

Keeping Client Secrets While Using Cloud Computing Resources: Ethical and Technology Considerations

By Joseph Decker, Esq. and Scott Ardisson, CCE

Lawyers, litigators and corporate counsel alike are charged with the ethical obligation to maintain and safeguard the confidentiality of their clients' information.¹ A casual survey of the deluge of legal articles on "cloud computing" would reveal that "protecting client confidences" is the topic that is discussed most frequently. But sometimes the relatively straightforward ethical issue is being "clouded" by "the sky is falling" commentary. What are the technology differences between "cloud computing" and network computing in a law firm, for example, which affect confidentiality concerns? Are the steps neces-

sary to discharging the duty to maintain client confidences in a cloud environment really much different than those necessary to establish and secure a law firm's own servers...."

minimal management effort or service provider interaction."² Simply put, a cloud computing environment is a group of computers that act like one really big computer. You can rent portions of the big computer as you need it. A computing cloud uses computing resources like a large and powerful version of the computer sitting on your desk. Your computer probably has multi-core processors. When software applications run, resources from those processor cores are dynamically allocated to each piece of

"Are the steps necessary to discharging the duty to maintain client confidences in a cloud environment really much different than those necessary to establish and secure a law firm's own servers...."

sary to discharging the duty to maintain client confidences in a cloud environment really much different than those necessary to establish and secure a law firm's own servers, or much different than making sure unencrypted emails are not intercepted or misdirected? The short answer is: not much – understanding, risk assessment and mitigation are the fundamental requirements – fear and mistrust of new "cloud computing" technology is unwarranted.

Comparing "Cloud Computing" with Traditional Computing

"Cloud computing" refers to a "model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with

software as needed. When you are done using a particular piece of software and no longer need the computing resources, those resources are made available for use by other pieces of software on your computer. The same thing happens in a cloud environment on a larger scale. In cloud environments there may be hundreds or even thousands of processors available to the users, and these processing resources are dynamically allocated to the applications that are running in the cloud. When a cloud subscriber finishes with an application, the computing resources that were being used by the application are made available to other applications

This issue of qubit and past issues are available on our website at: www.bit-x-bit.com

Keeping Secrets While Using Cloud Computing Resources (Cont. from p. 1)

and other subscribers using those cloud computing resources.

A “public cloud” is a cloud infrastructure or resources that are made available to the general public via the Internet by a third-party provider.³ An example of a public cloud is “Amazon Elastic Compute Cloud.” For a fee, Amazon provides computing power and data storage for businesses at a rate which makes it attractive. Amazon, however, in providing a “public cloud” does not provide the software to run the business’ applications. A “private cloud” is a cloud infrastructure operated solely for a particular business, which may be managed by that business or by a third party. It may be physically located on the organization’s premises or off-premise.⁴ “SaaS” (Software as a Service) allows a consumer to use the cloud provider’s applications or software

single computing system. Therefore, as demand for that application increases, the application itself can draw on the pool of available resources in the cloud so that it may scale up to meet the increased demand and, conversely, scale down when the demand decreases, releasing the computing resources it was just consuming. When software applications are written for this type of scalable environment, the underlying code does not need to change significantly as the company grows from serving ten users to serving 1,000 users.

Finally, reliability is a key factor. In a true cloud environment, hardware failures are automatically noted and handled by the applications that are running within the cloud. If a particular piece of hardware used by a software process fails, the software process will be automatically redirected to functioning

“A ‘public cloud’ is a cloud infrastructure or resources that are made available to the general public via the Internet by a third-party provider.”

that are running on a cloud infrastructure. Typically, these applications or software are available and accessible through a web-browser. Web-based or “hosted” e-discovery review and production tools are examples of SaaS.

There are three reasons why businesses find cloud computing attractive: efficiency, scalability, and reliability. In terms of efficiency, according to Werner Vogels, the CTO and Vice President of Amazon.com “. . . computer utilization in most cases, enterprise as well as startups, is dramatically low (less than 20% and often even lower than 10%) and is often subject to significant periodicity.”⁵ In a cloud environment the “idle” computer time can be used by other customers, and the startup or enterprise only needs to pay for the 20% or so they are actually using.

Application scalability is another key reason for utilizing cloud architecture. In a cloud environment, an application is not constrained by the limitations of a

hardware. In very large cloud environments, this redirection can occur almost instantly and to geographically dispersed data centers.

