The Ethics and Security of Cloud Computing

The Ethics and Security of Cloud Computing

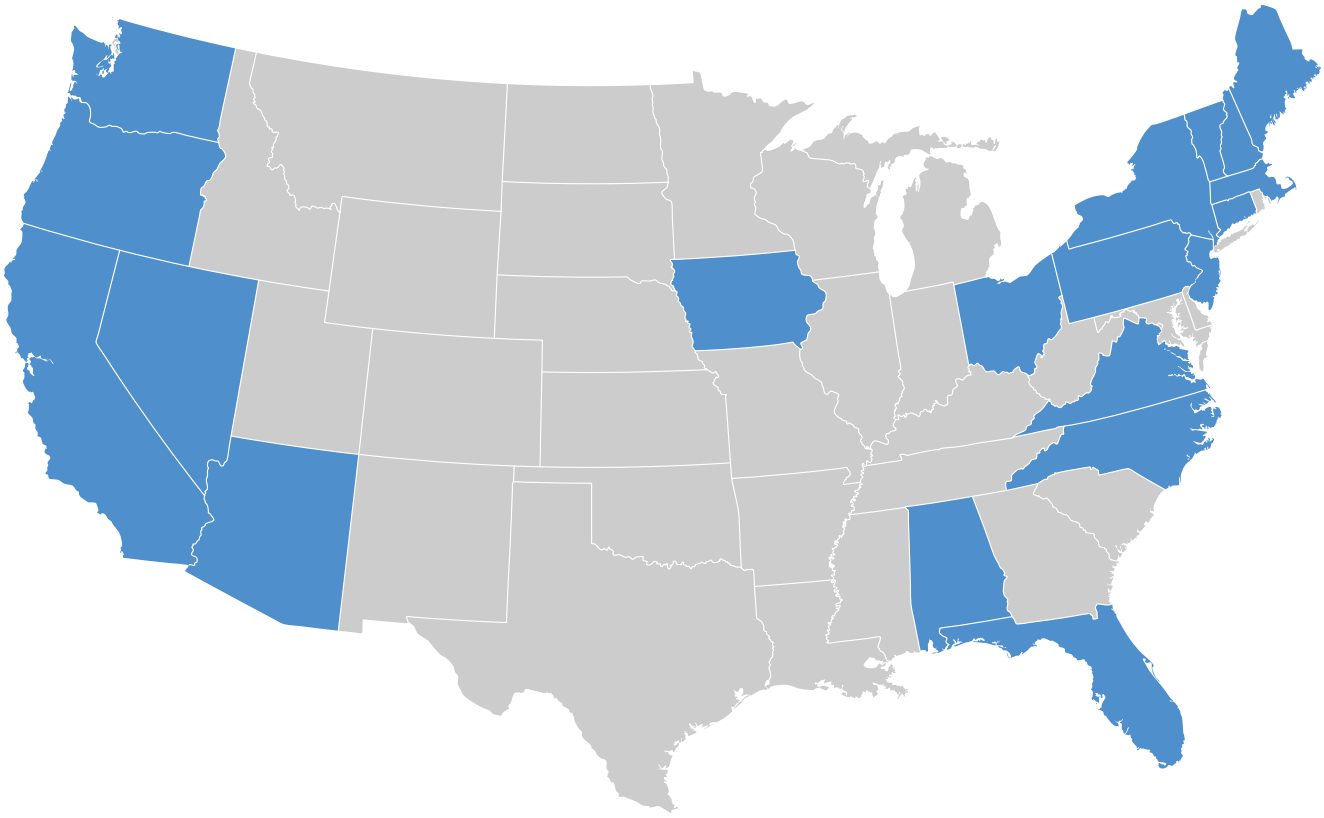
Nearly four thousand years ago, Hammurabi engraved the laws of Babylon onto a stone plinth and revolutionized the codification of law. Today, lawyers of all walks of life are engaged in a new revolution, with the ability to practice law armed with nothing more than a tablet device and an internet browser—a revolution brought about, in large part, by the rise of cloud computing.

The shift from desktop- and server-based software to software as a service (SaaS) or "cloud computing" is one of the most significant transitions in business to occur in the last 20 years. While the benefits offered by cloud computing are numerous, several outstanding questions remain for legal practitioners regarding the relative security of cloud-based systems as compared to traditional, on-premise solutions. In the context of a law firm, the use of cloud computing raises ethics issues around storing confidential client data on a system that the lawyer may not own or otherwise control.

