Why Go Cloud?

Five Reasons Why Lawyers Should Adopt Cloud-based Technology

By Brett Burney

clio

Practice Management Simplified

Floating the Idea of the "Cloud"

The "cloud" offers dazzling economies of scale for storing, managing, and securing the world's swelling volumes of digital data.

Cloud computing is no longer a cyber-playground for early adopters. It is now the digital backbone for individuals and companies that demand highly secure, infinitely scalable, perpetually accessible, and centrally managed data centers maintained by highly trained IT professionals.

When you perform a search on Google.com, you're in the cloud. When you check your free Hotmail account or click "Add to cart" on Amazon.com, you're in the cloud. How else could Google, Microsoft, Amazon and others offer the scale of their services to millions and millions of users?

Lawyers would argue, of course, that buying a flower vase on Amazon is a completely different scenario than ensuring the confidentiality of client data. On the other hand, those same lawyers freely entrust their home address and credit card information to Amazon with complete assurance that their personal information is held in strict confidence.

Building Software on Top of a Cloud

The concept of "cloud computing" is still new… at least to lawyers. The core idea behind the cloud has been around since the evolution of the Internet, but the contemporary concept of the cloud grabbed the spotlight in 2006 with Amazon's "risky bet" of offering their surplus server capacity to the public as cloud-based storage.[1]

The cloud supplies the digital scaffolding for Software-as-a-Service (SaaS). "SaaS" and "cloud" are regularly and mistakenly used interchangeably. But to be precise, the "cloud" describes the back-end infrastructure that provides storage and processing power at a fraction of the cost required to build and maintain your own data center. The concept has been compared to a utility like electricity[2] — we pay for the electricity we consume off the grid rather than building and running our own power generating plants.

"SaaS" describes the functional "software" delivered to a subscriber through a Web browser. SaaS applications aren't required to piggy-back on the cloud, but it's the ideal amalgamation for providing unsurpassed functionality, accessibility, and security.

1 Cover story, "Jeff Bezos' Risky Bet," Business Week, November 13, 2006 http://www.businessweek.com/magazine/content/06_46/b4009001.htm

2 see Nicholas Carr, The Big Switch, Rewiring the World, From Edison to Google (W. W. Norton 2008

Lawyers are hesitant to adopt new technology — they must have complete confidence that nothing will impinge upon their ethical responsibilities to clients and society. This paper highlights five motives for lawyers to adopt the benefits of cloud computing and SaaS applications.

#1. The Cloud Provides a Higher Standard of Protection for Confidential Data Than Most Law Firms Can Provide On Their Own

The ABA Commission on Ethics 20/20 is currently mulling over the question of how a lawyer's ethical responsibilities apply to confidential client data stored and accessed in the cloud.[3] A few state ethics committees have also recently attempted to address the question.[4] The issue is certainly ripe but the resolution has so far been elusive.

Everything written on the topic circles back to the standard expressed in Comment 17 of Rule 1.6 of the ABA Model Rules of Professional Conduct (Client-Lawyer Relationship, Confidentiality of Information):[5]

3 see ***For Comment: Issues Paper Concerning Client Confidentiality and Lawyers' Use of Technology***, ABA Commission on Ethics 20/20 Working Group on the Implications of New Technologies, September 20, 2010 http://www.abanet.org/ethics2020/pdfs/clientconfidentiality_issuespaper.pdf

4 Arizona Ethics Opinion 09-04: Confidentiality; Maintaining Client Files; Electronic Storage; Internet http://www.myazbar.org/Ethics/opinionview.cfm?id=704 and North Carolina Proposed 2010 Formal Ethics Opinion 7: Subscribing to a Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property http://www.goclio.com/blog/2010/04/nc-proposed-ethics-opinion-on-cloud-computing/

5 ABA Model Rules of Professional Conduct, Client-Lawyer Relationship, Rule 16. Confidentiality Of Information – Comment http://www.abanet.org/cpr/mrpc/rule_1_6_comm.html

> "When transmitting a communication that includes information relating to the representation of a client, the lawyer must take ***reasonable precautions*** to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a ***reasonable expectation*** of privacy." ***(Emphasis added)***

What Constitutes Reasonable Precautions for Cloud Computing?

It's impossible to dictate global guidelines for what constitutes "reasonable precautions" in regards to cloud computing and SaaS. The State Bar of California Proposed Formal Opinion Interim No. 08-0002 (Confidentiality and Technology[6]) states that it "will depend on the technology being used and the circumstances surrounding such use."

