Guidelines for the Use of Cloud Computing in Law Practice

From: eLawyering Task Force, Law Practice Management Section, American Bar Association

Introduction

Cloud computing has made its way into the practice management of many law firms. Cloud computing applications currently used by law firms range from simple administrative tools to full scale collaboration, case management applications, and complex legal applications such as web-enabled document automation, mini-expert systems, automated web advisors. From online legal research databases to efiling, the use of cloud computing by legal professionals is relied upon as part of the legal professional's technology toolkit. However, a law firm using cloud computing, as with any practice management software, must weigh the benefits of its use against the risks. By choosing to use cloud computing, the firm must find ways to minimize the risks that may arise from this form of technology in practice management.

Accordingly, an attorney using cloud computing in their law practice should have an understanding of 1) the nature of the law firm's relationship with the cloud computing software provider, and 2) best practices for the use of the cloud computing applications.

This document provides recommended guidelines for understanding both of these components necessary for the ethical use of cloud computing in law practice.

In addition to these guidelines, the attorney should consult with his or her state bar's rules and regulations related to cloud computing or electronic or third-party storage of law office data.

Researching the cloud computing software provider

Before beginning to research, understand current cloud computing and SaaS industry standards and become familiar with the terminology. For example, see the Cloud Security Alliance (http://www.cloudsecurityalliance.org/). See also ABA Legal Technology Resource Center "FYI: Software as a Service (SaaS) for Lawyers" (http://www.abanet.org/tech/ltrc/fyidocs/saas.html).

It is also important to make a distinction between “virtualization” and “cloud computing.” Not all cloud computing applications are based on “virtualization” architecture, but any kind of virtualization depends on cloud computing technologies.

Virtualization is the creation of a virtual (rather than actual) version of something, such as an operating system, a server, a storage device or network resources. Virtualization is a computing technology that enables a single user to access multiple physical devices. This paradigm manifests itself as a single computer controlling multiple machines, or one operating system utilizing multiple computers to analyze a database. Virtualization is about creating an information technology infrastructure that leverages networking and shared physical IT assets to reduce or eliminate the need for physical computing devices dedicated to specialized tasks or systems.

Cloud computing is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet. Through cloud computing, a world-class data center service and collocation provider offers managed IT services through a hosted or "Software as a

Service (SaaS)" model. A server or database can be physically located in a highly-secure, remote location while the data is accessed from a client's computer, using the database's server to retrieve, sort, and analyze the data. This arrangement eliminates the need for a costly in-house IT department and hardware and the associated capital expense. Instead, a cloud computing provider owns the hardware while providing hosted, managed services to its clients on a usage basis.

Cloud computing generally utilizes virtualized IT resources such as networks, servers, and computing devices, so these best practices apply to both the use of cloud computing and "virtualization" which can be viewed as a cloud computing architecture.

Here is a more precise clarification of the meaning of the terms used in these guidelines.

1. There are two published definitions of cloud computing:

The NIST is working on their version and The Gartner Group is working on one of their own.

- NIST – On-demand self-service, Ubiquitous network access (internet standards based), location independent resource pooling, rapid elasticity, and measure/metered service.

- Gartner – service-based, scalable and elastic, shared, metered by use, and uses internet technologies

2. Virtualization

Virtualization is the use of virtual machines to let multiple network subscribers maintain individualized desktops on a single, centrally located computer or server. The central machine may be at a residence, business or data center. Users may be geographically scattered but are all connected to the central machine by a proprietary local area network (LAN) or wide area network (WAN) or the Internet.

In either case, a third-party hosting company, not a specific software vendor, may be responsible for the security of any data placed in the cloud. If your software provider has a relationship with a third-party hosting company that covers the servers, support and/or maintenance of your law office data, understand these relationships when considering the terms covered in the software provider's service level agreement (SLA). The agreement between the law firm and the software services providers should incorporate key terms between the software provider and the third-party hosting company that deal with the support, and the confidentiality and maintenance of law firm data. Review the provider's Service Level Agreement (SLA) and understand how the following issues are addressed:

1. Make sure there are data return and retention policies. Return of data should be in a readable format and within a reasonable amount of time upon request.

2. Understand how the provider would handle government and civil search and seizure actions if handed a subpoena to deliver the contents of your law office.

3. Check for geo-redundancy of the servers or if there is data escrow offered through companies with servers located overseas. Servers located outside of the United States may be subject to international laws. Make sure that the servers are housed in Tier4 data centers.

4. Make sure the provider's services are in compliance with Federal Regulations. For example, make sure the service is Peripheral Component Interconnect (PCI) compliant if the provider will be collecting credit card information.

5. Look for a clear definition of the "use of the service" as it relates to the following: server memory, CPU time, hard drive space, growth of storage space used, "reasonable use" of the network, including computer hardware, network servers, and/or any third-party computer software programs used by the provider to host the service.

6. Understand how backups, maintenance and updates to the service are handled. Data should remain encrypted and only decrypted with the permission of the attorney. Does the provider conduct regular security audits? How often are data backups conducted?

7. Who has access to the law office data? Look for confidentiality, privacy policy and nondisclosure statements.

8. Consider whether the software services provider maintains an Internet Media policy that insures against data loss. The malpractice policy of the law firm may not provide coverage for data loss, and to secure a separate policy for this kind of coverage may be prohibitive, particularly for solo practitioners and small law firms. It is easier for the service provider to secure this coverage and spread the cost over all of the law firm clients they are servicing. The attorney is always responsible for keeping a client's data confidential and has financial exposure if it is disclosed, even if the disclosure is inadvertent. A claim against the software services provider for data loss that is covered by an insurance policy would mitigate the financial impact on the law firm.

Recommendations for Cloud Computing Best Practices

Because the security and standards for cloud computing change on a regular basis, it is not productive to list specific or technical requirements that would quickly become outdated. Instead, the following are basic recommendations to ensure that a law firm using cloud computing in their law practice is able to keep up with the technology to use it for the benefit of the firm and its clients.

1. Keep up to date on the security issues related to the use of the technology chosen for the law firm. Designate an attorney at the firm who is responsible for this task or retain the services of an IT consultant familiar with implementing cloud solutions in a law firm environment.

2. Consider establishing a law firm policy covering the best practices for use of cloud computing applications by firm members, including the firm's use of online social media applications.

3. Attorneys using cloud computing applications on mobile devices, might follow these basic security tips:

- If you use wireless networking, ensure that all wireless traffic is encrypted with WPA2.
- Keep antivirus software and all software patches updated. Turn on the software firewall for the computer.
- Use a safer browser, such as Mozilla with the No Script add-on installed, or use another pop-up blocker.
- Avoid free Wi-Fi hotspots when using any cloud computing application remotely. Use a cellular phone modem adapter instead.

4. Never write down usernames and passwords for access to any cloud computing application. Make sure that the passwords you create are strong and change them regularly. If you have a number of passwords, use an application like KeePass to organize them all.

Conclusion

The benefits of cloud computing for law firms are many. The use of cloud computing applications allows the legal professional from the solo practitioner to larger firms to retain the services of full-time IT specialists who handle security, technology maintenance and upgrades. For solos and small law firms, access to complex legal applications at a low cost may only be available over the Internet. Law firms of all sizes that provide a "client portal" for the benefit of their clients, where a lawyer can interact securely with the clients as part of a legal service delivery strategy, by definition requires the use of an internet based platform based on cloud computing technologies. . Attorneys must take individual responsibility for determining whether cloud computing is appropriate as a technology for the law firm. Once implemented, the law firm should commit to best practices for ethical use of cloud computing in their practice.