

# The Florida Bar News

floridabar.org

October 15, 2014



**FOOT, TWIN-ENGINE RESEARCH VESSEL**, donated by Bill and Carol Barrows of Vero Beach, has been renamed *Orlando's Rose* in honor of former Judge Frank Do, left, and his high school friend, the late Robert Rosof. Orlando was a juvenile court judge, he was disturbed by boys who kept getting into trouble and shared his concern with Rosof, who worked at an oceanography research center. Under Orlando's court supervision, the boys worked with Rosof, focusing on oceanography instead of crime. In 1969, Rosof founded AMIkids on a shoestring that now consists of national community-based programs dedicated to turning at-risk juveniles. So far, AMIkids has helped more than 200 at-risk teens. On the vessel's bow are these words: "Rating a troubled past from a bright future."



## How safe is the cloud?

*Using the cloud is a highly complex, technical matter that poses numerous risks and challenges for lawyers*

By Gary Blankenship  
*Senior Editor*

You might have been amused by recent stories about the hacking of celebrities' private data accounts in the "cloud" and the publishing of nude photographs. But if your law firm uses the cloud to store information or run programs, have you considered that a similar breach of your information might leave you — and your clients — feeling more exposed than an undressed star?

Storing of digital information in the cloud and using programs that run in the cloud — basically huge banks of computers and servers owned by private companies — has been a hyped service in both the legal world and society at large in recent years. The Bar in 2013 approved an ethics opinion to guide lawyers, and its Law Office Management Assistance Service (LOMAS) has published

an extensive list of tips on using cloud services.

Two experts contacted by the *News* echoed Bar cautions that using the cloud is a highly complex, technical matter that poses numerous risks and challenges for lawyers and law firms.

And any breaches might be more than just embarrassment — state and federal laws require reporting of any breach of a law firm's electronic records, if they affect enough clients or involve certain types of personal information.

"I only put stuff on the cloud that I don't

**See Cloud, page 5**



TEPPLER

## E-filing software updates to address uniformity concerns

By Gary Blankenship  
*Senior Editor*

A coming change to the Florida courts e-filing portal is aimed at making it easier for lawyers to choose the "document type" when they are electronically filing court documents.

The update to portal software, which will be installed after business hours

on Friday, October 24, will suggest document categories to users instead of requiring them to conduct a search or scroll through lists to find the correct title for the type of document they are submitting.

The Florida Court E-Filing Authority, which runs the statewide portal through which electronic

filing is done, got a look at the upcoming software update at its September 25 meeting in Tallahassee.

Other changes include allowing larger documents to be electronically filed in the appellate courts, making it easier to see who has been served with documents in

**See E-filing, page 4**



# Cloud —

*(Continued from page 1)*

mind being publicized across the world," said Sarasota attorney Steven Teppler, who co-chairs ABA and Florida Bar committees on e-discovery and teaches about technology and the law at Ave Maria Law School. "This is all part of an attorney's responsibility to supervise his or her agents. Depending on what flavor of cloud you use, there will be differing levels of risk. Most attorneys using the cloud ... are exposing themselves to anywhere from uncomfortable to unacceptable levels of risk."

If it seems unlikely to you that firms might be the target of hackers, consider what Eric Hibbard, who heads security for Hitachi Data Systems, serves on an ABA committee on digital security, and co-chairs the Cloud Security Alliances' International Standards Council, has to say.

"There have been instances where hackers have targeted law firms once they figured out the firms were involved in the company they were going after," he said, adding the hackers calculated the law firms would have less security on sensitive information than the target company. "There are some fairly sophisticated attackers out there who are involved in industrial espionage. Some are involved in organized crime. These are not your run-of-the-mill ordinary attackers."

Despite their many warnings, Hibbard and Teppler said they haven't heard — yet — of a law firm's information stored in the cloud being compromised. Teppler said there have been cases where internal information in a firm has been compromised, such as trust account information. But that's no reason not to be vigilant.

"The advice I give some of our clients is only put in the cloud what you're prepared to have some government entity or some very sophisticated attacker have access to. If you're

not comfortable with those conditions, don't use the cloud," Hibbard said.

He added, though, with sensible precautions, "if the data you have is not that sensitive, then the cloud works in your favor, and you can get a lot of security."

Judy Equels, who used to head the Bar's LOMAS operation and now works with lawyers as part of the Bar's Attorney Consumer Assistance Program, noted a state law effective July 1 requires taking reasonable care to protect information and reporting of some hacking incidents.

"The newly passed Florida Information Protection Act of 2014 requires that any data breach affecting 500 or more individuals (or clients) must now be reported to the Florida Department of Legal Affairs," she said, adding that could be any solo lawyer with 250 family law files. Clients also must be notified (F.S. §501.171).

Equels also said under changes to the federal Health Insurance Portability and Accountability Act (HIPAA) that became effective in September 2013, law firms that have health information about clients — that includes Social Security numbers — count as "business associates" under the law and also must report when data is compromised.