The discourse on the ethics of cloud computing took a significant step forward with a Formal Ethics Opinion (FEO) on cloud computing by the North Carolina State Bar in 2012. This was one of the first FEOs in North America to explicitly deal with the use of SaaS and cloud computing in a law firm. While the FEO ultimately endorses the use of cloud computing technology in a law firm provided that "reasonable care is taken effectively to minimize the risks to the confidentiality and to the security of client information and client files," the onus of evaluating a cloud provider's security infrastructure is placed on the law firm.

Subsequent to the FEO from the North Carolina State Bar, 19 states have adopted similar opinions on SaaS and cloud-computing. All 19 permit the use of cloud technologies in the practice of law, with specific requirements or recommendations. These should be addressed by the Terms of Service (ToS) implemented by SaaS and cloud providers.

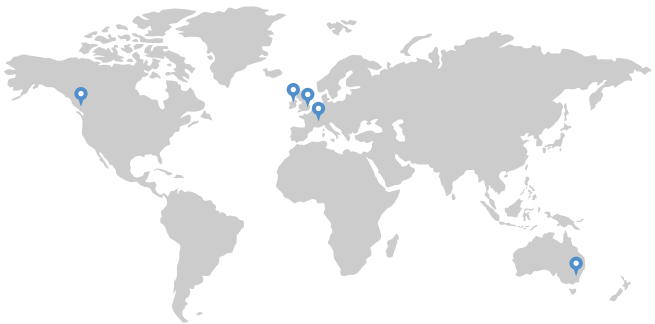
States with a Cloud Ethics Opinion

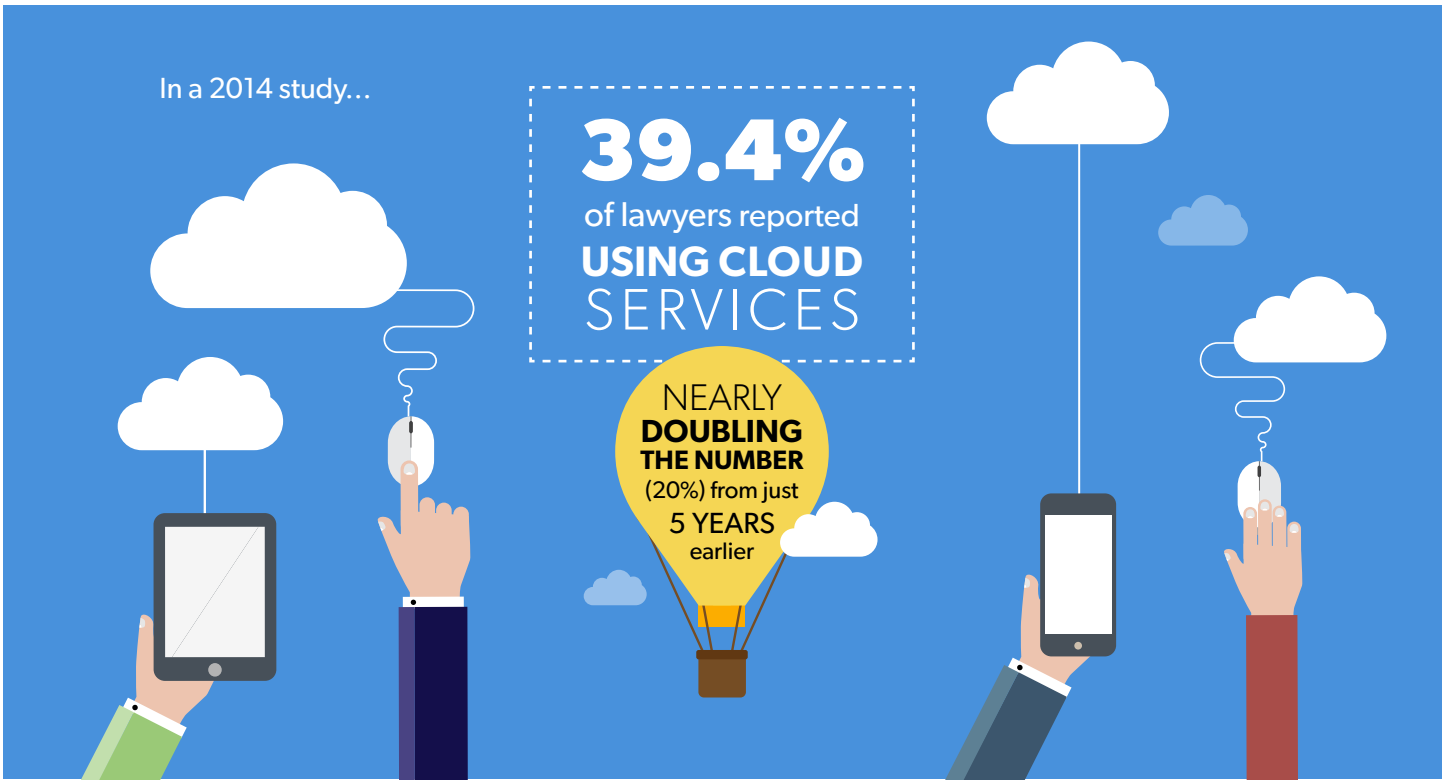


- Alabama
- Arizona
- California
- Connecticut
- Florida
- Iowa
- Maine
- Massachusetts
- New Hampshire
- New Jersey
- New York
- Nevada
- North Carolina
- Ohio
- Oregon
- Pennsylvania
- Vermont
- Virginia
- Washington

Other Jurisdictions:

- British Columbia, Canada
- Council of Bars and Law Societies of Europe
- England and Wales
- New South Wales, Australia
- Scotland



