Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Check The Forecast Before Using Cloud-Based Storage

Law360, New York (July 15, 2011) -- Lawyers typically take great care to protect the confidentiality and privacy of their clients' documents and other data, and to protect against the inadvertent disclosure of privileged communications and work product. They obtain protective orders, enter into confidentiality agreements, and spend hours upon hours redacting documents and creating privilege logs to shield documents from disclosure to their adversaries.

Yet some lawyers may be unwittingly throwing caution to the wind by using application software ("apps") with mobile devices in their everyday work life. There are numerous apps available for use with iPads, Android tablets, and a myriad of other mobile computing devices to work remotely from home, in meetings outside the office, at depositions, and in court.

These apps allow lawyers to seamlessly send — and store — client files to a remote server that does not belong to the law firm ("the cloud"). But could this unknowingly waive a privilege, destroy confidentiality or breach a data privacy law in doing so? Potentially yes, if reasonable steps are not taken to protect a client's data.

We've examined some popular mobile apps used by attorneys, the legal issues that may arise by saving client files in the cloud and some reasonable steps that attorneys should consider taking to protect their clients' data.

Cloud-Based Storage Solutions

Cloud computing refers to storing data on remote servers that is easily accessible from any PC, laptop or mobile device through an Internet connection. The data is not stored on the computer or mobile device, but on a server maintained by the cloud service provider.

It is unlikely that a cloud user will know exactly where the data is stored. Many popular apps are compatible with these cloud-based storage services, which provides for easy access to files from a mobile device. These services offer data storage in the cloud for a minimal cost — many offer free plans and charge nominal amounts for additional storage space.

For example, Apple's iCloud, which was introduced to great fanfare on June 6, 2011, is one of the newest cloud services. It currently works with iTunes for music. The full version, which will be released in the fall, will provide 5 gigabytes of free storage and will wirelessly sync every document edited on Apple's iWork platform as well as all apps, movies, e-books, email, calendar and contacts across all Apple devices.

Many other cloud service providers already offer free cloud storage, including Amazon, Box.net, Cx.com, Dropbox, Google, Microsoft and SugarSync.

Advantages of the Cloud

The cloud can be very useful to any attorney who is looking for inexpensive data storage or a backup solution. It also provides for a quick and easy way to access documents from virtually any mobile device at any time, and at little or no cost.

The cloud eliminates the cumbersome and time-consuming process of having to physically sync up a mobile device to a computer each time you want to transfer files. The cloud also eliminates the need to email files to yourself or having to carry physical media such as CDs, DVDs, memory cards and flash drives — all with less storage capacity, and all of which can easily be lost.

Popular Apps

The following are just a few of the popular apps that attorneys have quickly adopted for use with their mobile devices. All of them have cloud-based options for easy storage and retrieval of documents.

The Deponent App is specifically designed for use with the iPad. The attorney can select, customize and add questions to a series of preloaded deposition questions. The questions can then be linked to the exhibits formatted as either Microsoft Office files, TIFF images, PDFs or plain images.

TrialPad is another iPad app specifically designed for attorneys. The trial lawyer can connect the iPad to a screen in order to display exhibits in the courtroom. TrialPad allows the lawyer to highlight or mark up the exhibit up while it is displayed on the screen. The marked-up exhibit can then be saved to the cloud as a separate “hot doc” while the original is preserved.

Keynote Remote is the iPad version of Apple’s popular Keynote program. Users can create unique presentations from their iPads that may include photos, charts, tables, animations and other special effects. The presentations can be shown at a meeting or in court by connecting the iPad to a screen.

There are many other apps commonly used by attorneys. They include Quickoffice and Documents To Go Premium Office Suite, which allow the user to create, edit or view Microsoft Office documents right from the user’s mobile device. GoodReader and iAnnotate are examples of PDF readers that allow mobile users to annotate PDF files by adding text, notes, lines, arrows and freehand drawings. Evernote is a useful app for simple note-taking and allows the user to incorporate screenshots, photos and webpage clips.

Potential Issues With The Cloud

All of this sounds great, right? Who wouldn’t want free data storage and easy access to their files?

But because a cloud service provider is a third party, sending client data could potentially risk waiving claims of privilege or destroying confidentiality unless adequate safeguards are in place. International or domestic data privacy laws may be implicated depending on the nature of the documents and data, and where they are physically stored.

The cloud also increases the risk of unauthorized access to files by hackers or other security breaches. Dropbox recently disclosed a bug where, for several hours, all accounts were vulnerable to access by simply entering any password.

The Law

The law, like the technology, is still evolving. The American Bar Association and several state bar associations have issued rules or advisory opinions regarding attorneys that use the cloud to store client data. Courts have yet to opine on the issue.