Ethical Duties—Old and New Interpretations

As lawyers become more familiar with new technology, some of the initial ethical concerns fade. This happened with email. In 1999 the ABA addressed confidentiality issues in email use. ABA Formal Opinion 99-413 considered whether lawyer-client communications using unencrypted email would violate a lawyer’s duty of confidentiality. In concluding that unencrypted email afforded a reasonable expectation of privacy, the ABA Committee evaluated the risks and expectations in using email, and in using technological alternatives, such as U.S. Mail, telephone or facsimile transmissions. The Committee also concluded that an online service provider’s email system afforded a reasonable expectation of privacy because of password-protected mailboxes and federal law limitations on inspection and disclo-

Keeping Secrets While Using Cloud Computing Resources *(Cont. from p. 2)*

sure of the contents of email under the ECPA.⁶ Risks from administrator-snooping or hackers do not make privacy expectations unreasonable, “just as the risk of illegal telephone taps does not erode the reasonable expectation of privacy in a telephone call.” The Opinion states that privacy expectations must be reasonable, not “absolute.” The ABA Committee further noted that, although earlier state ethics opinions found that email was not reasonably private because of its “susceptibility to interception by unauthorized persons,” more recent opinions, which approved of email use, reflected a “greater understanding of the technology....”

In September 2010, the New York State Bar Association’s Committee on Professional Ethics issued Opinion 842 on the use of cloud computing. It provides: “A lawyer may use an online data storage system to

public cloud = bad,” or that cloud environments are less secure than traditional “on site” single-client server environments. The fact is that every computer system – whether used solely by one business and on its premises, or whether operated off-premises with multiple users and in multiple locations -- will have security vulnerabilities and different types of threats. The critical factor in determining whether a computing environment is secure, however, is how these vulnerabilities and threats are addressed, not the type of computing infrastructure used.

External threats

External threats like hackers, viruses and malware generally seek to exploit the vulnerabilities that exist within computing environments to crash systems or steal data. Cloud computing environments are subject to these threats. So is any computer network that ac-

“The critical factor in determining whether a computing environment is secure, however, is how these vulnerabilities and threats are addressed, not the type of computing infrastructure used.”

store and back up client confidential information provided that the lawyer takes reasonable care to ensure that confidentiality will be maintained in a manner consistent with the lawyer’s obligations under Rule 1.6. In addition, the lawyer should stay abreast of technological advances to ensure that the storage system remains sufficiently advanced to protect the client’s information, and should monitor the changing law of privilege to ensure that storing the information online will not cause loss or waiver of any privilege.”

Therefore, the ethical use of cloud infrastructure must be evaluated, in part, from a technology standpoint. We will focus our discussion on technology questions to ask when evaluating cloud computing.

Securing the Cloud Computing Environment: Technology to Consider

There is a lot of misinformation regarding the security of cloud computing, such as “private cloud = good;

cepts email and allows users remote access. From a technology standpoint, the following are some technology “checklist” questions to ask:

- Vendor encryption: Are communications between users and the cloud provider encrypted? It should be common practice to use “https” encryption for communications.
- Network security: How strong are the protections from unauthorized external access? Does the vendor have a network intrusion detection system to both monitor for and stop network intrusion attempts in real time?
- Types of passwords: How strong are the passwords which the cloud vendor has established? The vendor should require at least 8 characters, including upper and lower cases, numbers, and special characters. Microsoft recommends that passwords should be required to be changed every 42

Keeping Secrets While Using Cloud Computing Resources (Cont. from p. 3)

days. (Microsoft Technet website <http://technet.microsoft.com/en-us/library/c875814.aspx>)

- Security auditing and penetration testing: The cloud vendor should conduct periodic penetration testing, or have an outside firm that performs such testing. In a penetration test, the cloud computing environment is subjected to deliberate hacking attempts to expose vulnerabilities.
- Documentation: Ask for the documentation of the cloud provider's security policies. The procedures described above should all be part of its routine.
- Mother Nature is another external threat. Flooding, earthquakes, tornadoes and other types of

Does the vendor perform background checks on employees who have access to sensitive information?

What are the vendor's coding practices? If the vendor of cloud computing is also providing SaaS, remember it is not the cloud environment that is delivering the service that you are purchasing, but rather the software application itself. The software application should address application vulnerabilities such as SQL injection (where software code is injected into forms where data is required), and cross-site scripting (where code that is meant to be executed on the client's computer system is altered to run an attackers code instead) and should comply with OWASP recommendations?⁷ Without secure coding practices, running an application in a secure data center is like building a castle but leaving the front gate open. These same security principles exist no matter what

“Thus, the real consideration is not cloud vs. traditional network, or public cloud vs. private cloud, but rather ‘secure versus not secure.’”

natural disasters can destroy data centers and disrupt operations. Cloud service providers should have disaster recovery plans to cope with massive infrastructure loss. Those plans should include a “redundant” data center.

