note 6, at 294.
218. Id. at 295.
219. See Burger, supra note 25, at 949.
220. Couillard, supra note 13, at 2217 ("Businesses that use cloud-computing services must balance the financial benefits of outsourcing storage and services to the cloud against the costs of data security.").
though the risks of cloud computing are statistically minimal, they are far too significant to justify its rewards. Balancing risk versus reward implicates a gamble, an activity hardly ever associated with professionalism.

It is for these reasons I wonder if the cloud computing model is just “pie in the sky” for the legal profession. Thus far, the trend has shown that there is no line that attorneys will not cross, so long as the ethics committees allow it. As more innovative technology is progressively approved, I fear that attorneys will merely follow the legal dots, ignorant of the implications on the practice of law as a profession. If the practice of law amounts to more than just an ordinary business, it must keep its bargain for professional autonomy in mind, even when making decisions that only indirectly affect clients.221

CONCLUSION: SURVIVING THE STORM

There is no doubt that from a business standpoint, cloud computing presents a remarkable opportunity for law firms and solo practitioners to increase efficiency while dramatically reducing the overhead costs of their practice. With the cloud’s increasing acceptability in the legal profession, it seems that those who choose to stay with the conventional personal computing model will be left behind by the forward-looking market.222 But a deeper assessment of the current trend reveals troubling concerns. While much of the discussion concerning cloud computing examines the security risks posed by the use of third-party service providers to store highly privileged and confidential information,223 the less obvious implications on the legal profession continue to go largely unnoticed. Particularly, the cloud computing model presents a profound challenge to the ideology of the practice of law as an autonomous profession. Without question, the practice of law has slowly, but significantly, evolved over time into what has been

221. As opposed to decisions that directly affect their clients, such as strategic decisions about how to handle the client’s case.

222. See Black, supra note 5, at 746.

223. See Gilbert, supra note 10, at 17.
called "the business of law." This business mentality is no longer optional if a law firm or attorney intends to stay above water, and it has even been implemented into law school curriculums.

The decision whether to shift to a cloud computing model effectively blurs the line between the attorney as a businessman and the attorney as professional. While these alter egos can coexist, there must be a boundary somewhere between them. The attorney as a professional has a duty both to his clients and to the profession itself to abide by a code of ethics. Thus, when making a business decision such as whether to shift to a model of computing where the core responsibilities of the attorney as a professional are potentially at risk, an attorney should not make the decision strictly from the business perspective.

The business perspective, like in every business decision, calls for a balancing of risk versus reward. But the presence of "risk" in that equation should cause attorneys to question whether that analysis can be compromised with their professional responsibilities, both to their clients and to the profession itself. If not, then there appears to be no line that separates the law practitioner from a run-of-the-mill, wheeling and dealing businessman whose job is to turn risk into profit for his company. The emergence of cloud computing offers an opportunity for the legal profession to draw that line.

In arguing that the shift from the Professionalism Paradigm to a Business Paradigm presents the legal community with an opportunity to move to a new paradigm offering better service to clients and greater benefit to the public, Russell Pearce asserted that once the shift has occurred, the Professionalism Paradigm could be gone forever:

The legal community is poised on the brink of a paradigm shift. The anomaly arising from the disjunction between the Business-Profession dichotomy and prevailing perceptions of lawyer conduct

224. Burger, supra note 26, at 949.
225. Munneke, supra note 204, at 1217-18.
226. See Pearce, supra note 192, at 1230.
has provoked a crisis for the Professionalism Paradigm. The conditions creating the anomaly, and the indispensability of the dichotomy to the paradigm’s credibility, make it unlikely that it will be possible to revive the paradigm or bracket this anomaly.227

As more and more law firms and attorneys shift from personal to cloud computing, Pearce’s prediction is well on its way to fruition. The Professionalism Paradigm stands on a weather-beaten leg, and unless legal practitioners can commit unequivocally to decision-making that goes beyond the minimums of legal ethics, it will continue to wither away.

227. Id. at 1276.