Most lawyers who store their clients' data in the confines of their office would vow they are taking reasonable precautions to protect confidential data. But in reality, most law offices are pitifully deficient when it comes to protecting confidential electronic data, especially when compared to the extraordinary security found in the cloud's data centers.

For example, many "secure" servers found in law firms are located in un-locked broom closets accessible by anyone from building maintenance to cleaning crews. Surely a reasonable precaution would be to at least lock the door to restrict physical access. The equivalent of an un-locked door on the digital side would be a server without the latest security patches applied, or lackadaisical oversight on user accounts.

In contrast, most data centers for cloud-based applications are SAS 70 compliant which means they've passed a rigorous set of industry-standard auditing requirements ensuring the strictest levels of digital and physical access.

The Amazon Web Services Security Whitepaper[7] outlines the company's policies for proactive and continuous monitoring, background checks on employees, account access creation & removal, details of round-the-clock, on-premise security and surveillance measures, data destruction methods for end-of-life media, and overall network security. Amazon Web Services has even described how companies are using their cloud for HIPAA-compliant activities.[8]

Most lawyers would be hard-pressed to produce any document at their firm that covers data security, nor would they be able to outline their firm's practices for account creation or data destruction.

Parsing Some Of The Practical Precautions for Lawyers

The State Bar of Nevada's Standing Committee on Ethics and Professional Responsibility issued Formal Opinion No. 33[9] in February 2006 where they directly addressed the question on whether lawyers violate their professional responsibility when they store "confidential client information, without client consent, in an electronic format on a server that is not exclusively in the lawyer's control."

The opinion describes the potential risks:

> "The use of an outside data storage or server does not necessarily require the revelation of the data to anyone outside the attorney's employ. The risk, from an ethical consideration, is that a rogue employee of the third party agency, or a "hacker" who gains access through the third party's server or network, will access and perhaps disclose the information without authorization. In terms of the client's confidence, this is no different in kind or quality than the risk that a rogue employee of the attorney, or for that matter a burglar, will gain unauthorized access to his confidential paper files."

The Nevada Ethics Committee concluded that an attorney may use "an outside agency to store confidential client information in electronic forms" [sic] as long as the attorney exercises reasonable care in the selection of the vendor and there is a reasonable expectation that the information will be kept confidential.

6 The State Bar of California, Proposed Formal Opinion Interim 08-0002 (Confidentiality and Technology) http://calbar.ca.gov/AboutUs/PublicComment/201025.aspx

7 Amazon Web Services: Overview of Security Processes, August 2010 http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf

8 Amazon Web Services, "Creating HIPAA-Compliant Medical Data Applications with Amazon Web Services," April 2009 http://awsmedia.s3.amazonaws.com/AWS_HIPAA_Whitepaper_Final.pdf

9 State Bar of Nevada Standing Committee on Ethics and Professional Responsibility Formal Opinion No, 33, February 9, 2006 http://www.nvbar.org/Ethics/opinion_33.htm

How does an attorney exercise reasonable care in selecting a SaaS vendor? The North Carolina Proposed Ethics Opinion[10] has an excellent list of questions that lawyers should ask potential SaaS providers including:

- Has the lawyer read the user or license agreement terms, including the security policy, and does he/she understand the meaning of the terms?
- Does the SaaS vendor's Terms of Service or Service Level Agreement address confidentiality? If not, would the vendor be willing to sign a confidentiality agreement in keeping with the lawyer's professional responsibilities?
- How does the SaaS vendor, or any third party data hosting company, safeguard the physical and electronic security and confidentiality of stored data?

The Proposed North Carolina Ethics Opinion also suggests that lawyers consult with an IT or security professional if they are unable to comfortably determine if the precautions taken by the cloud or SaaS provider are reasonable. This suggestion is echoed in the Arizona Ethics Opinion:[11]

"It is important that lawyers recognize their own competence limitations regarding computer security measures… and consult someone with competence in the field of online computer security."

If the cloud provides more security for confidential data than an un-secured server in a law office, or a lawyer's confidential paper files, then plainly a lawyer is taking all reasonable precautions to protect data when they use a secure cloud-based service. The important caveat is that the lawyer must utilize reasonable care in selecting the SaaS provider which includes asking questions, becoming competent in the necessary technology, and consulting with an IT or security professional.