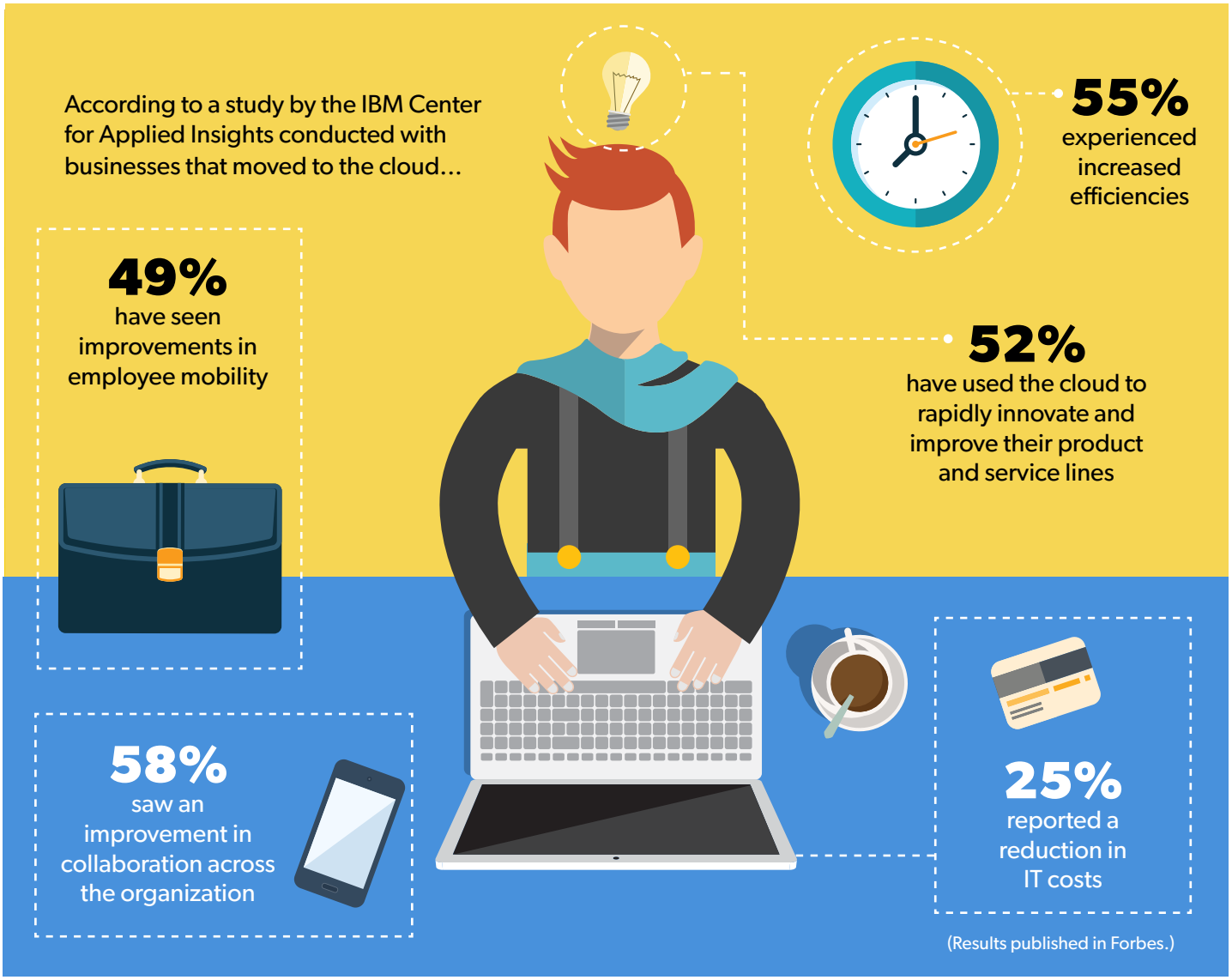


Cloud Computing

Cloud computing is computing delivered as a service over the Internet, accessible via any internet-connected device with a web browser. Increasingly, it matters less and less which device you use to do your work; your documents, email messages, media, other types of information will be stored and securely accessed online. The shift to cloud-based services typically offers increased security and dramatically reduced overhead and IT costs as compared to on-premises servers and software.

While the concept of practicing in the cloud may seem novel, most web-savvy computer users have been using cloud-based technologies for a number of years via longstanding services such as email providers (Gmail or Hotmail), storage providers (Dropbox or Box.com), or photo-sharing services (Flickr, Photobucket), among others. These technologies were among the first to pioneer the idea of centralized services delivered efficiently over the Web, and they have succeeded in laying the groundwork for a software revolution that is gradually leading most applications to evolve toward a web-based mode of delivery.

As of 2015, adoption of cloud services has become the new normal for many businesses, extending well beyond email services. Bank and financial institutions employ cloud technologies to allow customers to access account and investment information. Architects and engineers use cloud technologies to collaborate on projects. Marketing and sales professionals rely heavily on SaaS providers such as Salesforce, Marketo, and HubSpot, all of which contain sensitive company and customer data. And professional services organizations such as accountants, doctors, and dentists use the cloud to manage confidential client and patient information. In fact, in October of 2014, PwC, one of the global Big Four accountancy and audit firms, **announced a groundbreaking partnership** with Google to move their operations to the cloud, bringing 45,000 accounting professionals in the United States and Australia into the realm of cloud computing.



