How to Protect Trade Secrets In The Cloud

By Andrew Martin

Although cloud computing often delivers reduced costs and increased flexibility, cloud customers now find themselves storing potentially sensitive data via someone else's applications, on someone else's databases, located at someone else's facilities. What used to be locked up in a filing cabinet in the basement is now…well…who knows where? And this loss of logistical control over company information can be troubling—especially for that most tenuous form of intellectual property: the trade secret.

The Uniform Trade Secrets Act (which most states have adopted) defines a trade secret as information that is the subject of efforts that are reasonable under the circumstances to maintain secrecy. So long as secrecy is maintained, the trade secret remains protectable under trade-secret law. This means that unlike other forms of intellectual property, trade secrets can remain protected indefinitely. The flip side of that coin, of course, is that public or other inadvertent disclosure of the trade secret can destroy its protectability and its value.

Combine the tenuous nature of the trade secret with the inherent uncertainty surrounding data processing and storage in the cloud, and it is not hard to see that storing trade secrets in the cloud can be fraught with risk. When moving to the cloud, the threshold question with respect to trade secrets is this: Does your trade secret data really need to be stored in the cloud? For those organizations that answer "yes" to that question, the following steps must be taken prior to moving forward:

1) Understand the technical details of how the cloud vendor processes, transmits, stores, and destroys customer data.
    - Customer data should be segregated.
    - Data should be encrypted using NIST-approved encryption methods.
    - Physical location of the data storage should be disclosed.
    - Robust data destruction policies should be in place.

2) Ensure the cloud agreement legally obligates the vendor to maintain the agreed-upon technical details and also provides an avenue for recovery if trade secret information is disclosed.
    - Vendor should warrant that it takes steps to ensure the security and confidentiality of your data.
    - Confidentiality terms should extend beyond the termination of the agreement.
    - Vendor should be liable for its employees, agents and subcontractors.
    - Most importantly, vendor should be required to maintain data-protection or cyber-liability insurance coverage at limits that are commensurate with the nature of the data being stored.

How the courts will address whether information stored in the cloud loses its trade secret status has yet to be determined. However, by addressing the issues above, a company will at least be in a better position, should it find itself trying to convince a judge that it took reasonable steps to maintain the secrecy of its trade secret stored in the cloud.

About the author Andrew Martin:

As an associate attorney with extensive prior experience advising information technology start-ups, Andrew's practice focuses on finding solutions for his clients' intellectual property issues. Due to his extensive experience in the software and technology industries, Andrew understands both the practical and legal issues involved in IP licensing agreements and disputes. In addition to licensing, Andrew helps his clients find new ways to use existing technologies to assist his clients in areas such as data privacy compliance. Andrew uses his diverse background which includes founding a record label and working for a world-wide concert promoter when counseling the firm's entertainment clients.

Get in touch: amartin@scottandscottllp.com | 800.596.6176

CLICK HERE for a complimentary subscription to Scott & Scott, LLP's bi-weekly ***Business & Technology Law*** newsletter.