#2 The Cloud Affords a Higher Standard of Privacy for Communication than E-mail

Does interaction and communication with the cloud provide a "reasonable expectation of privacy?" We can look to e-mail for a precedent.

In 1986, the ABA issued a report cautioning lawyers against electronic client communications and concluded that an attorney should not communicate with clients electronically without first obtaining the client's informed consent or being reasonably assured of the security of the electronic system in question.[12]

Today, the practice of law would slow to a crawl if every lawyer had to obtain client consent to communicate with them via e-mail. E-mail has become the standard for client communication and even the preferred method for efficient delivery of confidential documents.

But the transmission of un-encrypted e-mail is woefully insecure, and actually travels through multiple servers across the Internet before it reaches the intended recipient. Why aren't lawyers required to encrypt e-mails to prohibit unintended recipients from reading the plain text of an e-mail? Granted, encryption would require multiple layers of added complexity, but wouldn't that constitute a reasonable precaution for adequately protecting the confidentiality of the message?

Fortunately, lawyers are not required to encrypt e-mails because the ABA opined in 1999 that un-encrypted e-mail communication carries a reasonable expectation of privacy from "both a technological and legal standpoint."[13] The view is shared among the states.[14]

In fact, ABA Formal Opinion No. 99-143 states:

> "The Committee believes that e-mail communications, including those sent unencrypted over the Internet, pose no greater risk of interception or disclosure than other modes

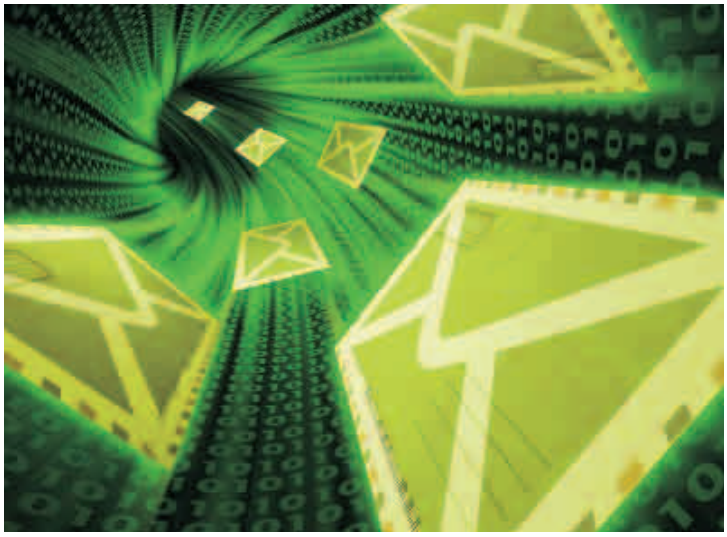
10 North Carolina Proposed 2010 Formal Ethics Opinion 7: Subscribing to a Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property
http://www.goclio.com/blog/2010/04/nc-proposed-ethics-opinion-on-cloud-computing/

11 Arizona Ethics Opinion 09-04: Confidentiality; Maintaining Client Files; Electronic Storage; Internet
http://www.myazbar.org/Ethics/opinionview.cfm?id=704

12 ABA Committee of Lawyers' Responsibility for Client Protection, L***awyers on Line: Ethical Perspective in the Use of Telecomputer Communication (1986)*** - see State Bar of Nevada Standing Committee on Ethics and Professional Responsibility Formal Opinion No, 33, February 9, 2006
http://www.nvbar.org/Ethics/opinion_33.htm and Nancy Blodgett, "Computer Ethics – Interstate Practice On The Line," ABA Journal, March 1, 1986, Volume 72, Page 17
http://bit.ly/ABAJournalMarch1986

13 ABA Formal Opinion No. 99-143 - Protecting the Confidentiality of Unencrypted E-Mail, March 10, 1999
http://www.abanet.org/cpr/pubs/fo99-413.html

14 see Legal Ethics and Technology: Confidentiality, ABA Legal Technology Resource Center
http://www.abanet.org/tech/ltrc/research/ethics/confidentiality.html



of communication commonly relied upon as having a reasonable expectation of privacy."

If un-encrypted, un-secured e-mail communications are deemed sufficient to provide a reasonable expectation of privacy, then surely cloud-based services surpass this standard when they actually ***insist*** on utilizing encryption for all communication and data transfers.

