Cloudy with a Chance of Trade Secret Forfeiture

Brian Bouchard

Cloud computing has become ubiquitous. These days, every tech company seems to be promoting a cloud based service. And it makes sense; it sells. Who doesn't want the universal accessibility, cost saving programs, and unparalleled storage that cloud computing provides? Companies with valuable trade secrets, that's who.

Trade secrets are a burgeoning legal market. To obtain trade secret protection, information must meet three criteria: (1) it must be secret (i.e. not known or readily ascertainable); (2) it must derive an economic benefit from its secrecy; and (3) it must be the subject of "reasonable efforts" to maintain its secrecy. Disclosure of a trade secret compromises its protection and trade secret status. And once lost, this status is gone forever—you cannot rebottle a known secret.

As a result, trade secrets can be precarious. Introduce the uncharted legal territory of cloud computing, and the enterprise becomes fraught with risk.

What makes the combination of trade secrets and cloud computing so risky isn't that clouds are susceptible to hacking. To be sure, hacking is a risk. But there are many other risks that come simply from using a cloud service.

When a company uploads information to the cloud, it, arguably, discloses that information to a third party, or, at the very least, enables third party access. What prevents the cloud services provider from accessing or disseminating that information? Not as much as you might think. While some service contracts contain non-disclosure agreements, many do not. Some service contracts permit government agencies or private litigants to access stored information through a search warrant or subpoena without notice to the user. Companies embroiled in trade secret litigation may be hard pressed to argue that they adopted "reasonable efforts" to protect their trade secrets under these circumstances.

Even when protective measures are implemented, pitfalls may be lurking beneath the surface. For example, cloud service providers often reserve the right to alter contractual terms and services at will. Unless a company monitors and reviews such changes, it could unknowing be agreeing to substandard levels of protection. Other pitfalls to consider are termination and default. In some cases, protective services—to the extent such services exist—will cease upon termination of the service contract or when a default occurs, until the default it cured. This could leave a company's date vulnerable.

Other issues emerge when we consider how information is stored. Not all cloud providers segregate data according to consumer needs. When data is stored in a shared environment, the risk of disclosure and eventual forfeiture is amplified.

All this assumes, of course, that United States law controls—a bold assumption. Cloud servers are located throughout the world. This means that information stored in foreign servers may be

subject to foreign law. Most service contracts do not guarantee where information will be stored, making it impossible to anticipate variations in applicable law.

Moral of the story: avoid storing trade secrets in the cloud, especially public and semi-public clouds. Understandably, this directive is more complicated than it sounds. For some, the cloud is irresistible. For others, the cloud serves only as a productivity tool and not a storage bank. But even here, sensitive information can hitchhike to the cloud through e-mails, memos, and other shared documents.

Companies cannot eliminate the risk of cloud computing completely, but proactive measures can help mitigate risk. Any company using the cloud should, at a minimum, negotiate protective terms with the cloud service provider; review service contracts carefully (preferably with legal counsel and technical experts); ensure that the service contract legally obligates the provider to maintain confidential information; identify the cloud server's physical location(s); require the service provider to maintain data-protection insurance or maintain insurance itself; ensure that any protective measures survive termination or default; and restrict employee access to sensitive information stored in the cloud—only employees on a "need to know" basis should have access to such information.

Trade secrets are treasured commodities. Once gone, they can never be recovered. Treat your trade secrets accordingly and use precaution when cloud computing.