Managing and Protecting Information (including Trade Secrets) in the Cloud

Robert B. Milligan

Biographical Information

Robert Milligan

Mr. Milligan is a Los Angeles, California based partner in the Litigation and Labor & Employment Departments of Seyfarth Shaw LLP. His practice encompasses a wide variety of commercial litigation and employment matters, including general business disputes, unfair competition, trade secret misappropriation and other intellectual property theft. Mr. Milligan has represented clients in state and federal courts in complex commercial litigation and employment litigation. His experience includes trials, binding arbitrations and administrative hearings, mediations, as well as appellate proceedings. Mr. Milligan also provides advice to clients concerning a variety of business and employment matters, including non-disclosure, non-competition, and invention assignment agreements, corporate espionage, and trade secret and intellectual property audits.

Mr. Milligan is an iTechLaw member as well as a Vice Chair of the Intellectual Property section. He is also a member of the State Bar of California Intellectual Property Law Section Executive Committee. He also served as a contributing editor of Trade Secret Litigation and Protection in California and is an author of chapters in Continuing Education of the Bar's Trade Secrets Practice in California. He frequently lectures and writes on timely trade secret and other intellectual property issues. He is the co-editor of his firm's trade secret blog, www.tradesecretslaw.com.

Introduction

The explosion of cloud computing has provided companies with many technological benefits; but with those well recognized benefits, there are incumbent risks to valuable company data, including prized trade secrets. Companies utilizing cloud computing must employ effective measures to protect and secure their intellectual property. Vendor agreements with cloud providers should be carefully scrutinized to ensure that appropriate contractual provisions are in place to protect company data, including provisions addressing ownership, access, protection, and privacy from both a national and international perspective. Companies should attempt to incentivize their contractual arrangements with vendors to ensure that their business objectives, including secure data protection are met. Social media, which uses cloud computing, has also provided companies with access to a dynamic platform for business growth. To effectively navigate in this new environment, companies must ensure that they adopt effective policies that foster creative expression yet protect company data and secrets, including employment policies with clear direction and guidance for employees. Sensible executives will seek advice from competent counsel to ensure that the cost savings and financial opportunities in cloud computing, including social media, are not outweighed by the potential legal and business risks.

Robert B. Milligan
Los Angeles, California, April 18, 2011

Cloud computing is the hot technology movement. Gartner Group states it is the number one business and technology priority for 2011 and over 43% of Chief Information Officers expect to move their data and utilize cloud services within the next few years.[1] MarketsandMarkets estimates that the cloud computing market will grow from $37.8 billion in 2010 to $121.1 billion in 2015.[2] Verizon recently spent $1.4 billion to acquire cloud services provider Terremark Worldwide, Inc., which is expected to stimulate other rival carriers to enter the cloud industry.[3] However, the new cloud computing buzz is not new technology to many industry insiders. In fact, as Larry Ellison of Oracle stated, it is "[e]verything that we already do."[4]

Cloud computing is a metaphor for the internet. It comes from the early days when network engineers used a cloud to indicate unknown domains. The engineer knew the domain was there, but the details of that domain were unknown. This network of clouds is how we view the internet today. Cloud service users know their information is readily accessible, but generally lack any interest

[1] According to a 2010 survey, http://www.gartner.com/it/page.jsp?id=1526414.
[2] http://www.marketsandmarkets.com/Market-Reports/cloud-computing-234.html.
[3] http://news.businessweek.com/article.asp?documentKey=1376-LFPBHT6JIJUX01-4B7UIEITJ82MA34J8V0CJMEHFP.
[4] Quoted in the Wall Street Journal, September 26, 2008.

where it is physically located. Cloud service users can generally access their information at any place, at any time, and on any device, as long as they have an internet connection. Indeed, cloud computing is part of our every day lives. If you have performed a Google search, checked Yahoo email, or signed in to Facebook, Twitter, or LinkedIn, you have reached into the cloud.

Cloud computing lacks a universal definition. Ask different individuals working in the IT industry what cloud computing is and you will get different answers. The National Institute of Standards and Technology (NIST) has provided the most widely accepted definition of cloud computing: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[5] The NIST also notes five essential characteristics of cloud computing services: On-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.[6]

Cloud computing has numerous technical benefits. Users typically pay the cloud provider for the services and resources they use. This pay-as-you-go infrastructure allows companies to reduce costs. Companies can avoid paying for costly equipment, personnel, and maintenance. For example, if a company needs additional storage space for its data, it can purchase more from the

[5] NIST Definition of Cloud Computing, v. 15, http://csrc.nist.gov/groupsSN/Sloud-computing/.
[6] Identified by NIST as part of its definition of Cloud Computing.

cloud provider. Without cloud computing, the company may have to pay for additional servers, allocate space for bulky servers, and higher additional IT staff, among other costs. Cloud computing also provides scalability. The ability to adapt and quickly respond to increased market demands is invaluable to small companies who lack the finances to significantly invest in expensive IT infrastructure. The on-demand access provides access wherever a cloud user has a network connection. This mobility and convenience is one of the reasons low cost netbooks and tablet devices, such as iPads, have rapidly radically increased in popularity. Companies are embracing the cloud as a cost effective way to do business. Specifically, it provides smaller companies with a better chance to compete.