When you log on to a cloud-based SaaS application, your Web browser's address bar adds an "s" to http://". The "https://" indicates that everything you type and view from that point forward is being transported over the Secure Sockets Layer (SSL) protocol. This is the same technology that protects your credit card number when you hit the "Checkout" button at Amazon.com.[15]

All a lawyer needs to do is select a strong password and keep it confidential. This is a simple assignment, yet so many lawyers unashamedly use a simplistic, easy-to-guess password. Is your password "123456" or "654321"? Or the name of your spouse, child, or family pet? Or the current month/year such as "january2010"? Or some variant of "password"?

Strong passwords are one of the important, but overlooked, components of cloud security. A strong password is longer than 6 characters and use a combination of letters, symbols, punctuation and numbers.[16] Once you formulate a strong password, do not write it on a post-it note and stick it to your computer monitor or the inside of your desk drawer.

#3 The "Total Cost of Ownership" Analysis Demonstrates that SaaS is a More Economical Investment than Traditional Software

It should be easy to compare the costs of SaaS to traditional software. After all, most cloud-based services charge an ongoing monthly subscription fee while traditional software requires a simple, one-time purchase. The traditional software model would be the clear economical winner if you stopped there.

This naïve assessment, however, fails to account for the true "total cost of ownership" between the purchase of a software product versus paying for a software service.[17]

The "Hidden" Costs Involved With Traditional Software

The initial purchase of a traditional software product (in reality only a license-to-use[18]) is merely the preamble to an on-going catalog of obligatory and indirect costs.

Software is easy enough to install on a single computer, but when you have a small network, or need to configure the software to run from a server, you should consult an IT professional.

Annual software maintenance fees ensure that you'll have access to the latest upgrades, but you're still responsible for scheduling when and how those upgrades are applied. You may also need to pay for a tech support contract if the software company charges extra.

Remote access is also important to your practice, so you'll need to set up a way to securely connect back to the servers and software at your office. This could require more servers, more software, and will certainly require a professional to ensure it's done right.

Last but not least, our country has suffered its fair share of natural and man-made disasters, which means redundant backups of client data and firm software shouldn't even be a question. You'll need more storage for backups and may even need to subscribe to an online backup service.

All of these additional fees and expenses are part of "owning" (licensing), maintaining, and supporting traditional software. They are sometimes called "hidden" or "soft costs," but Gartner estimates that companies spend around 75% of their total IT budget on maintaining and running existing systems and software infrastructure[19] — there's nothing "soft" about those costs.

15 see "10 Things Every Lawyer Should Know About Legal SaaS (Part 4): Security http://www.goclio.com/blog/2009/06/10-things-every-lawyer-should-know-about-legal-saas-part-4-security/ for an excellent visual contrasting data sent with and without SSL.

16 see "Data Accessibility, Security, and Privacy (Part II) http://www.goclio.com/blog/2008/10/data-accessibility-security-and-privacy-part-ii/ with includes a link to an excellent resource for how to create strong passwords from Microsoft: http://www.microsoft.com/protect/fraud/passwords/create.aspx

17 see "10 Things Every Lawyer Should Know About Legal SaaS (Part 7): Total Cost Of Ownership" http://www.goclio.com/blog/2009/06/10-things-every-lawyer-should-know-about-legal-saas-part-7-total-cost-of-ownership/

18 see generally David Kravets, "Guess What, You Don't Own That Software You Bought" September 10, 2010 http://www.wired.com/threatlevel/2010/09/first-sale-doctrine

19 Timothy Chou, The End of Software, SAMS Publishing, 2005, page 6

The Costs of Subscribing To The Cloud

By contrast, every expense listed above is incorporated into the monthly fee of a cloud-based SaaS application. You don't need to buy servers, upgrade software, administer backups, purchase maintenance agreements, pay extra for tech support, or configure remote access — it's all part of the package.

One of the more recent studies analyzing the total cost of ownership of a cloud-based SaaS application and a comparable "on-premise" solution found that the SaaS model was 77% less for 10 users over four years.[20]

Some studies suggest that a return on investment (ROI) for SaaS applications is apparent in 6 months[21], while other studies estimate it takes a little longer at 12 to 24 months.[22]

These ROI studies focus on illustrating how SaaS is a worthy investment in the long run, but the reality is that the entry point is incredibly accessible for solo practitioners and small firms. Signing up for a SaaS application completely eliminates the need for a large, initial outlay of cash for servers, software licenses and consultant fees. And going forward, all of the tech support, upgrades, backups, and maintenance are included in the monthly fee, avoiding the need for future "soft" expenses.

