InsideCounsel.com
BUSINESS INSIGHTS FOR LAW DEPARTMENT LEADERS
FEBRUARY 26, 2015



Keeping secrets in the cloud: Are storms ahead for trade secret protection?

Companies must forecast how they can best protect their intellectual property as it moves into the cloud

BY ANDREA L. GOTHING, SETH A. NORTHROP, LI ZHU

Cloud computing is taking the world by storm as more and more businesses run their applications from remote and often vendor-owned servers over the Internet rather than local networks. In 2014, 69 percent of companies reported using the cloud for at least part of their infrastructure, up 12 percent since 2012. This is not surprising — the cloud's low initial cost and easy access attracts startups and growth-stage companies alike. Storing proprietary data on the cloud, however, creates unique legal and business risks, especially as companies consider trade secret protection in lieu of patent protection for their data. As a result, companies must forecast how they can best protect their intellectual property as it moves into the cloud.

Getting wind of trade secret protection

Traditionally, technology companies have protected their proprietary information from competitors either through patent protection or trade secret protection. With patent protection, the intellectual property is published as a public patent, and the company can prevent its competitors from practicing its invention for approximately 20 years. Yet, technology-related patents in certain sectors are becoming increasingly difficult to obtain and protect. In fact, there is a perception among some technology companies that the patent system itself is under assault in light of the recent Supreme Court case of *Alice Corp. Pty. Ltd. v. CLS Bank Int'l.*

Given the perceived uncertainty surrounding patent protection, many companies are taking a rain check, opting instead for trade secret protection or alternative ways to protect their intellectual property. In most states, "trade secrets" are defined as information, including formulas, programs, devices, methods, techniques or processes, that both derive independent economic value from not being generally known or readily ascertainable by others, and are protected by reasonable efforts to ensure secrecy under the circumstances. Technological information, such as proprietary software, often has no trouble meeting the first requirement, because such information is more valuable if nobody else has released it. The significant benefit of trade secret protection is that the owner can keep the information secret indefinitely, which can be critical for startups competing against well-funded industry leaders. Trade secret protection is also immediate and avoids expensive patent filing and prosecution fees.

In operation, trade secret law provides a startup with a legal mechanism to prevent competitors from misappropriating the company's trade secrets and money damages if misappropriation occurs. Specifically, in most states, an injured company can bring a misappropriation claim for money damages against a competitor or third party that acquires the company's trade secrets from a person who "knew or had reason to know" that the trade secret was acquired by improper means, such as theft, unauthorized disclosure or espionage. And the money damages can be substantial, with some verdicts reaching billions of dollars. But, while trade secret law can provide significant protection to companies moving their proprietary information to the cloud, the protection is only available if companies take reasonable efforts to ensure that information's secrecy.

Clear skies ahead?

Cloud computing is attractive to small companies and startups because it provides them with low-cost services without the large upfront investment in hardware, software and support. But one can readily imagine the risks — trade secrets and proprietary data are vulnerable to unauthorized access by hackers or even the vendor. In addition, most vendors will have some form of authorized access under the cloud contract's terms of service (TOS). Some legal commentators believe even this access may run afoul the second criteria for trade secret protection, which requires companies to use reasonable efforts to ensure the information's secrecy.

How, then, can companies, especially startups, exercise caution when storing their trade secrets in the cloud? As an initial matter, while the law on trade secret protection of data in the cloud has not fully developed, it is unlikely that courts will find that cloud storage is a per se unreasonable way to store trade secrets, even if an outside vendor obtains custody of that data. By way of example, several courts have recognized that disclosing trade secrets to a limited number of outsiders for a particular purpose does not forfeit trade secret protection.

Since courts have yet to weigh in on cloud computing in particular, safeguards are not a guarantee for success. Still, startups can exercise caution by taking a number of steps under their control.

First, inventory all trade secret materials. This includes identifying the "secret sauce" of your company's business, as well as design and other internal documents that may embody secret details. The company should then unambiguously mark these materials before transferring them to the vendor for cloud storage.

Second, fully vet the vendor. This means performing due diligence and investigating the vendor's physical and virtual security practices, track record, and recent intrusion testing results, among other things. Ask the important questions: Does the provider have extensive security measures to protect against hackers? Does the provider encrypt highly sensitive data? Is proprietary information segregated from other data? How up-to-date is the vendor's backup and

[InsideCounsel].com
BUSINESS INSIGHTS FOR LAW DEPARTMENT LEADERS
FEBRUARY 12, 2015

recovery system? Does the vendor have robust data deletion procedures? In short, the provider should be established, reliable and reputable.

Third, require the vendor to sign a confidentiality agreement. This confirms the vendor knows it is hosting trade secret information. Be wary of provisions in the TOS that disclaim this responsibility.

Last, consider negotiating service level agreements (SLAs) and audit rights. Customized SLAs may better align a company's expectations with those of the vendor, while providing a clear picture for evaluating the vendor's performance, and audit rights will ensure that the vendor is complying with advertised security policies.

A company's proprietary information is often the result of countless hours of sweat poured into constructing and refining efficient algorithms that distinguish their end product (and therefore, the company) from the competition. Startups should ensure that they have experts, either internal or external, who are well-versed in both patent and trade secret law, to protect the company's most valuable intellectual property. That way, the company will be "right as rain" when storing its data in cloud.

About the Authors

Andrea L. Gothing
Andrea Gothing is an attorney at Robins Kaplan LLP. She assists clients with complex technology-centric challenges including intellectual property, business, cybersecurity, and privacy litigation. algothing@robinskaplan.com

Seth A. Northrop
Seth Northrop is a trial attorney at Robins Kaplan LLP. whose practice focuses on intellectual property and global business and technology sourcing. He has substantial experience with complex business litigation involving various technologies including software and hardware design, analytics, networking, database, and E-commerce systems. sanorthrop@robinskaplan.com

Li Zhu
Li Zhu is an attorney at Robins Kaplan LLP. He assists clients with complex technology-centric challenges including intellectual property, business, cybersecurity, and privacy litigation. lzhu@robinskaplan.com