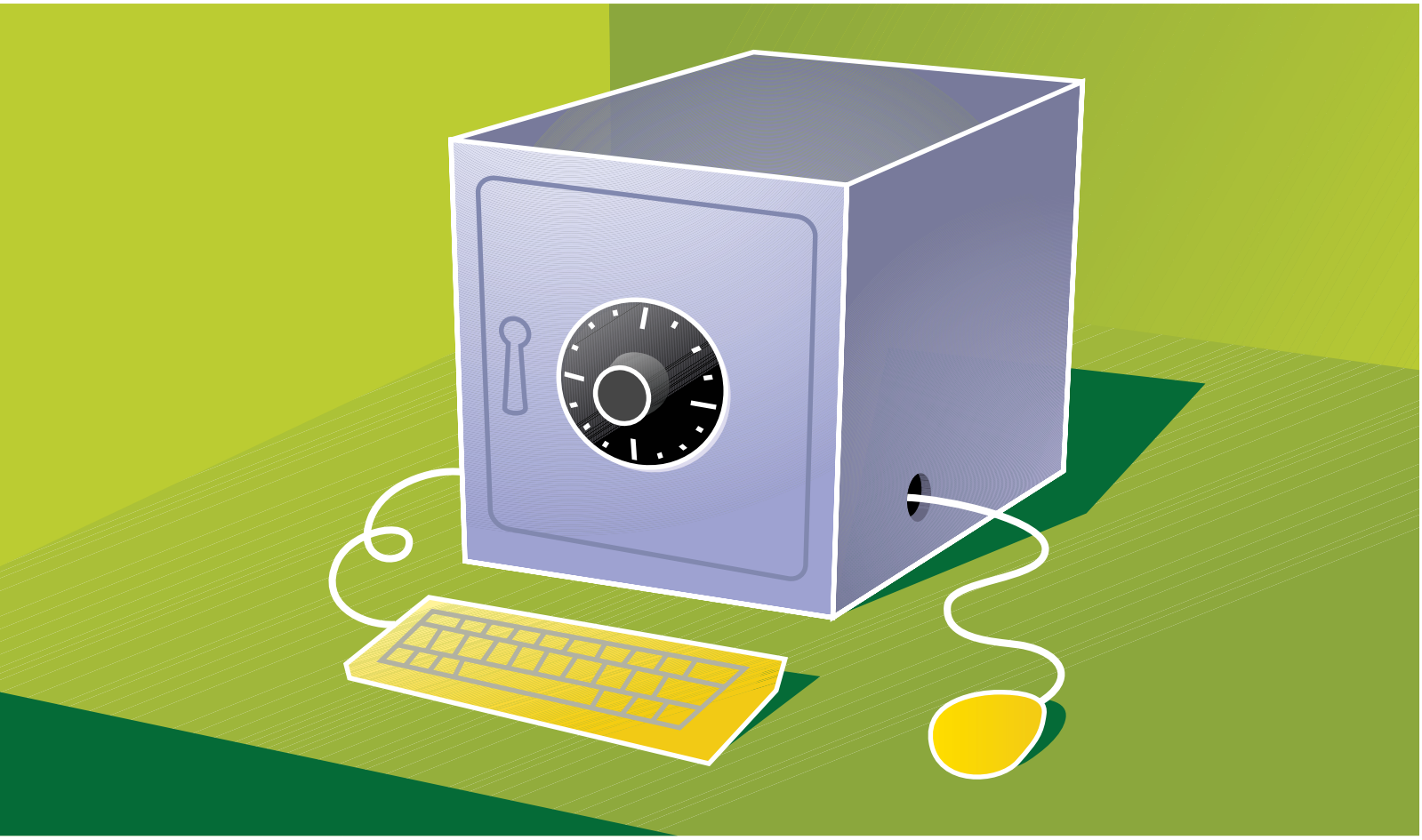
JACK NEWTON CLIO



The Ethics and Security 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 computing to occur in the last 20 years. While the benefits offered by cloud computing are numerous, several outstanding questions remain regarding the relative security of cloud-based systems as compared to traditional, on-premises solutions. In a law firm context, the use of cloud computing raises ethics issues around storing confidential client data on a system the attorney may not own or otherwise control.

The discourse on the ethics of cloud computing took a significant step forward in March 2010 with the issuance of a proposed Formal Ethics Opinion (FEO) on cloud computing by the North Carolina State Bar.

This was the first FEO in North America to explicitly deal with the use of SaaS/cloud computing in a law firm. While the proposed 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.

CLOUD COMPUTING

Cloud computing is computing delivered as a service over the Internet, with less need for software on your desktop computer. Increasingly, it will matter less and less which computer you use to do your work: your documents, e-mail messages, pictures, and all 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 much of 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 Hotmail, Gmail, or Yahoo Mail, 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.

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 OS X.

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. Alice Neece Mine, Executive Assistant Director of the North Carolina State Bar, outlines the primary concerns in the proposed FEO (2010 FEO 7):

> *SaaS for law firms may involve the storage of a law firm's data, including client files, billing information, and work product, on remote servers rather than on the law firm's own computer and, therefore, outside the direct control of the firm's lawyers. Given the duty to safeguard confidential client information, including protecting that information from unauthorized disclosure, the duty to protect client property from destruction, degradation or loss (whether from system failure, natural disaster, or dissolution of a vendor's business), and the continuing need to retrieve client data in a form that is usable outside of the vendor's product, may a law firm use SaaS?*

To this question the proposed FEO answers, "Yes, provided steps are taken effectively to minimize the risk of inadvertent or unauthorized disclosure of confidential client information and to protect client property, including file information, from risk of loss."

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 outlined by the proposed FEO. 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 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 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 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 installing TrueCrypt (http://www.truecrypt.org) a free tool that will encrypt the entire contents of your hard drive.

• 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 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 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 a cloud-based provider's data availability strategy cannot be overstated. A recent catastrophic data loss at Danger, a division of Microsoft, where information for thousands of users was irretrievably lost, highlights the importance of a proper data availability strategy. 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 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 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 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 attorneys 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 North Carolina State Bar's proposed FEO echoes this assertion, having concluded that cloud-based services are acceptable for legal practice, provided reasonable care is exercised to ensure appropriate technologies are being leveraged to protect client privacy and confidentiality. Ideally, the pragmatic opinion proposed by the North Carolina State Bar will help to set a precedent that will be considered as other bar associations and regulatory bodies formalize and standardize their stances on the use of cloud-based technologies in legal practice. **ILTA**