20 Valerie Valentine, "SaaS CPM Costs Less than On-Premise, Study Finds," Information Management, May 10, 2010 http://www.information-management.com/news/saas_cpm_costs_less_than_on_premise-10017837-1.html and full report at http://www.adaptiveplanning.com/docs/Hurwitz_TCO_of_SaaS_CPM_Solutions.pdf

21 Software & Information Industry Association White Paper, "Software-as-a-Service; A Comprehensive Look at the Total Cost of Ownership of Software Applications," September 2006 http://whitepapers.zdnet.com/abstract.aspx?docid=272803 and http://www.winnou.com/saas.pdf

22 Forrester Research Inc. White Paper, "The ROI of Software-As-A-Service," July 13, 2009 http://www.forrester.com/rb/Research/roi_of_software-as-a-service/q/id/53885/t/2 and http://www.docstoc.com/docs/22147200/The-ROI-Of-Software-As-A-Service

#4. Data in the Cloud is Persistently Accessible and Safer Than On Your Laptop

As the Internet continues to proliferate and infiltrate every crevice of our lives, we demand access to our data anytime from anywhere. That's why mobile devices like the BlackBerry, iPhone and iPad are becoming indispensable tools for today's lawyers. Such prolific accessibility has begun to erode the differences between the devices that we use to access the Internet - all you need is a Web browser.

The Web browser is becoming the ubiquitous operating system. It's the platform we use for legal research or to map an address. It's where we read newspapers and check up on friends. It's where we shop, bank, and watch movies. Google even developed their own Web browser (Chrome) to create "a modern platform for web pages and applications."[23]

Some would argue that since SaaS applications are limited to running inside a Web browser, they are partially "walled-off" from interacting with other locally installed software applications such as Microsoft Word, Outlook, etc. This is true in some respects today, but it is rapidly changing as Web browsers get more powerful and SaaS providers offer "application programming interfaces" (APIs) into their services.[24] Even Microsoft is blurring the line between traditional and cloud-based versions of their Office software.[25]

What If The Internet Goes Down?

To effectively use a Web browser and a cloud-based SaaS application, you must be connected to the Internet. So what happens when you can't connect to the Internet?

Fortunately, connectivity is becoming more pervasive every day, but skeptics will not allow the question to fade. Everyone is vulnerable to connectivity interruptions whether your data lives in a local storage bubble or across the nation. Ross Kodner puts it this way: "digital bad days blacken all doorsteps… [but] if the world's largest corporations can place their trust in wildly successful and field-proven SaaS products such as Salesforce.com, legal SaaS systems will become just as trustworthy."[26]

If your Internet connection went down today, how would you send or receive e-mail? Hasn't e-mail become a critical communication tool in your practice?

How would you conduct research without the Internet? Do you still have a physical law library?

23 see The Official Google Blog, "A fresh take on the browser," September 1, 2008 http://googleblog.blogspot.com/2008/09/fresh-take-on-browser.html

24 see "Clio Announces Google Apps Integration, Joins Google Apps Marketplace" http://www.goclio.com/blog/2010/10/clio-announces-google-apps-integration/

25 Ina Fried, "Microsoft Office 265 best on the cloud," October 19, 2010 http://news.cnet.com/8301-13860_3-20020029-56.html

26 "SmallLaw: Ending the SaaS Stalemate in the Small Firm Market," TechnoLawyer SmallLaw column, March 8, 2010 http://blog.technolawyer.com/2010/03/smalllaw-saas.html

How would you look up phone numbers without the Internet? Send text messages? Check sports scores? Read news? Catch up on Facebook gossip?

The Internet isn't going anywhere. There will always be interruptions, but you already have essential and critical aspects of your law practice that require an Internet connection today. Subscribing to a cloud-based SaaS application won't make the Internet any ***more*** critical to your practice than it already is.

Accessing Your Data When The Unthinkable Happens

Let's turn the question around: If you hoard confidential data on your computer for fear of not being able to connect to the Internet, what happens to that data in the event of a disaster or loss or theft?