Benefits of Cloud Computing

The benefits of moving traditional desktop- and server-based applications to the cloud are numerous for firms of all sizes. Cloud-based services typically eliminate large up-front licensing and server costs, offer drastically reduced consulting and installation fees, and do away with the "upgrade treadmill" usually associated with traditional desktop- and server-based software. Cloud-based services also offer "anywhere accessibility," a high level of ease-of-use, and compatibility with both Windows and Mac.

And with the rise of mobile technologies, cloud and SaaS applications are now almost universally available on smartphone and tablet devices, meaning that business professionals, including legal practitioners, have free reign to work from virtually anywhere.

Ethics of Cloud Computing

In the context of a law firm, cloud computing raises concerns associated with entrusting a third party with confidential client data. Ohio's Informal Advisory Opinion 2013-03 outlines the primary concerns in law firms using cloud computing:

"The issues and ethical duties regarding cloud storage are analogous to the ones that apply when lawyers opt to use a vendor to store their paper files offsite rather than in their own offices. The analogy to paper files can help lawyers as they exercise their professional judgment in adopting specific practices that address new storage technologies such as "the cloud." That process of exercising individual judgment would not be overly assisted by overly-detailed regulatory input from this Committee. As one state bar ethics committee noted, a lawyer "has always been under a duty to make reasonable judgments when protecting client property and information. *Specific practices regarding protection of client property and information have always been left up to individual lawyers' judgment, and that same approach applies to the use of online data storage,*" subject as always to the relevant conduct rules." Adv. Op. 2215, 2 (Wash. St. Bar Rules of Prof' 1 Cond. Comm. 2012) (emphasis added)."