Bar Ethics Opinion 12-3 advises members that they "may use cloud computing if they take reasonable precautions to ensure that confidentiality of client information is maintained, that the service provider maintains adequate security, and that the lawyer has

## Roy B. Gonas, Arbitrator



AV Rated attorney

Cumberland School of Law,  
City of London College,  
The Hague Academy of International Law

Telephone: (786) 420-5598

roygonas@att.net

Fulbright Specialist Grantee  
-International Commercial Arbitration  
Over 35 years experience as arbitrator in  
domestic and international cases

Visiting Lecturer in International  
Commercial Arbitration

Panels: AAA, ICDR and FINRA

Facsimile: (786) 420-5599

rgonasarbitration.com

## Digital security resources

If you want more guidance and information about digital security, start with Ethics Opinion 12-3, which can be found at [floridabar.org](http://floridabar.org). Also, the LOMAS has the "Cloud Computing Check List" and "Cybersecurity Tips for Lawyers," as well as other technology information on its page on the Bar's website.

Cybersecurity expert Eric Hibbard recommends resources available from the Cloud Security Alliance's website. An overview is available at <https://cloudsecurityalliance.org/research/>. One article he recommends is "Security Guidance for Critical Areas of Focus in Cloud Computing" at <https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/>.

adequate access to the information stored remotely. The lawyer should research the service provider to be used."

The opinion cites similar opinions in other states, which offer guidance to lawyers about vetting the provider to ensure that records remain confidential and available only to the firm, and that records are backed up.

Beyond Opinion 12-3, LOMAS has published on the Bar's website tips on cybersecurity in general and a checklist for lawyers using the cloud. One tip — which Teppler and Hibbard also emphasized — is lawyers must make sure the way they send information to the cloud is also protected. Sending unencrypted data from the public Wi-Fi at your local McDonald's or bookstore is not a good idea.

Another point is cloud storage providers must agree they provide storage only and have no ownership or security interest in the data.

Teppler recounted an instance where a major corporation became embroiled with a cloud company over the storage fees. The provider refused to provide access to, or to return the data, until the dispute was settled.

"One of the problems is attorneys don't always know what to ask. They accept vendors' representations," he said.

Teppler and Hibbard said attorneys need to know how secure the cloud servers are and where backups will be kept in case there is a total system failure. At the same time, they also need to know that when the firm removes information from the cloud service, or just wants to delete the information as part of routine record housekeeping, that the information will be completely removed.

The provider must be able to segregate information in case some confidential information must be available to the attorney, but not to law firm nonlawyer staff. And there must be a way to provide the information that must be shared with other parties in a secure way, they said.

Hibbard noted a flurry of concern recently over Dropbox, a company that specializes

in online storage and transferring of digital information, and whether information transferred through its service was viewable by Dropbox employees.

He and Teppler said cloud companies will offer encryption, but noted if the company gets hacked, its encryption is also vulnerable. They said lawyers can encrypt the data in their offices before transmittal, as an extra security precaution. Hibbard drily noted he's heard of cloud storage companies asking customers for encryption keys when they submit encrypted data and said he's seen users of encryption software select obvious passwords — which he likened to changing the locks on your house and then taping the key to the front door.

Teppler said lawyers should check with their insurance companies to see what's covered if data is stored in the cloud. The insurance company might claim the lawyer acted negligently and decline to provide coverage, if there's a breach of stored information.

And what's the cloud company's liability if there's a leak? "They may limit their damages to the cost of the subscription you pay for," Teppler said. "They basically exonerate themselves in advance from any problem that might arise from a data breach."

"Online security is an absolutely crazy, busy, evolving, still-frontier-dangerous place," he added. "The more you put your information in the cloud, the less control you have over it. The more control you have over it, the more you can guarantee its security."

Hibbert warns: "Probably my biggest concern is getting the legal community to understand that, one, it's a shared responsibility [with the cloud storage company] and, two, they need to be smart buyers. They need to protect themselves and their clients. If they don't do that, there's going to be serious problems. . . .

"If you whipped out your credit card and bought it [cloud storage] and that was the extent of it, you're going to get crucified at the other end of it."

## Cocoa Beach seeks special masters

The City of Cocoa Beach may adopt an alternate code enforcement system which gives special masters the authority to hold hearings and assess fines against violators of city codes and ordinances.

Applicants must be retired Florida judges or members of the Bar whose practices are substantially in the area of administrative, governmental, zoning, land use, or real estate law. The appointments will be for two year terms and the job pays \$125 per hour.

Applications are available at [www.cityofcocoabeach.com/bids](http://www.cityofcocoabeach.com/bids)

and must be mailed to City of Cocoa Beach Finance Department, P.O. Box 322430, Cocoa Beach 32932-2430 or delivered to the office of the Assistant City Manager/Chief Financial Officer, City Hall, 2 South Orlando Ave., Cocoa Beach 32931 no later than 2 p.m., October 24.

For more information contact only C.H. Holland, Jr., assistant city manager, P.O. Box 322430, Cocoa Beach 32932-2430, 321-868-3248, [cholland@cityofcocoabeach.com](mailto:cholland@cityofcocoabeach.com).