The ABA's Model Rule of Professional Conduct 1.6 and Comments require lawyers to act competently to protect their clients' confidential information. The ABA has proposed amending Rule 1.6 to explicitly impose an ethical duty on the lawyer to take "reasonable" measures to protect a client's confidential information from "inadvertent disclosure" or "unauthorized access." These obligations are currently described in the Comments to Rule 1.6.

The New York State Bar Association Committee on Professional Ethics, in Opinion 842 (2010), concluded "that a lawyer may use an online 'cloud' computer data backup system to store client files provided that the lawyer takes reasonable care to ensure that the system is secure and that client confidentiality will be maintained." The lawyer should also "stay abreast of technological advances" to ensure that the client's information will be protected and to "monitor the changing law of privilege."

At least six other state bar associations have similarly issued opinions permitting attorneys to store client data with third-party vendors, including cloud service providers. The general rule is that lawyers do not have to guarantee that a breach won't occur. They only need to act with reasonable care to protect security and confidentiality. See, e.g., Alabama Opinion 2010-02 (2010); Arizona Opinion 09-04 (2009); California Opinion 2010-179 (2010); Massachusetts Opinion 05-04 (2005); Nevada Opinion 33 (2006); New Jersey Opinion 701 (2006).

Protecting Client Data

So, how does one take reasonable care to ensure that client files stored on the cloud remain secure thus protecting confidentiality, privilege and privacy?

The safest option is to use a "private" cloud service, such as SharePoint or WorkSite's cloud service, which allow only authorized users to access files. Regardless of which service provider an attorney chooses, he or she should first carefully review the provider's "privacy policy" and "terms of use" to see if they adequately protect the data by ensuring confidentiality and security. The policies and terms are usually standard and are typically found through links on the provider's website. Some are better than others.

For example, until recently, Dropbox did not make any guarantees to maintain confidentiality or security. According to its standard "terms of service," the user acknowledged that "use of the site, content, file and services may result in unexpected results, loss or corruption of data or communications, project delays, other unpredictable damage or loss, or exposure of your data or your files to unintended third parties."[1] Dropbox provides the service "as is" without "warranty or condition of any kind."

Conversely, Cx.com purports to have a very strong policy to keep data confidential and secure. "CX will never share any of your data with any third party for marketing the products. Your stuff is your stuff — we just help you keep track of it, keep it safe and get better access to it. In that process our team and engineers cannot even see you [sic] files. The search mechanisms built into the system are for you only to search through your own files and data." Cx.com also provides the service "as is" and disclaims all warranties regarding the service.

An attorney may want additional terms to be incorporated into a standard cloud service

agreement to establish an agency relationship with the provider. A contract establishing an agency relationship is one way to protect against the possibility of allegations that the mere transfer of data to a third party de facto waived a privilege or breached confidentiality. Paid service providers may show more willingness to negotiate specific contract terms or to enter into separate non-disclosure or confidentiality agreements.

The agreement should require the cloud service provider to commit to using the highest possible standards for maintaining not only privacy and confidentiality, but also security. This may include the use of firewalls to segregate your data from others'.

Attorneys should consider negotiating clauses holding the service provider liable if it withholds or destroys data without prior notice and consent. Include provisions to ensure retrieval of the data should the service terminate for any reason. Select a cloud provider that will promptly notify the attorney of any subpoena it receives for disclosure of files and one that will cooperate in obtaining a protective order to limit such disclosure.

Subcontractors should also be required to adhere to the service provider's obligations under the agreement. Finally, the service provider should furnish a statement describing where it will store the data and warrant that it will comply with the local laws in each country where the data is stored.

Be aware that, even if the cloud service guarantees privacy and security, many free cloud service providers reserve the right to terminate the service at any time, at their own discretion and without any notice. They generally are not obligated to return files upon termination.

Attorneys should occasionally reconfirm that the provider's security measures are keeping up with technological advances. Use a service that either offers or allows the use of encryption to secure files. Attorneys should never use unsecure wireless Internet connections to transmit client files and should ensure that the apps themselves are not transmitting any confidential client data to third parties. Attorneys should also keep abreast of the latest developments in this area of the law, including the latest state bar association ethics rules and opinions.

Finally, attorneys should avoid saving any client documents to a cloud service provider's "public folder" because anyone who learns of the existence of those files will be able to access them.

The cloud can certainly be a convenient and low-cost option for attorneys working with client files on their mobile devices. In order to guard against these low-cost options from becoming high-risk, attorneys should take reasonable steps designed to ensure that cloud service providers keep client files secure and private.

--By Alysia Solow and Alan Schwartz, Constantine Cannon LLP

Alysia Solow is a partner in the New York office of Constantine Cannon. She directs the firm's e-discovery practice group. Alan Schwartz is an associate in the firm's New York office, focusing on e-discovery and antitrust litigation.

[1] Approximately two weeks after fixing the bug that rendered Dropbox accounts vulnerable to access by anyone, Dropbox modified these terms on July 2, 2011, in part, by eliminating the language regarding the exposure of data to third parties.