



North Carolina Proposed Ethics Opinion on Cloud Legal Practice Management and Time and Billing Applications

Originally published on Sui Generis--a New York law blog on May 3, 2010.

For attorneys and law firms considering using a cloud based legal practice management and time and application, a specific ethics decision from a state bar association has been a long time coming. We're happy to share encouraging news coming from the Tarheel State.

At long last a state bar ethics opinion tackled legal SaaS head-on. North Carolina issued "Proposed 2010 Formal Ethics Opinion 7: Subscribing to Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property"

In the document, the drafters of the proposed ethics decision pose the following questions, which goes right to the heart of the matter:

"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?"

SaaS means "Software as a Service", also known as cloud or Internet-based computing. And the answer is a win-win for users of Internet-based practice management and time and billing applications:

"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."

Then, there's the follow-up question, which is of equal importance for consumers:

"Are there any "best practices" that a law firm should follow when contracting with a SaaS vendor to minimize the risk?"

North Carolina echoes our own advice in this regard. Not all legal SaaS providers are created equal. Each law firm must conduct due diligence to ascertain the trustworthiness and reliability of their provider:

"Yes, a lawyer should be able to answer the list of questions below satisfactorily in order to conclude that the risk has been minimized."



- ▶ *What is the history of the SaaS vendor? Where does it derive funding? How stable is it financially?*
- ▶ *Has the lawyer read the user or license agreement terms, including the security policy, and does he/she understand the meaning of the terms?*
- ▶ *Does the SaaS vendor's Terms of Service or Service Level Agreement address confidentiality? If not, would the vendor be willing to sign a confidentiality agreement in keeping with the lawyer's professional responsibilities? Would the vendor be willing to include a provision in that agreement stating that the employees at the vendor's data center are agents of the law firm and have a fiduciary responsibility to protect client information?*
- ▶ *How does the SaaS vendor, or any third party data hosting company, safeguard the physical and electronic security and confidentiality of stored data? Has there been an evaluation of the vendor's security measures including the following: firewalls, encryption techniques, socket security features, and intrusion-detection systems?*
- ▶ *Has the lawyer requested copies of the SaaS vendor's security audits?*
- ▶ *Where is data hosted? Is it in a country with less rigorous protections against unlawful search and seizure?*
- ▶ *Who has access to the data besides the lawyer?*
- ▶ *Who owns the data-the lawyer or SaaS vendor?*
- ▶ *If the lawyer terminates use of the SaaS product, or the service otherwise has a break in continuity, how does the lawyer retrieve the data and what happens to the data hosted by the service provider?*
- ▶ *If the SaaS vendor goes out of business, will the lawyer have access to the data and the software or source code?*
- ▶ *Can the lawyer get data "off" the servers for the lawyer's own offline useful backup?*
- ▶ *If the lawyer decides to cancel the subscription to SaaS, will the lawyer get the data? Is data supplied in a non-proprietary format that is compatible with other software?*
- ▶ *How often is the user's data backed up? Does the vendor backup data in multiple data centers in different geographic locations to safeguard against natural disaster?*
- ▶ *If clients have access to shared documents, are they aware of the confidentiality risks of showing the information to others?*
- ▶ *Does the law firm have a back-up for shared document software in case something goes wrong, such as an outside server going down?*

After more than two years of providing web-based legal software, we're excited to finally see a forward thinking proposed ethics opinion that directly relates to our service. We appreciate the efforts of the committee and the detailed knowledge of cloud systems that Erik Mazzone, Director of Center for Practice Management at the N.C. Bar lent in the creation of these guidelines.

About the Author



Larry Port (www.rocketmatter.com/blog) is the Founding Partner and Chief Software Architect of Rocket Matter. A speaker and writer at the crossroads of the legal profession and cutting edge technology, Larry frequently discusses efficiency and quality techniques in the software industry that can be leveraged by law practitioners. He has published extensively in legal publications, including Law Technology News, Law Practice Today, ILTA's Peer to Peer, FindLaw, Chicago Lawyer, and others. Larry also conducts free monthly webinars on emerging topics for attorneys and speaks at bar association CLEs around the country.