ADMINISTRATOR'S ADVANTAGE

JULY / AUGUST 2015 ISSUE FOR THE GREATER CHICAGO CHAPTER OF THE ASSOCIATION OF LEGAL ADMINISTRATORS

INSIDE:
Technology Issue

10 Three Trends in Legal e-Discovery By: David Horrigan

12 The Era of Lean Training By: Doug Striker

14 The Value of Technology Transparency By: Mike Barry

18 Creating Collaboration Platforms for Law Firms By: Michael Silverman

36 Confidence in the Cloud By: Dylan Smith and Salvador Carranza

Confidence in the Cloud

By Dylan Smith and Salvador Carranza

The professional relationship between client and attorney depends on the ability to maintain client confidences. Yet the rise of the internet and the expanding use of mobile platforms, combined with the steady march of globalization, have made it ever more difficult to protect sensitive information. High profile data breaches have become an almost-daily occurrence. Given their status as repositories of personal and corporate secrets, law firms are increasingly attractive targets to hackers. At the same time, new technologies promise greater efficiency and responsiveness in the practice of law. It is within this challenging context that law firms of all sizes are adopting cloud-based computing services.

From the standpoint of the legal administrator, the first thing to recognize about cloud computing is that its use implicates the ethical responsibilities of attorneys. Indeed, one of those responsibilities is to ensure that the conduct of a non-lawyer employed or retained by a lawyer is compatible with the professional obligations of the lawyer. The question when and how a law office will use the cloud cannot merely be handed off to the legal administrator, without input from the firm's attorneys. Nor does it satisfy attorneys' ethical responsibilities simply to delegate decisions over cloud computing to a third-party vendor. Therefore, it is necessary for all legal administrators to have at a minimum a basic understanding of the technology behind cloud services.

In cloud computing there are three types of clouds: Public, Private, and Hybrid. A public cloud provides services and infrastructure off-site over the internet. With a private cloud, services and infrastructure are maintained on a private network. A hybrid cloud combines features of both public and private clouds. There are also various types of cloud services, including Infrastructure as a Service ("IaaS") and Software as a Service ("SaaS")—the two models most likely to be used by law firms. IaaS is a self-service model for accessing, monitoring, and managing remote datacenter infrastructure and allows a law firm to collect, store and use data remotely. Amazon Web Services, Microsoft Azure, and Google Compute Engine are examples of IaaS. SaaS makes up the largest cloud market and allows for the delivery of applications through the web, often with no downloads and only the use of a browser. Microsoft Office 365 and Google Apps are two Saas examples.

Armed with a basic understanding of cloud computing, a legal administrator, in consultation with the firm's attorneys, must take account of the ethical responsibilities implicated by the firm's use of the cloud. Fortunately, cloud computing has been around long enough that a number of state bar ethics agencies have had the opportunity to offer guidance on this question. Though there are nuances from state to state, that guidance is generally consistent in identifying certain ethical obligations that should be kept in mind as a legal practice adopts and makes use of cloud computing:

- *The duty to preserve client confidences.* The obligation not to disclose client confidences is at the core of the attorney-client relationship, and is perhaps the ethical responsibility most obviously implicated by the decision to put client materials in the hands of a third-party vendor of cloud services.
- *The duty to safeguard client property.* Lawyers have an obligation to keep client property "appropriately safeguarded." That obligation extends to the (often valuable or sensitive) information entrusted by the client to the attorney and other materials in the client file.
- *The duty to communicate.* Lawyers must "reasonably consult" with clients about the means used to achieve the client's objectives. Available ethics guidance, particularly more recent opinions, appear to recognize that client consultation may not be required in each instance involving use of the cloud. Nevertheless, particular circumstances—for example, the handling of particularly sensitive intellectual property—may dictate advance client consultation before the decision is made to store specific information on the cloud.
- *The duty of competence.* Lawyers owe their clients a duty of competent representation, which encompasses the obligation to "keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology." This responsibility requires attorneys to have some basic understanding of the cloud-related services they adopt—and to recognize when outside expert advice may be needed. After all, without that basic understanding, it is impossible to evaluate whether the attorney's use of cloud technology is consistent with the other ethical obligations outlined above.

These ethical obligations give rise to a number of practical considerations with regard to a law firm's use of cloud technology.

First, to fulfill the attorneys' ethical obligations, any law practice must exercise reasonable diligence in selecting a cloud service vendor and in reviewing the terms governing the services to be obtained. In selecting a vendor, the following areas, at a minimum, should be investigated: reputation and track record; financial stability; the existence of procedures and infrastructure to protect against unauthorized disclosure or theft of information; and the existence of procedures and infrastructure to prevent interruption of service or loss of information in the event, for example, of a natural disaster. It is also important to scrutinize the agreement (often called a "Service Level Agreement," or "SLA") that governs the terms of service. For

example, any attempt by the vendor to assert an ownership or security interest in data stored on the cloud would run afoul of the obligation to safeguard client property. Various state bar ethics opinions suggest a non-exclusive list of additional terms and conditions that should govern the relationship with any cloud vendor. These include the obligation to preserve security and to have protections against reasonably foreseeable attempts to infiltrate data, provisions concerning the handling of confidential data, an agreed method for data retrieval if the cloud vendor goes out of business or there is otherwise a break in continuity, and an obligation to host the data only within specified geographic areas with laws that afford adequate protection for data security and privacy.

Second, even when a vendor has been carefully selected and appropriate terms negotiated, any safeguards will be only as strong as the weakest link in the chain. Storing information in the cloud necessarily entails the need to access it. Therefore, a law firm that has opted to use the cloud should make sure that it has taken reasonable steps, with regard to its own policies and practices, to ensure compliance with the ethical obligations discussed above. Those steps should include training and technology to prevent data breaches at the law firm level. Ideally, a law firm should have alternate means of connecting to the internet so that client data can be accessed at all times. The firm should also have in place a plan to notify clients and appropriate authorities in the event a data breach occurs.

Finally, the use of cloud computing requires constant evaluation in response to changing technology and specific client imperatives. A matter involving particularly sensitive client information might trigger the obligation to obtain client consent to the use of the cloud, or might warrant additional security measures that have not previously been put in place. Further the obligation to stay abreast of the benefits and risks associated with relevant technology may very well require the law firm, from time to time, to reevaluate its use of cloud services.

In sum, cloud technology is a powerful tool that can enhance the provision of legal services. But, as with any other tool employed by the legal profession, the lawyer's ethical responsibilities must be at the forefront when a law firm decides to use any form of technology. All legal administrators must therefore ensure that when new technology is evaluated, they consult with their firm's lawyers, and inside or outside counsel with expertise in the technology and the applicable legal issues. A

Dylan Smith is a Partner in Freeborn & Peters' Litigation Practice Group. Prior to joining Freeborn & Peters, Dylan served as an Assistant United States Attorney in Chicago, where he prosecuted and tried criminal cases in federal district court.

Salvador Carranza is an Associate in Freeborn & Peters' Litigation Practice Group. He is also a "Certified Information Privacy Professional" in United States laws.