TECHGEAR

The Iomega iConnect ($99) allows you to connect up to four USB storage devices (like external hard drives or flash drives) to your home computer network. You can also configure the iConnect to share and access connected devices over the Internet.

WEBLINKS

TYLER FLOOD is certified in criminal defense law by the Texas Board of Legal Specialization. He dedicates his practice exclusively to DWI defense. Flood is certified by the National Highway Traffic Safety Administration as an instructor in Standardized Field Sobriety Testing. His practice is based in Houston.

DontMesswithTexas.org

My favorite website is Don't Mess with Texas, where you can report litterbugs. The state then sends the person a litterbag, along with a letter telling them where they were seen littering and not to mess with Texas. I've reported probably 25 people who have thrown cigarette butts out their window. It drives me crazy!

www.Dropshots.com

Being a DWI lawyer, it's a good place to share videos that you can invite people to view by emailing them the link.

http://www.tdcaa.com/dwi/case_law/

This is TDCAA Richard Alpert's case law outline on DWI. It's always good to know what the other side is reading!

thinkexist.com

This is a great place to find quotes from anybody about anything. Type in Clarence Darrow and many of his greatest come right up!

DoNotBlow.com

My site — I wouldn't be me if I didn't engage in a little self-promotion.

Putting Your Practice in the Cloud
A Pre-Flight Checklist

BY JACK NEWTON

Cloud computing is one of the hottest legal technology trends to emerge over the past five years. The promise of reduced IT expenditure, coupled with increased mobility and convenience, has lawyers across the country thinking about putting their practices "in the cloud."

However, while this new era of legal IT offers many benefits, it also introduces several new risks that a lawyer must consider before selecting a cloud-based service provider. The following "pre-flight checklist" will help you understand cloud computing, its benefits, and the potential risks to be minimized.

CLOUD COMPUTING FUNDAMENTALS

Cloud computing may be an exciting buzzword, but understanding the established and even mundane technical details underlying the cloud is key to understanding the potential risks. As opposed to the traditional computing model, in which a firm hosts its own servers, software, and data "on site," the cloud computing model delivers software and data "on demand" over the Internet via a third-party provider, avoiding the need to maintain local hardware or infrastructure.

This might seem abstract, but if you use web-based email such as Gmail, Yahoo! Mail, or Hotmail, you are already computing "in the cloud." Instead of using an on-premise email server and client, such as Microsoft Exchange or Microsoft Outlook, you are using your cloud-based email provider's infrastructure to host your email, which you can then access via any device with a web browser.

THE ETHICS OF CLOUD COMPUTING

Inherently, cloud computing means trusting a third party with your data — something that has clear ethical implications for lawyers. While the majority of states have not yet explicitly ruled on the ethics of cloud computing, the North Carolina State Bar recently issued a proposed ethics opinion on the permissibility of storing confidential client data with a cloud-computing provider.

The first of its kind, the proposed opinion conditionally accepts the use of cloud-based products in legal practice, "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." (The full opinion is available at **http://scr.bi/aIA1cV**).

Other bar associations have steered away from explicitly issuing opinions on cloud computing. Instead, they point to the principles outlined in the state's Rules of Professional Conduct and ask attorneys to perform adequate due diligence prior to selecting a cloud computing provider.

JACK NEWTON is co-founder and president of Clio, a provider of cloud-based practice management software. He has spoken at CLE seminars across the United States about how cloud computing can help law practices run more effectively and efficiently. Contact him at **jack@goclio.com**.

WHAT ABOUT TEXAS?

Ellen Pitluk, an ethics attorney for the State Bar of Texas, comments: "While Texas doesn't have a formal opinion on cloud computing, Ethics Opinion 572 deals with the use of independent contractors to perform services in connection with a lawyer's representation of a client, and many of the same concepts apply to cloud computing. As the opinion suggests, lawyers should perform adequate due diligence prior to selecting any independent contractor."

ENCRYPTION

Does the cloud computing provider use an encrypted connection for all communications? Without an encrypted connection, it would be easy for an unauthorized party to eavesdrop on your potentially sensitive communications. Ensure your cloud computing provider utilizes SSL-based secure encryption — something you can easily check by looking for the "lock" icon in your web browser's address or status bar.

SERVER SECURITY

Although encryption helps secure the communication between your computer and your cloud provider, you also need assurances that the provider's servers are properly secured against hackers and other threats. When considering a cloud computing provider, ask whether external security experts are routinely auditing the provider's servers for potential security holes and vulnerabilities.

PROVIDER VIABILITY

When selecting a cloud computing provider, you also want to ensure the provider has a sustainable business that you'll be able to depend upon in the long term. Ask the provider how long it has been in business, how many customers and employees it has, and if it is profitable. While not every provider will answer every question you ask, a refusal to provide any information on how the company stands financially should serve as a warning.

DATA LOCALITY

Due to the distributed nature of the web, your cloud computing provider's computing infrastructure might not necessarily be located in the United States. Be sure to understand where the provider's data centers are located; you might unintentionally be subjecting your data to the search and seizure laws of a foreign country.

DATA PORTABILITY

Another key consideration: If you choose to leave the cloud service, can you easily take your data with you? Is it possible to export your data in a useable form, and if so, is there an associated cost?

GEOGRAPHIC REDUNDANCY AND BACKUP PROVISIONS

Ask a potential provider to explain how often your data will be backed up and whether the backups are distributed across multiple geographic locations. This "geographic redundancy" eliminates the risk that a single catastrophic disaster in one location will wipe out all backup copies of your data.

TERMS OF SERVICE

Lawyers, in particular, need to read the fine print! Review and understand the provider's terms of service, outlining the rules that cloud service users must follow. Generally speaking, the terms of service are there to protect the cloud provider from potentially abusive users, but it is important to ensure these provisions are not overly one-sided in the provider's favor.

PRIVACY POLICY

Likewise, make sure you read and understand the provider's privacy policy. Ensure that the policy is clear that (a) you own all of the data uploaded or entered into the cloud provider's service, and (b) your data will not be re-used for any purpose other than providing you access to the service and your data.

SERVICE AVAILABILITY

You rely on your cloud computing provider's availability, so any unexpected downtime could have a potentially severe impact on your business. While some service providers provide Service Level Agreements (SLAs) that guarantee minimum uptime levels (such as 99.9 percent availability), most SLAs offer limited recourse (such as a pro-rated refund based on the amount of downtime) should they fail to meet their SLA commitment.

We recommend you look at the provider's historical uptime data. Ask what third-party monitoring service the provider uses to monitor uptime, and ask to review the last 12 months of data. If the provider historically has had greater than 99.9 percent uptime, you can reasonably expect they will be able to continue that trend in the future.

ALL SYSTEMS GO?

Not all services are created equal, and attorneys bear an ethical burden to ensure the integrity and quality of the services they choose to support their practice. Armed with sufficient knowledge of cloud technologies and the policies that apply to them, legal professionals from all walks of life can feel confident that the technologies deployed in their practices have been met with the appropriate level of scrutiny.

While not exhaustive, the foregoing checklist provides a sound due diligence framework to assess a cloud computing provider's suitability to host your practice's valuable data. You too may find blue skies just beyond the clouds. ✪