NIESAR & VESTAL LLP
ATTORNEYS AT LAW

90 NEW MONTGOMERY STREET 9TH FLOOR
SAN FRANCISCO, CALIFORNIA 94105
TELEPHONE (415) 882-5300
FACSIMILE (415) 882-5400
www.nvlawllp.com

Law Alert

To: Firm Clients and Contacts

From: Niesar & Vestal LLP

Date: November 8, 2012

Re: **California Trade Secrets and the Cloud**

The cloud is a nascent data-hosting model experiencing explosive growth around the world. [1] Cloud services are cost-effective while providing increased accessibility and scalability to single users and large companies alike. Users considering cloud services must fully appreciate security risks that arise when trusting a third-party with sensitive information, particularly with regard to the storage of valuable trade secrets. Fundamentally, a trade secret is a legally protected business idea that derives its competitive advantage from secrecy. In order to protect trade secrets and other valuable data, users considering the storage of highly sensitive information in the cloud should understand the model and the security arrangements contained within the user agreement.

Following three years of drafts and interpretations, the National Institute of Technology officially defines cloud computing as a "model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable resources that can be rapidly provisioned and released with minimal management effort of service provider interaction." [2] Stated more simply, in the cloud model a provider centrally stores

---

[1] Pedro Hernandez, *IDC: Public Cloud Market to Reach $100B by 2016*, Datamation (Sept. 11, 2012), http://www.datamation.com/cloud-computing/idc-public-cloud-market-to-reach-100b-in-2016.html.
[2] National Institute of Standards and Technology (NIST) Special Publication 800-145, The NIST Definition of Cloud Computing (2011), available at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (establishing the official definition of cloud computing and listing possible service and deployment models).

user data and allows access to the data from nearly any Internet connected device. Three basic deployment models exist at the core of cloud computing: public, private, and hybrid clouds.

Based upon the idea of outsourcing IT infrastructure, the public model employs a third-party cloud provider that maintains physical servers hosting all user data, applications, and services. Users can easily scale their cloud subscription to meet storage or application needs including as e-mail, multimedia storage, virtual Windows desktop, or secure document collaboration. Providers charge relatively cheap rates for public clouds because each server is capable of hosting many cloud subscribers. Users no longer need to hire an IT staff or purchase and maintain the expensive computer infrastructure hardware. Analysts believe the $40 million public cloud market is the future of IT and will develop at a 26.4% compound growth rate to reach $100 million by 2016. [3] Amazon.com, Apple iCloud, DropBox, Google Cloud, Microsoft SkyDrive and OnLive are a few major providers poised to benefit from the explosive growth.

Private clouds function similarly to its counterpart, although rather than outsource, the cloud is hosted and implemented internally by the end user's IT department. Security is the greatest advantage of the private cloud, as keeping data within the company network eliminates trusting a third-party with sensitive data. Hybrid clouds are typically private clouds in which old or innocuous data is archived with a third-party public cloud provider. Given the hardware required to operate these types of clouds, large companies with existing IT infrastructure and personnel are ideal candidates.

Under California law, "'Trade Secret' means information, including a formula, pattern, compilation, program, device, method, technique, or process, that: 1) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and 2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy." [4] California law does not contain the Uniform Trade Secret Act requirement that a trade secret be "information not readily ascertainable," although authors of the law instruct courts to examine the requirement, if necessary. [5]

According to the Restatement of Torts, a trade secret loses protection upon appropriation through a breach of confidence or through improper means. [6] A breach of

---

[3] Hernandez, *Supra note* 1.
[4] Cal. Civ. Code § 3426.1(d) (West 2012).
[5] The California statute was amended in Legislative Committee to replace the "not readily ascertainable" language in favor of the phrase "the public or to." Drafters viewed the original wording as ambiguous; although the official comments expressly allow for the defense that information was "readily ascertainable" through "proper means." *See id.* official comments.
[6] Restatement (First) of Torts § 757, comment a (1939).

confidence occurs when a party divulges a trade secret in violation of an express or implied confidential relationship. [7] Such a breach may occur upon disclosure of company trade secrets during the course of or following employment. In order to balance preventing unfair competition and labor mobility, California law provides an exception to the state ban on non-compete agreements, providing that a former employer may not divulge trade secrets. [8]

Proper means of trade secret discovery include: public display, reverse engineering, independent invention, and published literature such as patent or other government filings. Cloud users must be particularly wary of the public display of trade secrets, as a New York court recently held that a company's customer list was not a trade secret because the company previously uploaded the data to the cloud and the customer information was accessible on a variety of social networks hosted in the cloud. [9] Although trade secret protection typically extends to customer lists, the court noted that perhaps the accessibility of personal information in the 21st century is broadening the definition of public information. [10]

Taking "reasonable efforts" to protect a secret is the primary method through which a company might demonstrate the existence of a trade secret. [11] Reasonableness is an imprecise standard that depends upon the foreseeability of the risk of misappropriation in each unique circumstance. [12] Although the owner of the trade secret bears the risk and consequence of actual loss of the secret, in the public cloud model responsibility of actually protecting against misappropriation shifts externally to a third-party provider. Traditional internal efforts such as express confidentiality agreements, security badges, and locked vaults are ineffective when a secret is accessible with a single company password or by commandeering access to an employee's mobile phone or tablet. A provider agreement based upon the results of a scrupulous risk assessment is the ideal way to ensure reasonable efforts in protecting secrets in the cloud.

