

Technology eReport



NOV 2009
Vol. 8, No. 4

- [Home](#)
- [Features](#)
- [Columns](#)
- [About GPSolo](#)
- [Feedback](#)

• [Download](#) 

• [Past Issues](#)

Features

- **Is Your Website OK Today? »**
Attracting clients and making favorable impressions.
- **SaaS Security: Can You Trust Your Data in the Cloud? »**
How to pick the right SaaS provider, come rain or shine.
- **Setting Up a Web-Based Virtual Law Office »**
Practical and ethical considerations to address when moving online.

SaaS Security: Can You Trust Your Data in the Cloud?

By Jack Newton

The shift from desktop- and server-based software to what is alternately referred to as “Software-as-a-Service” (SaaS) or “the cloud” is one of the most significant transitions to occur in computing in the last 20 years. Although the benefits offered by SaaS are numerous, there are risks and legal implications of this paradigm shift that should be understood and mitigated by all lawyers considering moving their data into the cloud.

For solos and small firms, the benefits of moving traditional desktop- and server-based applications to the cloud are clear. Cloud-based services typically eliminate large up-front licensing and server costs, offer drastically reduced consulting and installation fees, and eliminate the “upgrade treadmill” typically associated with traditional desktop- and server-based software. Cloud-based services also offer the advantages of “anywhere accessibility,” intuitive ease-of-use, and compatibility with both Windows and Mac operating environments.



Though all software, both desktop and Web-based, is subject to certain issues relating to security, privacy, confidentiality, and data availability gain special relevance with cloud-based services, especially in the context of law practices. Though most bar associations don't yet provide direct guidance or ethics opinions on the usage of cloud-based services, they do advise their members to select a cloud-based provider with due concern for the maintenance of client confidentiality and data security.

For a typical solo or small firm, conducting this due diligence in a buzz-word and acronym-laden field can be daunting. For this reason, this article will endeavor to provide both an introduction to the relevant technologies, as well as assessment criteria for the evaluation of any cloud-based service. If you adopt the best practices outlined below, your data is likely to be *more* secure in "the cloud" than it would be stored on your laptop or on a server in your office.

Data Security

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

Encryption

Secure sockets layer (SSL) is an industry-standard encryption technology that enables sufficient security for activities like online banking and e-commerce. SSL ensures that all communications between your computer and the cloud-based server are encrypted. 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, in an airport, or at Starbucks. Properly encrypted Web browsers use some variant of a "lock" icon to indicate that the website is using an SSL connection—look for that lock prior to inputting any confidential data into a website.

Server Security

Although SSL helps secure communications between your computer and the cloud, you also need to know the servers you're communicating with are properly secured against hackers and other threats. Though 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 that server security. Ask for evidence of a third-party security audit from McAfee or another reputable provider before entrusting your

data to a cloud-based service.

Client Security

Though SaaS provides the advantage of handling server-level security and backup through a trusted third-party service provider, one often-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 software, and the latest security updates for your operating system and Web browser. For Windows users, Google Pack (www.pack.google.com) offers free antivirus, antispyware, and Google's own Web browser, Chrome.

To ensure data stored on your desktop or laptop remains private even if your machine is stolen, you may want to look at installing TrueCrypt (<http://www.truecrypt.org>) a free, open-source tool which will encrypt the entire contents of your hard drive.

Password Security

Finally, looking at 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're using, and try to avoid using the same password for more than one website. A great free password generator and manager is **PasswordSafe** (<http://www.passwordsafe.com>).

Data Privacy

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

What is the SaaS provider's 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 data to a SaaS solution, it's critical to understand the impact of the company's privacy policy on your ethical requirements as a legal practitioner.

How can the data be used? When it comes to confidential client information, the privacy policy generally outlines how the SaaS provider can (or can't) use the

data you enter into the application. In general, all information you enter into a SaaS application should be treated as confidential, private information that can be used by the SaaS provider. Furthermore, the SaaS provider should only be permitted to view any of your private information with your explicit consent (say, for example, to troubleshoot a technical issue).

Although 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 a cloud-based provider's data availability strategy cannot be overstated. Although catastrophic data loss (such as that which occurred recently at Danger, a division of Microsoft) understandably justifies concern over entrusting important data to the cloud, in the vast majority of cases SaaS providers are going to extraordinary lengths to ensure the quality and persistence of their customer's information. Backups should be performed multiple times per day at regular intervals, tested for validity, and geographically distributed to ensure protection from natural or localized catastrophe. Provided such measures are in place, SaaS applications can arguably provide a much higher level of data availability than desktop applications, simply by virtue of the fact that the core function of the SaaS provider is to ensure the uninterrupted provision of the service.

In asking a SaaS provider about its data availability strategy, you are essentially getting an answer to a 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, or if you go out of business?"

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 region. Human-induced disasters could include a simple network misconfiguration to a situation where the SaaS provider must shut down for any number of business-continuity-related issues.

Although many of these scenarios are extremely unlikely, the value of the data that is being stored should motivate a comprehensive contingency plan to

mitigate the risk associated with the spectrum of potential disaster scenarios. Luckily, there is a broad range of extremely effective technologies and techniques available to both SaaS providers and end-users to ensure that your data is safe and secure. These include:

Geographic Redundancy: If a SaaS application's data are all hosted in a single data center, this means there is a single point of failure that could, potentially, make the entire application unavailable. Geographic redundancy, or georedundancy, leverages several geographically distributed data centers. The impact of an outage at one data center can thus be minimized by automatic backup provided by additional data centers.

SaaS Provider Backups: At minimum, the SaaS provider should be performing daily backups of all data and storing this backup in a secure, offsite location. Ideally, backups should be performed several 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 their members to 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: Although 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. Though in many cases this is an extremely unlikely scenario, it is one lawyers have the fiduciary duty to plan contingencies against.

To help address this concern, at Clio we've established a data escrow policy that is included with subscribership. On a regular basis, we securely archive our data to a completely independent and bonded third party. The data will be held in escrow so that, in the event of an extended service interruption, users taking advantage of our data escrow service can securely retrieve their data from an organization completely independent of Clio.

These measures, taken together, make data availability one of the most compelling advantages of SaaS 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 attorneys in geographic locations exposed to a high

risk of natural disasters such as hurricanes or earthquakes, SaaS can provide a compelling solution to the problem of data availability, as the cloud-based application will remain accessible even if your offices are inaccessible or damaged.

With the adoption of the above best practices and risk-minimization strategies, your data can be trusted to SaaS and “the cloud” with an extremely high degree of privacy, security, and availability.

Jack Newton is president and founder of Themis Solutions, Inc., which created Clio, a SaaS product for solo and small firm attorneys. He can be reached at jack@goclio.com.

© Copyright 2009, American Bar Association.