



Cloud Computing Considerations for Nevada Attorneys

By Jeff Grace and Lizette B. Sundvick

Cloud computing promises to solve a multitude of business problems. Properly implemented, the cloud can provide a higher level of performance and reliability, superior security and scalability, and unprecedented mobility. Naturally, it also carries some inherent risks and raises some legal questions and issues.

Nevada's state bar has issued a formal statement on the potential legal risks of cloud computing for attorneys and law firms, and recommends law firms:

- Exercise reasonable care in choosing a cloud provider, such that the firm has a reasonable expectation that privileged client information will be kept confidential.
- Specifically instruct cloud providers to safe-

guard client data.

- Ensure providers have a specific provision in their agreement that guarantees the provider will take measures to preserve the confidentiality of the firm's data.

Vetting the cloud computing service provider

Assessing the reputation and reliability of a provider is the logical first step. How long has the cloud provider been in business, and are they using time-tested, proven technology? Because technology changes at a rapid pace, the longevity of a provider may be difficult to evaluate, but look for some quantifiable history of the company and the technology it employs. Reputable cloud providers use technology that is consistent with industry standards and holds up to expert opinions and analysis, as well as complies with standards, such as Statement on Auditing Standards No. 70: Service Organizations (SAS 70), Payment Card Industry Data Security Standard (PCI DSS), or the Health Insurance Portability and Accountability Act (HIPAA).

Any cloud provider trying to sell its platform is going to tout its security features. The best measure of a company's worth in terms of security should be gathered from a third-party security audit. The provider should also be able to explain any occurrences of security breaches, as well as the actions the provider took in terms of restoring the lost or compromised data and compensating the injured parties.

If the provider has had no history of security breaches, it should be able to provide a detailed contingency plan, including a detailed description of where data is stored and backed up.

Performing due diligence will yield information that will allow you to make a well-informed decision.

Types of information

Clearly, a client's personally identifiable information must be protected at all costs. However, according to Nevada Revised Statutes Chapter 603A, personally identifiable information consists of any information that directly or indirectly identifies an individual.

The language in a cloud service provider's contract may

CLE PASSPORT

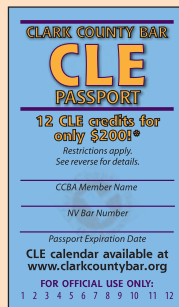
The cost of this amazing offer?
Only \$200 for 12 CLE credits!

While others are charging much more, we offer the best deal in town! The CLE PASSPORT offers a savings of over 33% off of regular CCBA CLE prices, and 60% or more off of the competition's prices!

- **CCBA members, get your order form online at www.clarkcountybar.org.**
- **Non-members may join CCBA, then purchase the card by contacting Donna Wiessner at (702) 333-2266.**

For one low price, attorney members of the Clark County Bar Association may purchase twelve CLE credits, redeemable for attendance to CCBA sponsored CLE seminars. The 2011 CLE Passport is valid January 1, 2011 to March 30, 2012. CCBA membership must be renewed for the Passport to remain valid during Jan.–Mar. of the upcoming membership years.

*Restrictions apply to this offer. This offer is non-transferable and limited to CCBA members for admittance to CCBA-sponsored CLE seminars during the current calendar year. This offer does not include CLE seminars not solely sponsored by the CCBA (i.e., co-sponsored by the State Bar of Nevada). The CLE PASSPORT must be presented upon attendance of live seminar or upon ordering of audio/visual materials. The Passport cannot be used for online purchases for any type of CLE seminar, including live, or downloadable CLE files.



not be specific enough. Before attorneys begins placing sensitive information on the Internet, they should draft language into the agreement that specifies the types of information that are protected under the provider's security agreement. This may include, but not be limited to, data from a third party, data drawn from both electronic and non-electronic formats, metadata, trade secrets, personally identifiable information, and intellectual property. Attorneys should carefully formulate this language so it accurately covers all of the categories of information contained in their records.

Per NRS Chapter 603A, law firms are "data collectors" because they handle nonpublic personal information. "Personal information" is defined as first name or first initial and last name combined with one of the following when the name and data elements are not encrypted: social security number; driver's license number or identification card number; account number; credit card number; and access code or password that would allow access to a person's financial account.

Therefore, law firms must require cloud providers to implement and maintain reasonable security measures to protect their records from unauthorized access. An easy way to accomplish this is to contractually bind the cloud provider to adhere to NRS Chapter 603A.

Understanding what cloud computing "security" means

Unlike physical data storage, cloud computing relies on servers in data centers, authorized user passcodes, and electronic security measures. Cloud servers are typically stored in highly secure facilities requiring a biometric match and the consent of an on-premise security guard to gain entrance. The bigger risk with the cloud is unauthorized electronic intrusion, or "hacking," in which the hacker steals user names, passwords, and client records. Hacking can be as disastrous as having a pack of thieves make off with a filing cabinet.

Realistically, there is no way to guarantee against unauthorized electronic intrusion in the cloud, just as it isn't possible to guarantee against it with your on-premise computer equipment. All network connected computers carry some level of inherent risk. Agreements with cloud providers should specify that they are responsible for exercising a "reasonable standard of care" to prevent unauthorized access to the information on cloud servers.