When considering a cloud agreement it is important to realize that ultimate risk and responsibility for misappropriation cannot shift to the cloud provider. California business law mandates a minimum level of security by requiring that all businesses that transmit information to nonaffiliated third parties must include contractual provisions requiring the third parties maintain "reasonable" security measures. [13] The meaning of the term "reasonable" in the business law circumstance is disparate to the meaning in the

---

[7] Restatement (Third) of Unfair Competition § 41 (2012).
[8] Cal. Bus. & Prof. Code §§ 16600 (West 2012).
[9] *Sasqua Group, Inc. v. Courtney*, 2010 WL 3613855 (E.D.N.Y. Aug. 2, 2010).
[10] *Id*.
[11] 2 Callmann on Unfair Comp., Tr. & Mono. § 14:26 (4th Ed.)
[12] ***Id.***
[13] Cal. Civ. Code § 1798.81.5(c) (West 2012).

context of trade secret law, so clients must be proactive in taking security measures rather than relying upon third-party boilerplate language guaranteeing "reasonable" data security.

Taking reasonable precaution to protect information is particularly important when considering that cloud user agreements contain provisions disclaiming most provider liability. Courts are increasingly willing to enforce such liability clauses, leaving plaintiffs with no adequate remedy and sometimes without a basis on which to file suit. [14] Carefully reading the agreement is necessary as courts will not invalidate an agreement based upon the user's failure to fully understand the agreement and carefully consider the terms. [15]

Consider the Amazon user agreement, which places sole security responsibility on the user and states, "We strive to keep Your content secure, but cannot guarantee that we will be successful in doing so, given the nature of the Internet." [16] Deep within the Google user agreement is language granting Google a worldwide license in all uploaded content, even after the user ceases using the service. [17] In addition to protecting the provider from an improper means claim, agreements aimed at disclaiming confidentiality place users on notice that no confidential agreement exists, thus precluding a trade secret claim based upon a breach of confidence cause of action.

Potential users should consider how many employees would access the cloud and take measures to limit exposure to the trade secret. Employees bound by company confidentiality agreements are unlikely to appreciate how often secret information is uploaded, as protected information is sent to the cloud during routine data backup, collaborative projects, and even through certain e-mail clients. Internal company policies

---

[14] Timothy J. Calloway, *Cloud Computing, Clickwrap Agreements, and Limitations on Liability Clauses: A Perfect Storm?*, 11 Duke L. & Tech. Rev. 163, 169 (2012).

[15] *See* Nathan J. Davis, Note, *Presumed Assent: The Judicial Acceptance of Clickwrap,* 22 BERKELEY TECH. L.J. 577, 579 (2007) ("[A]bsent fraud or deception, the user's failure to read, carefully consider, or otherwise recognize the binding effect of clicking 'I Agree' will not preclude the court from finding assent to the terms.").

[16] *See Amazon Web Services Terms of Agreement 7.2*, Amazon, http://aws-portal.amazon.com/gp/aws/developer/terms-and-conditions.html, (Last Checked Sept. 11, 2012).

[17] *See Google Terms of Service – Policies & Principles*, Google, http://www.google.com/intl/en/policies/terms/, (Last updated Mar. 1, 2012). ("When you upload or otherwise submit content to our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content. The rights you grant in this license are for the limited purpose of operating, promoting, and improving our Services, and to develop new ones. This license continues even if you stop using our Services.").

must strike a careful balance between limiting employee exposure to critical information and stifling creation and productivity. Even the cloud providers must consider employee security, as hackers recently obtained the e-mail password belonging to an employee of DropBox. [18] The employee used the same password for all of her accounts and hackers easily accessed her personal cloud storage account and obtained a document with an undisclosed number of DropBox users' personal account information. Despite the well-publicized security breach, DropBox is doing well and recently announced that each day 110 employees overlook 500 million files belonging to 50 million users. [19]

In conclusion, companies reliant upon trade secrets should undergo a risk-assessment analysis in order to determine whether the cost-savings, accessibility, and scalability of the cloud business model outweigh the threat to confidential information. Despite the tremendous growth of the public cloud, a user must act wisely with regard to the storage of sensitive data. Currently user agreements benefit providers, yet as the cloud market becomes more saturated competition will surely necessitate provider concessions in the form of more favorable agreement terms. Only through an individualized and diligent analysis will a user have the proper timing and best opportunity to smoothly and securely transition into the future of IT.

If you would like to speak with a Niesar & Vestal attorney about any matter discussed in this law alert, please contact Stephen Rush (srush@nvlawllp.com), Oscar Escobar (oescobar@nvlawllp.com) or Jay Begler (jbegler@nvlawllp.com).

---

[18] Nicole Perlroth, *Dropbox Spam Tied to Stolen Employee Password*, N.Y. Times, Aug. 1, 2012 (*available at* http://bits.blogs.nytimes.com/2012/08/01/dropbox-spam-attack-tied-to-stolen-employee-password/).
[19] *DropBox Fact Sheet*, DropBox, http://www.dropbox.com/static/docs/DropboxFactSheet.pdf, (Last Checked Sept. 11, 2012).