Lawyers considering cloud computing need to understand the technologies and practices that both the provider and they themselves can leverage to effectively minimize the risks. The following provides an in-depth look at the technologies and best practices that can be employed to effectively minimize risks related to using cloud computing.

Data Security

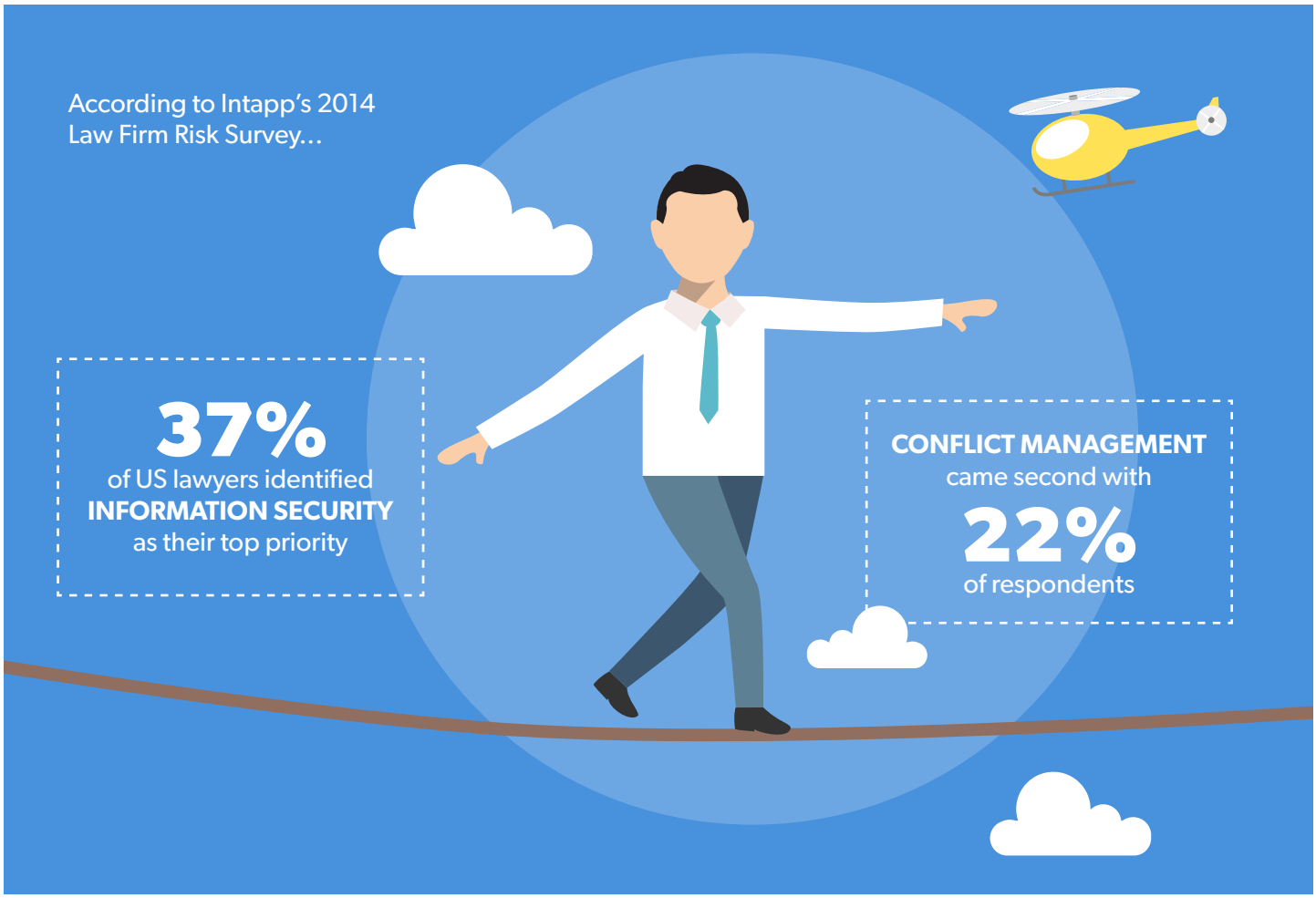
Data security covers four primary areas: encryption, server security, client security, and password security.