Cloud computing involves three general service models. The simplest model is Infrastructure as a Service (IaaS). This involves basic storage and data hosting. The second model is Software as a Service (SaaS). In this model, the cloud provider provides the software to access, manage, and utilize the data. For example, this is commonly seen with email (e.g. Gmail, Yahoo mail, Hotmail) and social media sites (e.g. Facebook, LinkedIn, Twitter). The third model is Platform as a Service. This model provides an operating system in which the company can develop and build its own applications. For example, Facebook allows third parties to build and distribute applications within its service. The main factor distinguishing the three models is the level of control the subscriber retains over its data.

While cloud computing is not new, expansive and accelerated network connectivity has fueled the ascent of this technology movement. Companies embracing cloud computing will move data previously stored in house, into servers provided by third parties. However, moving confidential and proprietary information, such as trade secrets, raises numerous legal, security, and business concerns.

Trade Secrets

A trade secret is any information not generally known, that is economically valuable, and subject to reasonable efforts to maintain its secrecy.[7] Many people think of secret formulas, such as the ingredients for Coca-Cola, KFC, or WD-40. Yet trade secrets can also include a wide variety of technical and nontechnical information. Common trade secrets include manufacturing methods, formulas, techniques, business and marketing plans, customer lists, and computer programs. There is no requirement to register or publish a trade secret to receive protection. Additionally, a trade secret does not have to involve novel information. The heart of the trade secret's value is its secrecy.

A trade secret owner must take reasonable efforts to ensure the information's secrecy.[8] He or she must take actual efforts to protect the trade secret so that the trade secret is not lost through improper, illegal, or unethical means. The burden is on the trade

[7] *See e.g.* 18 U.S.C. § 1839 (3) (A), (B) (1996); Cal. Civ. Code § 3426.1(d).

secret owner to keep the information secret. Furthermore, he or she cannot expect others to hold a higher obligation to keep the information secret.

Trade secret law protects against misappropriation, i.e., the illegal or unauthorized acquisition, disclosure, or use of information. Trade secrets are creatures of statute and protected under several laws such as the Uniform Trade Secrets Act (UTSA), Economic Espionage Act of 1996 (EEA)[9], and the Computer Fraud and Abuse Act (CFAA).[10] Varying versions of the UTSA are enacted in forty-six states in the United States.

Trade secret law holds third parties liable if they knew or had reason to know of misappropriation.[11] However, it does not generally protect against the accidental disclosure or the reverse engineering of a trade secret.[12] For example, if a trade secret is accidentally disclosed by a cloud provider or third party, it could potentially lose its trade secret status if the data leak is not promptly and effectively addressed.

Unlike patent, trademark, or copyright protection, there is no set time period for trade secret protection. A trade secret is protected as long as it is kept secret. However, once a trade secret is lost, it is lost forever. As we have seen in a post-Wikileaks

---

[8] *J. T. Healy & Son, Inc. v. James A. Murphy & Son, Inc.*, 357 Mass. 728, 730-31 (1970).
[9] 18 USC § 1831.
[10] 18 USC § 1030.
[11] See *Kozuch v. CRA-MAR Video Ctr., Inc.*, 478 N.E.2d 110 (Ind. Ct. App. 1985).
[12] *Kewanee Oil Co. v. Bicron Corp.*, 94 S. Ct. 1879, 1883 (1974).

world, once confidential information is disclosed, it can be posted online for hundreds of millions to see, access and download.[13]

Problems

An issue with new technology is that the law is constantly behind. "[Courts] try to keep up with technology and understand it, but things move so quickly."[14] The use of cloud computing raises several problems for trade secrets. The heart of a trade secret's status is its secrecy. Thus, placing confidential information in the hands of a third party cloud provider seems contrary to maintaining secrecy. Moreover, information placed into the cloud increases the risk that the information will be accidentally or intentionally disclosed to third parties.