Statistics reveal that most security breaches originate from inside an organization, so attorneys are advised to use the evaluation of cloud systems as a precipitant to review their own internal security processes as well.


Properly implemented and managed cloud systems are likely to be more secure than on-premise equipment due to a higher level of proficiency in the design, along with adher-

ence to more rigorous protocols. But most attorneys are not technology experts, so a potential cloud provider should be able to clearly articulate the security measures they employ.

Ramifications of the Nevada security of personal information law on cloud computing

Nevada Revised Statutes Chapter 603A requires that personal information be encrypted. Attorneys should review this law and determine what methods of encryption the provider is using. A big problem comes in the language of the provision, which focuses on the transmission of information from a "secure system." Technically, anyone transmitting data from an "insecure system" may be able to evade the requirements of the provision. Also, telecommunication providers conveying the communications of other people are technically exempt from the requirement to use encryption. Nevada attorneys should write language that clearly defines the role of the provider so they do not manage to technically evade their responsibilities. Under this law, the technical methods of encryption used by the provider should meet the standards or guidelines of an established institution, such as the Federal Information Process Standards, which is maintained by the government-

Cloud *continued on page 32*



ARA SHIRINIAN
MEDIATION

Mr. Shirinian practices exclusively as a
mediator and arbitrator.

Selected for inclusion in the
2011 Super Lawyers Mountain States Edition

and

2010 Super Lawyers Corporate Counsel Edition
in the area of Alternative Dispute Resolution.

Tel: (702) 496-4985
Fax: (702) 434-3650
E-mail: arashirinian@cox.net

www.arashirinianmediation.com

Cloud continued from page 31
tal agency, National Institute of Standards and Technology (NIST).

Defining a security breach in compliance with NSPI law

Attorneys should also make sure that the terms of a “security breach” are adequately defined. If, for example, a provider defines a breach as unauthorized access to its user codes *only*, a breach that managed to exploit a weakness in the firewall of the underlying cloud computing system not related to the official password system itself could technically be described as falling outside the purview of the definitions of a security breach. When reviewing the provisions of the contract, attorneys should consider consulting a third-party cloud computing engineer who can provide terminology describing how breaches occur.

This is especially important in light of the “safe harbor” provision of NRS Chapter 603A. According to the law, “data collectors” are exempt from damages for a security breach if they follow the provisions of the law and the breach is not caused by the data collector or any of its associated employees. Again, this provision can be avoided if the cloud computing provider is not defined as a data collector. However, it is a scenario that attorneys should be careful to avoid. If the provider claims they are a “data collector,” then they would be able to evade practically any form of responsibility for a data breach they did not directly cause as long as they had followed the provisions of the law, even if their security procedures were sloppy but technically adequate.

Stating the obvious: limiting “sharing” policies

Attorneys should make sure contractually they are the sole owners of the data they store with a cloud provider.

Furthermore, attorneys should make sure that the provider will not share or use the information it stores for any other reason than the reasons stated in the agreement. Providers should not “share” the information with other providers or service entities unless they have been specifically instructed to do so. Additionally, should the transfer of data or “sharing” be a part of the provider’s regular security activities, any agents, associates, or entities involved in this process should be prepared to agree to the terms written between the provider and the attorney.

The same best practices that apply to on-premise computer equipment apply to cloud-based systems. Law firms should make sure their staff is adequately trained to create strong passwords that are more difficult to compromise, not share passwords with anyone, and report any suspicious activity on their computer that may indicate a virus or other malware.

Reporting and notification procedures

Attorneys and providers should have a clear policy on how breaches or other security problems will be reported. If a breach occurs, the provider should state what actions will take place. First and foremost, the provider should notify the attorney’s office promptly if a breach occurs and provide them with procedures to prevent any further data from being exposed or lost. An investigation involving the seizure of related documentation or an active evidence collection phase may be necessary in order to establish how the breach occurred. The policy should specify that notice of these actions will occur within hours, not days, of an investigation or of the service of any subpoena or other legal process.

Conclusion

Cloud computing offers attorneys a multitude of compelling benefits, including improved mobility, reliability, security, and the ability to cost-effectively store and reference virtually any of their firms’ resources. By taking the time to carefully review the language of provider agreements and the applicable laws, attorneys can realize the benefits of the cloud while minimizing their exposure to risk. **G**

Jeff Grace is the President & CEO of NetEffect, a Las Vegas-based technology support and consulting firm serving the IT needs of small- and medium-sized organizations in southern Nevada since 2002. In February of 2011, NetEffect launched MyGrid, a fully hosted cloud computing platform.

Lizette B. Sundvick, Esq. has been serving the Las Vegas and Henderson community since 1993. She is the President of Sundvick Legacy Center, an innovative law firm providing strategic estate planning and asset protection services to professionals, business owners, and families.

**Social Networking Online?
Follow CCBA!**

Twitter:
[@clarkcountybar](#)

Facebook:
[facebook.com/ccbanv](#)

Website:
[clarkcountybar.org](#)