Encryption

One important component of the security equation is encryption. Secure Sockets Layer (SSL) is an industry-standard encryption technology that enables secure online banking and e-commerce. SSL ensures all communications between your computer and the cloud-based server are encrypted and protected from interception. SSL is an extremely powerful technology, as it allows for completely secure communications even over public, untrusted networks, such as a public Wi-Fi connection. Each Web browser uses a variant of a "lock" icon to indicate a website is using an SSL connection—look for it prior to inputting any confidential data on a website.

Server Security

While SSL helps secure communications between your computer and the cloud, you also need to know that the servers you are communicating with are properly secured against hackers and other threats. While it is hard for the average web user to assess a cloud-based provider's server security, there are services from companies such as McAfee that perform regular security audits on SaaS providers to ensure server security. Ask for evidence of a third-party security audit, be it from McAfee or another provider, before entrusting your data to a cloud-based provider.



Client Security

Though cloud computing has the advantage of outsourcing server-level security and backup to a third-party service provider, one oft-overlooked part of the security equation is the security of the desktop or laptop from which you are accessing the SaaS application. SaaS doesn't obviate the need to ensure your desktop or laptop is properly secured with a firewall, antivirus protection, and the latest security updates for your operating system and web browser. For Windows users, Google Pack offers free antivirus, anti-spyware, and Google's own web browser, Chrome.

To ensure data stored on your desktop or laptop remains private even if it is stolen, you may want to look at utilizing BitLocker (Windows) or FileVault (Mac), native encryption options that come pre-installed on most modern computers.

Password Security

Finally, security also encompasses password security. The best SSL encryption and client/server security can all be undone by the choice of a weak password. Be sure to choose a secure password for any website you are using, and try to avoid using a given password for more than one website. A number of free password generator and manager exist, such as PasswordSafe (passwordsafe.com), Passpack (passpack.com), or LastPass (lastpass.com).

Data Privacy

The following questions provide a summary of some important considerations when evaluating a cloud-based provider:

What is the privacy policy?

Policies should be clearly stated and disclose how information supplied to the service is housed, protected, shared, manipulated or disposed of.

Who owns the data?

When entrusting your practice to a SaaS solution, it's critical to understand the impact of the company's privacy policy on the lawyers' ethical requirements as legal practitioners.

How can the data be used?

When it comes to confidential client information, the privacy policy generally outlines how the cloud computing provider can (or cannot) use the data you enter into the application. In general, all information you enter into a cloud computing application should be treated as confidential, private information that cannot be used by the cloud computing provider. Furthermore, the cloud computing provider should only be permitted to view any of your private information with your explicit consent (for example, to troubleshoot a technical issue).

While in many cases this seems to be the only obvious and fair way of treating private data, there have been some high-profile cases of very popular websites imposing less-than-fair privacy policies on their users. For example, Facebook recently caused a virtual firestorm with an update to its privacy policies that apparently granted the company perpetual control over content posted by its users.

Data Availability

The importance of cloud-based providers' data availability strategies cannot be overstated—and IBM has taken note. It recently opened a "cloud resiliency center" in North Carolina with the aim of protecting businesses from potential disasters related to storing data in the cloud. "Open 24 hours a day, seven days a week, the resiliency center team will monitor developing disaster events and then mobilize as needed to ensure that the infrastructure for all customers is configured to handle the latest threats to keep data, applications, people and transactions secure." As long as an appropriate strategy is in place, SaaS applications can arguably provide a much higher level of data availability than desktop applications.

By asking a cloud computing provider about their data availability strategy, you are essentially seeking an answer to this very important question: What are you doing to ensure that my data remains available, even in the event of a natural or human-induced disaster?

The types of disasters that need to be contemplated in a data availability strategy are numerous. Natural disasters could range from a lightning bolt that causes a simple power outage at one data center to an earthquake that wipes out power for an entire state. Human-induced disasters could include a simple network misconfiguration or a situation where the SaaS provider must shut down for any number of issues related to business continuity.