One threshold issue is whether confidential information placed into the cloud diminishes its status as protectable information. In other words, can trade secrets lose their protection in the cloud? The answer may vary depending on the nature of the information and who places the information in the cloud. Courts have used six factors to determine whether a piece of information is secret. These comprise: (1) the extent to which the information is known outside the company, (2) the extent to which the information is known by employees and others inside the company, (3) the extent of measures taken by the company to protect the secrecy of its information, (4) the value of the

[13] WikiLeaks website publishes classified military documents from Iraq, http://articles.cnn.com/2010-10-22/us/wikileaks.iraq_1_wikileaks-website-classified-documents-iraq-wiki-leaks-iraqis?_s=PM:US.

information to the company and competitors, (5) the amount of time, effort, and money expended by the company in developing the information, and (6) the ease of difficulty with which the information can be properly acquired or duplicated by others.[15]

A recent New York district court found a company's customer list was not a trade secret because the information at issue had already been disclosed in the cloud. In *Sasqua Group v. Courtney*, 2010 WL 3613855 (E.D.N.Y. Aug. 2, 2010), an executive search consulting firm alleged that a former employee stole confidential customer information from a client database and later solicited those clients. The confidential database contained client contact information, individual profiles, resumes, descriptions of interactions with clients, and hiring preferences. The court focused on the sixth factor in the six-factor analysis; i.e. the ease of difficulty the information could be properly acquired by others. The defendant former employee demonstrated how easily she could find the same client database information by searching Google, LinkedIn, Bloomberg.com, and FX Week. The court found the client database did not constitute a trade secret. In doing so, the court noted that the protection of certain information may

---

[14] Judge Alex Kozinski, Ninth Circuit U.S. Court of Appeals, speaking at Golden Gate University's Intellectual Property Distinguished Speaker Program, April 13, 2011.

[15] These factors are the "most-cited listing of the objective criteria for determining the existence of a trade secret." *M. Jager*, Trade Secrets Law § 5.05 (1995).

no longer be viable in the 21st century in light of new technologies.[16]

Another issue arises when cloud providers use the hosted information for secondary purposes. For example, information containing customer lists or contact information are highly valuable for market studies and behavioral targeting. Providers can earn substantial revenues reselling this raw data to advertisers and other third parties.

Additionally, and perhaps more threatening to trade secrets, are cyber attacks. Hackers have recently targeted their attacks towards corporate trade secrets and proprietary information. McAfee recently reported on the Night Dragon cyber attacks that have targeted oil and gas industry trade secrets.[17] IBM's X-Force cyber security team also reported that cybercriminals now pinpoint valuable corporate data.[18] There is a thriving criminal market for converting stolen trade secrets into cash.[19] In fact, criminal gangs in China, Russia, and the Ukraine will steal information for companies looking to undercut their rivals.[20] Hackers are eagerly awaiting more corporations to embrace cloud computing and release prized data into the cloud.

---

[16] *Sasqua Group v. Courtney*, 2010 WL 3613855, *22 (E.D.N.Y. Aug. 2, 2010).
[17] Global Energy Cyberattacks: "Night Dragon," http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf.
[18] Available at http://www-03.ibm.com/security/landscape.html.
[19] http://www.usatoday.com/tech/news/2011-03-31-hacking-attacks-on-corporations.htm.
[20] http://www.usatoday.com/tech/news/2011-03-31-hacking-attacks-on-corporations.htm.

The risks of cloud computing were demonstrated with the recent Epsilon security breach; potentially one of the biggest in United States history.[21] Epsilon is one of the largest permission based email marketing companies. It sends over 40 billion emails each year on behalf of over 2,500 clients. Its clients include US Bank, Capital One, Chase, Citi, JPMorgan, Best Buy, Hilton, Target, and Disney. On March 30, 2011, Epsilon detected the unauthorized entry into its customer databases. Hackers obtained access to thousands of names and email addresses. As are result, these hackers have the ability to send highly effective spear-phishing emails.[22]

For instance, the following scenario could arise from the Epsilon or other cloud computing breaches: (1) hacker reviews improperly obtained customer information and discovers that the customer works at a large corporation, (2) hacker crafts a well designed email posing as the company the client gave their email address (e.g. Best Buy, Target, Citi), (3) customer opens the email at work, clicks a provided link, and undetectable software is downloaded onto the customer's computer, and (4) undetectable software quietly sits inside the corporate network, searches for trade secrets or confidential information, and sends it back to the hacker.

---

[21] Epsilon data security breach expands, could be history's largest, http://www.digitaltrends.com/computing/epsilon-data-security-breach-expands-could-be-historys-largest/.