Internal threats

One example of an internal threat is a dishonest employee or contractor working at a cloud computing vendor. Standard practices for addressing internal threats do not change when using a cloud environment versus a traditional networked computing environment. The following are questions to ask:

Is information only accessible to the software, systems and personnel who need to have access? This is called “compartmentalization.” Compartmentalization means that data exists in “compartments” to which only authorized software processes, systems or individuals have access.

back room computing platform is used to host an application.

“Seal of Approval”

Because the vast majority of lawyers do not have the expertise to identify potential security weaknesses or breaches, in order to gain comfort, lawyers should look for a “seal of approval” from a recognized certifying agency. Some cloud providers and data centers are “SAS-70 compliant” with standards promulgated by the American Institute of Certified Public Accountants. This means that an accounting firm has evaluated the cloud provider's internal controls, procedures, and documentation which govern the organization's data security, and has concluded that those procedures give reasonable assurance that the company's control of data will be achieved. Another desirable certification to look for is ISO 27001.

Thus, the real consideration is not cloud vs. traditional network, or public cloud vs. private cloud, but rather “secure versus not secure.” Although tradi-

Keeping Secrets While Using Cloud Computing Resources (Cont. from p. 4)

tional and cloud computing environments have different types of threats and vulnerabilities due to different system architectures and software types, these threats are all manageable and should be addressed by the cloud computing service provider. By inquiring and documenting such inquiries, lawyers will be satisfying their ethical obligation to evaluate the technology dedicated to maintaining the confidentiality of client data “in the cloud.”

Legal Protections for Cloud Users

Finally, a reasonable expectation of privacy for data in the “cloud” is provided, in part, by legal protections which apply to data in transit or stored in the cloud – a consideration noted in the ABA’s 1999 opinion finding that there is a reasonable expectation of privacy when using unencrypted email. Title I of

¹ The ABA Model Rules of Professional Conduct, Rule 1.6(a) regarding confidentiality of Information provides that “A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent....”

² National Institute of Standards and Technology, Information Technology Laboratory (NIST), Peter Mell and Time Grace, NIST Definition of Cloud Computer (2009).

³ P. Mell and T. Grance, *The NIST Definition of Cloud Computing (Draft)*, January 2011; found at http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

⁴ *Id.*

⁵ www.Quora.com; <http://www.quora.com/How-and-why-did-Amazon-get-into-the-cloud-computing-business>.

⁶ Electronic Communications Privacy Act of 1986, 18 U.S.C.

“By inquiring and documenting such inquiries, lawyers will be satisfying their ethical obligation to evaluate the technology dedicated to maintaining the confidentiality of client data ‘in the cloud.’”

the ECPA, the Wiretap Act, protects electronic communications while they are being made, are in transit, and (arguably) are being stored on computers. Title II of the ECPA, the Stored Communications Act, protects the contents of files stored by service providers, and protects the identity of and information about subscribers. The ECPA provides for criminal penalties of up to five years imprisonment for unauthorized access of stored communications, and for civil damages, penalties, and attorney’s fees as well. Although some have criticized the ECPA – a 1986 law -- for being “outdated,” for treating email differently from stored communications, and because, they argue, certain information requires a warrant and other information only a government subpoena, the legal protections afforded by the ECPA were a factor in finding unencrypted email provided a reasonable expectations of privacy. These legal protections support the same conclusion as to cloud computing.

Section 2510 et seq.

⁷ See Open Web Application Security Project (OWASP) “The ten most critical web application security vulnerabilities 2007update,” https://www.owasp.org/images/e/e8/OWASP_Top_10_2007.pdf.



For questions or comments regarding this issue of qubit, please contact Susan Ardisson at Susan.Ardisson@bit-x-bit.com.

qubit \ˈkyü -bit\ n. a quantum bit, the counterpart in quantum computing to the binary digit or bit of classical computing. Just as a bit is the basic unit of information in a classical computer, a qubit is the basic unit of information in a quantum computer.
whatis.com

This publication is for informational purposes only and is not meant to be, nor should it be, construed as legal advice.

© 2011 bit-x-bit, LLC. All rights reserved.