Although many of these scenarios are extremely unlikely, the value of the data that is being stored should require a comprehensive plan to mitigate the risk associated with potential disaster scenarios. Luckily, there are a broad range of extremely effective technologies and techniques available to both SaaS providers and end users to ensure that their data is safe and secure:

Geographic Redundancy

If a SaaS application's data is hosted in just one data center, this means there is a single point of failure that could, potentially, make the entire application unavailable. Geographic redundancy, or geo-redundancy, takes advantage of multiple, geographically distributed data centers. The impact of an outage at one data center can thus be minimized by automatic failover to additional data centers.

SaaS Provider Backups

The SaaS provider should, at a minimum, be performing daily backups of all data and storing this backup in a secure, offsite location. Ideally, backups should be performed multiple times per day and replicated to multiple, secure offsite locations.

User Backups

As a risk-mitigating precaution, making regular backups of your data from the SaaS provider is a good strategy. Additionally, some bar associations require that their members retain on-premises copies of their practice's data. Ensure your SaaS provider allows for a full export of your data from their system.

Data Escrow

While SaaS- and user-level backups provide an extremely high level of protection against data loss, other scenarios (such as the SaaS provider going out of business) should be assessed. While in many cases this is an extremely unlikely scenario, it is one that lawyers have the fiduciary duty to plan contingencies against.

Conclusion

These measures, taken together, make data availability one of the most compelling advantages of cloud computing over traditional desktop applications. To achieve an equivalent level of data availability with desktop applications would be cost-prohibitive and technically challenging, whereas cloud-based providers can leverage economies of scale to make this kind of infrastructure available to users for a low monthly cost. For lawyers in geographic locations exposed to a high risk of natural disasters, such as hurricanes or earthquakes, cloud-based applications can provide a compelling solution to the problem of data availability, as the cloud-based application will remain accessible even if the firm's offices are inaccessible or damaged.

With the adoption of the above best practices and risk-minimization strategies, your data can be trusted to the cloud with an extremely high degree of privacy, security, and availability. It is encouraging that the FEOs from the 19 state bars previously listed echo this assertion, having concluded that cloud-based services are acceptable for legal practice, provided that reasonable care is exercised to ensure appropriate technologies are being leveraged to protect client privacy and confidentiality. The pragmatic opinion issued by the North Carolina State Bar in 2012 has continued a precedent that has since been more or less adopted by 18 other states. This is likely to be considered the guiding principle by which other bar associations and regulatory bodies refer to, as they formalize and standardize their stances on the use of cloud-based technologies in legal practice.

Cloud Computing Due Diligence Checklist

☐ Terms of Service

- Does the cloud computing provider have a clear and accessible Terms of Service and Privacy Policy?
- What uptime does the vendor guarantee as part of their Service Level Agreement?
- Is there an initial setup fee?
- Is there a cap or limitation on the cloud provider's ability of service? (bandwidth caps, storage limits, etc)
- Are there additional usage or bandwidth fees?

☐ Confidentiality

- Does the cloud provider recognize and agree to abide by the duties of lawyer/client confidentiality?
- Does the cloud computing provider explicitly recognize your ownership of any intellectual property stored with the provider?
- Does the cloud provider have a strong contractual obligation to notify you of any demands for client information in time for you to intervene?
- Are features available to provide user authentication and prevent unauthorized access? (Ex: Two-factor authentication, IP monitoring, strong password requirements)

☐ Backup of Data

- Are you able to easily retrieve your data from the cloud computing provider?
- Are you able to maintain a local backup of your data?
- Is the retrieved data in a usable, non-proprietary format?

☐ Reasonable Security

- Does the cloud provider have technology built to withstand a reasonably foreseeable attempt to infiltrate data, including penetration testing?
- Does the cloud provider employ encryption during transmission of your data?
- How often does the cloud provider have their security audited?
- Will the provider allow the law firm to obtain copies of any security audits performed?
- Does the cloud provider offer remedies in the event of data breaches and service availability failure?

☐ Geolocation

- Where are the cloud provider's servers located?
- Does the cloud provider have multiple storage locations—and if so, how often are they synced?

☐ Termination of Services

- Are there any additional costs or penalties for terminating the cloud computing service?
- Can your data be sanitized from the cloud provider in the event of termination?

☐ Additional Considerations

- Does the cloud provider integrate with your other office systems?
- Have you evaluated the cloud provider's history, including how long the provider has been in business, and funding and stability?