[22] Epsilon hacking shows new "spear-phishing" risks, http://www.reuters.com/article/2011/04/04/us-hackers-epsilon-idUSTRE7336DZ20110404.

Aside from the intentional theft by outside parties, trade secrets have always been susceptible to misappropriation by current or former employees. The typical case involves the disgruntled employee who discloses or uses trade secrets after termination. Yet, the use of cloud services such as social media increase the risks of both intentional and accidental disclosure by such employees.

A related issue involves the ownership of data. If a provider or employee modifies the data, do they have any ownership rights? Taking the case of a customer list, if an employee friends clients and adds them to a LinkedIn profile, does the contact belong to the employee or the employer. Consequently, if the employee leaves his or her employer, can the employee later contact previous clients? This issue is currently the dispute in *TEK Systems v. Hammernik*, No 0:10-cv-0081, (D. MN, 2010).

In *TEK Systems*, the plaintiff, an IT staffing firm, alleged that a former employee violated a non-solicitation agreement when the employee contacted previous clients on LinkedIn. The non-solicitation agreement lacked any social media restrictions. The issue is whether the employee violated the agreement when she allegedly contacted the clients through her personal social media account during her employment, and then allegedly later contacted the clients after she left for a competitor. The case is scheduled for trial August 2011 and it deserves watching.

The nature of trade secrets as digital information within the cloud raises potential litigation concerns. For example, data is

often transitory, moving between various servers and facilities. Trade secrets may move from state to state, and even across international borders. Thus, difficulties may arise in establishing jurisdiction in instances of trade secret theft. Moreover, a cloud provider's obligation to comply with e-Discovery demands may compromise the integrity of trade secrets or confidential information if secrecy protections such as protective orders and confidentiality agreements are not employed.

Finally, problems may arise with data access continuity. What happens when the contract or subscription for cloud services terminates? The cloud provider may withhold data when a company fails to pay for services. Additionally, what happens when a small startup provider goes bankrupt or is purchased by another company? These and many of the problems discussed above may be addressed with effective and well drafted contracts as part of a well developed cloud computing strategy before placing your company's data in the cloud.

Solutions

The problems of storing data in the cloud are not insoluble. The first step is to conduct a trade secret audit or inventory before placing information in the cloud. Determine what information is sensitive and confidential. Highly valuable trade secrets can remain off the cloud and stored in house on secured networks or physical areas. Keeping information out of the cloud inherently reduces the risk it will not be disclosed on the cloud. When in doubt, don't make the information able on the cloud. To the extent that you determine that certain trade secret information can be

placed in a secure cloud, keep track of such data, as well as the security measures in place to protect such data (encryption, confidentiality designations, written agreements, etc.) and who has access to such data.

Once you decide to utilize cloud computing, take all prudent and necessary measures to select the correct provider. Perform diligent checks on all potential providers. Obtain references. Determine whether they have the capabilities to provide the type of services you desire. Conduct interviews with the providers. Find out their financial viability. View their security and privacy policies and discover how many security breaches they have experienced. Determine whether your data will be encrypted. Determine whether your cloud provider contracts its services with third parties. Evaluate choice of law, choice of forum, and indemnification provisions carefully. Security rather than price should be your top priority. Try to incentivize the cloud provider's conduct to keep your information absolutely secure. You may want to consider diversifying your portfolio of data stored on the cloud with multiple providers or backup all information stored in the cloud locally .

State law may require you to contract with the cloud provider to ensure reasonable security procedures and practices are in place. California requires businesses that possess personal information about California residents to implement and maintain reasonable security procedures and practices.[23] Business that disclose this personal information to third parties (e.g. cloud

[23] Cal. Civ. Code § 1798.81.5.

providers) must contract with the third party to implement and maintain reasonable security procedures and practices. Massachusetts also requires contracts to implement and maintain appropriate security measures when providing personal information to cloud providers.[24] Nevada requires businesses to use encryption on data storage devices that contain personally identifiable information.[25]

After the provider is chosen and a trade secret audit or inventory has been conducted, the best way to protect trade secrets and other information is through well drafted contracts and policies and periodic audits of the cloud provider. This includes contracts with both cloud providers and the company's internal employees who may access the information. First, define the ownership rights in the data. For example, you may want to explicitly state that the cloud provider and employees have no ownership rights in the data. The agreement can state that the provider and employees have limited access to the data only for certain reasons. Defining the limits of authorization can also help establish rights under the CFAA if the provider or employee violate the scope of their authorizations. Next, define the scope of the protected information. Specifically indicate which information is considered trade secret or confidential. The Economic Espionage Act's language may be preferred because it provide a broad trade secret definition. Also include language protecting confidential and propretiary data. Prohibit the unauthorized use or disclosure of company data, including trade

[24] 201 C.M.R. 17.00 et seq.

secrets and confidential and proprietary information. Contracts can also provide for injunctive relief, liquidated damages, arbitration, and attorneys' fees.