Reports indicate that 10% of laptops used by American businesses are stolen during their useful lives and 97% of them are never recovered.[27] An August 2007 study by the Ponemon Institute reported that 70% of data breaches results from the loss of "off-network" equipment.[28] A report sponsored by Dell found that over 12,000 laptops per WEEK are lost JUST in U.S. airports.[29] That doesn't account for the thousands of mobile devices left in cabs, coffee shops and elsewhere.

With those staggering numbers, why aren't lawyers required to encrypt and more severely protect the data located on their laptops and mobile devices? Un-encrypted confidential data on a stolen or lost laptop is at the most extreme risk of falling into the hands of an unintended recipient.[30]

Cloud data centers provide multiple and geographically disperse layers of backup and redundancy capabilities that most law firms could never afford or imitate. Confidential data located in the cloud is always available after the loss or theft of a laptop. The cloud grants you and your clients the assurance that data is consistently backed up and accessible from any computer connected to the Internet (even one you have to borrow).

Cloud-based practice management provider Clio has even gone a step further by offering a unique "data escrow" service which uses an independent third-party to securely archive data in the unlikely scenario that the Clio service is unavailable for a disastrously long time.[31]

#5. The Cloud Offers a Refreshingly Simple and Usable Option in Today's Sea of Bloated Software

A common argument against cloud-based SaaS applications is that the list of features is usually dwarfed by those found in comparable traditional software products.

But is this really a ***DIS***-advantage? With traditional software, there's always that nagging feeling that if you just had more time to learn to use the software better, you could be so much more productive. And every time that you finally master a task in your traditional software, another feature supersedes your efforts.

Comprehensive feature sets certainly sound attractive on the surface, but come at the cost of increased complexity and steeper learning curves. The fact that SaaS providers are "limited" to providing a core functionality is actually a benefit. Perhaps the "less is more" concept is appropriate here, in that the "less" you have to worry about in using software, the "more" you can focus on your practice instead of getting frustrated by technical logistics.

Lassoing the Cloud

Once you unsnarl the issues around confidentiality, accessibility, security, encryption, and cost, it ultimately comes down to a personal comfort level — are you comfortable with your data and your clients' data being stored in the "cloud?" More importantly, are your clients comfortable with it? Actually, would your clients even care?

27 see David Ries and Reid Trautz, "Securing Your Clients' Data While On the Road," Law Practice Today, October 2008 http://www.abanet.org/lpm/lpt/articles/tch10081.shtml

28 see "Off-Network Security: A Crisis at Hand" http://www.redemtech.com/ponemon-study.aspx

29 "Airport Insecurity: The Case of Missing & Lost Laptops," June 30, 2008 http://www.dell.com/content/topics/global.aspx/services/prosupport/en/us/exec_summary

30 see Section I(C) in For Comment: Issues Paper Concerning Client Confidentiality and Lawyers' Use of Technology http://www.abanet.org/ethics2020/pdfs/clientconfidentiality_issuespaper.pdf

31 see "10 Things Every Lawyer Should Know About Legal SaaS (Part 6): Data Availability http://www.goclio.com/blog/2009/06/10-things-every-lawyer-should-know-about-legal-saas-part-6-data-availability/

Most lawyers are not comfortable with the cloud… yet. It's difficult to comprehend that your data can be safe even though you can't see or touch the server it's stored on. You can argue that your clients' data is safe and secure on your own equipment, but you can never provide the level of physical and digital security offered by cloud vendors.

The reality is that you're already using the cloud, and so is everyone else. Twenty-five years ago, it was impossible for lawyers to fathom they would electronically communicate with their clients — they certainly would never use such an insecure method of communication to transport confidential documents. And today, it's rare to find a lawyer that is not using e-mail. "Cloud computing" will become as accepted and expected as e-mail, and we'll wonder why we even thought otherwise.

About Brett Burney

Brett Burney is Principal of Burney Consultants LLC, and focuses his time on bridging the chasm between the legal and technology frontiers of electronic discovery. Brett is also very active in the Mac-using lawyer community, working with law firms who desire to integrate Mac and iOS devices into their practice. Prior to establishing Burney Consultants LLC, Brett spent over 5 years at the law firm of Thompson Hine LLP where he worked with litigation teams in building document databases, counseling on electronic discovery issues, and supporting them at trial. Brett graduated from the University of Dayton School of Law in 2000 and quickly became active in the world of legal technology. Brett is a frequent contributor to Law.com and speaks around the country on litigation support, e-discovery and Mac-related topics. You can email him at burney@burneyconsultants.com.