Companies should also control access to their data. Agreements with cloud providers should restrict the use of data to outside vendors or third parties. Provisions should also hold the provider and any subcontractors liable for security breaches. This is especially important in light of the recent Epsilon security breach. Companies should require heightened security standards by providers such as ISO standards. These standards represent an international consensus on good quality management practices. For example, they require quality audits, effective training, and corrective actions for problems. Additionally, the Federal Trade Commission has provided 5 key principles for sound data security plans: (1) know the personal information you have, (2) scale down and keep only what you need, (3) protect the information you want to keep, (4) properly dispose of what you no longer need, and (5) create a plan to respond to security incidents.[26]

Contracts should include ongoing confidentiality obligations in case of termination. Additionally, contracts should require the return or deletion of any copies of the data (as appropriate) by the provider or employee after the termination of the agreement. Finally, there should be a provisions prohibiting the withholding of data by the provider or employee in the case of a dispute.

---

[25] Nev. Rev. Stat. 603A.010 et seq.

[26] http://www.ftc.gov/bcp/edu/microsites/infosecurity/.

As part of a comprehensive policy to address data protection in the cloud, companies should establish effective security and social media policies to prevent the disclose of information by employees. Information security measures include password protection, email and electronic data policies, departmental trainings, and exit interviews to remind employees of confidentiality obligations.

Social media policies are even more critical today with explosion of social media in the workplace. Well drafted and communicated policies can effectively reduce the amount of sensitive information disclosed both accidentally and intentionally on the internet. Social media policies can restrict employees from posting confidential information on sites such as Facebook, Twitter, or LinkedIn. Employees should be educated about the implications of posting information to these sites through recurring training. For example, Facebook grants itself a license to any information posted on its site.[27] Twitter grants itself a license to make any posted content available to other companies.[28] Employers should provide constant reminders to employees not to disclose confidential data on such sites.

Employers should, however, be very cautious in the drafting of their social media policy. In fact, an overly broad policy may violate employee rights. Section 7 of the National Labor Relations Act protects both unionized and non-unionized employees right to engage in concerted activities in the United States. The National Labor Relations Board (NLRB) has recently criticized two social

[27] http://www.facebook.com/terms.php.

media policies as being overly broad and violative of employee rights.

In *NLRB v. American Medical Response of Connecticut*, an employer terminated an employee who allegedly posted negative remarks about her supervisor on Facebook.[29] The employer's policy prohibited employees from describing the company in any way on the internet without its permission. The NLRB alleged that this policy violated the employees right to engage in concerted activities and discuss her work environment. The parties eventually reached a settlement and thus the NLRB did not officially pronounce the illegality of the employer's policy.

In *NLRB v. Thomson Reuters Corp*, an employee was disciplined for criticizing management on Twitter.[30] The NLRB alleged that the company's social media policy chilled the employee's rights to discuss working conditions.

Employers should employ specifically tailored social media policies that protect trade secrets and confidential information. Employers should distance the company from personal social media use by employees that attempts to associate the employee with the company. For example, employers should prohibit the use of company trademarks, graphics, or logos for personal use. Companies should also prohibit, or at least limit, the use of

---

[28] http://twitter.com/tos.

[29] *American Med. Response of Conn.*, NLRB Reg. 34, No. 34-CA-12576, *complaint issued* 10/27/10.

[30] The NLRB told Thomson Reuters on [April 6, 2011] that it planned to file a civil complaint accusing the company of illegally reprimanding a reporter over a public Twitter posting she had sent criticizing

company provided email addresses for personal social media activity. Companies must be vigilant to ensure that their cloud computing policies and agreements, including social networking policies, remain current with changing technology to protect their most valuable assets.

Conclusion

Cloud computing provides significant benefits for the development and growth of businesses. Companies that embrace this technology and venture into the cloud must be careful and thoughtful. Companies should scrutinize what they put into the cloud and select reliable and security conscience cloud providers. Well drafted agreements and policies with both providers and employees can help reduce the risk of the disclosure of trade secrets in the cloud. A comprehensive cloud computing strategy can help companies realize the cost savings and financial opportunities in cloud computing, including social media, while ensuring that these benefits are not outweighed by the potential legal and business risks.[31]

---

management.
http://www.nytimes.com/2011/04/07/business/media/07twitter.html.

[31] A special thanks to Joshua Salinas, an IP law clerk, for his assistance with this article.