AMERICAN BAR ASSOCIATION
Section of Litigation
Intellectual Property

Protecting Trade Secrets Stored in the Cloud

By Benjamin J. Bradford, Justin A. Maleson, and Michael T. Werner
March 28, 2014

As cloud computing has become a ubiquitous part of our personal and professional lives, businesses are rethinking how they store and protect their trade secrets. Over the past 30 years, trade secrets have moved from locked file cabinets and desk drawers, to floppy disks and PCs, to Dropbox and Google Docs. While the many benefits of cloud services are driving the current explosion in popularity, there are a host of related issues that businesses should consider when storing sensitive and valuable information in the cloud. This article provides a brief introduction to cloud computing and trade-secret law, before identifying challenges and practical tips for maintaining and protecting trade-secret information in the cloud. This article also discusses ways to preserve trade-secret status in the event of unauthorized use or disclosure, and during the course of litigation.

What Is Cloud Computing?

Gartner, Inc., a leading information technology research and advisory firm, defines cloud computing as "a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using Internet technologies." Gartner IT Glossary (last visited Jan. 24, 2014). Simply put, data on the "cloud" are accessible anywhere there is an Internet connection.

Cloud computing is now a way of life for many of us. It provides a way for friends and families to share photographs and videos, for employees to collaborate on documents while working from different parts of the world, and for businesses to store their sensitive information in a way that allows for on-demand access to the information. As companies increasingly turn to the cloud, it is important to understand what steps they can take to protect their trade-secret and confidential information.

What Is a Trade Secret?

Fundamentally, a trade secret is information that provides a business with a competitive advantage as a result of other businesses not having that information. While the secret formula for Coca-Cola is the classic example of a trade secret, it is not the type of trade secret generally stored in the cloud. Instead, customer lists, computer source code, and product designs and schematics are examples of information commonly stored in the cloud today. Unlike patent and copyright protections, which provide owners with certain legal rights only after disclosure (to the Patent and Trademark Office and Copyright Office, respectively), "[w]hether the information sought to be protected qualifies as a trade secret focuses fundamentally on the secrecy of such information." Thermodyne Food Serv. Prods., Inc. v. McDonald's Corp., 940 F. Supp. 1300, 1304 (N.D. Ill. 1996) (emphasis by court).

With the exceptions of New York and Massachusetts, every state has adopted a version of the Uniform Trade Secrets Act (UTSA), which defines a "trade secret" as information that (1) "derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, 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." UTSA § 1 (1990).

Here, we touch on the economic value requirement before focusing primarily on the reasonableness of steps taken to maintain secrecy, which is critical to the issue of protecting trade secrets in the cloud. (For a more detailed discussion of trade-secret law, along with practical suggestions for counseling clients and defending or prosecuting trade-secret misappropriation claims, see Debbie L. Berman et al., Understanding and Litigating Trade Secrets: An Outline for Analyzing the Statutory and Common Law of Trade Secrets in Illinois (2011)).

What does it mean to derive economic value from not being generally known or readily ascertainable by proper means? For information to qualify as a trade secret, the owner must derive value from the information's secrecy. Stated another way, "the real value of the information 'lies in the fact that it is not generally known to others who could benefit [from] using it.'" Sys. Dev. Servs., Inc. v. Haarmann, 907 N.E.2d 63, 73 (Ill. App. Ct. 2009) (applying Illinois version of UTSA). Once a court determines that the information is secret, "[e]ven a slight competitive edge will satisfy [the] [economic value] requirement of trade secret protection." ISC-Bunker Ramo Corp. v. Altech, Inc., 765 F. Supp. 1310, 1333 (N.D. Ill. 1990). For example, one court denied a defendant's summary- judgment motion on a trade-secret claim where the evidence showed that the plaintiff had increased its revenues through its use of a trade-secret program for treating mental-health patients, and that the defendant could potentially gain additional patients by using that program. See Reliant Care Mgmt., Co. v. Health Sys., Inc., No. 4:10CV38 CDP, 2011 WL 4342619, at *9 (E.D. Mo. Sept. 15, 2011).

What does it mean to take reasonable steps to maintain secrecy? Courts will not protect information that is left exposed to the public. See Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 179 (7th Cir. 1991). Accordingly, the reasonableness of steps taken to ensure secrecy often is the most important factor in determining whether information qualifies for trade-secret protection. Because the question of whether steps are reasonable "depends on a balancing of costs and benefits that will vary from case to case," Learning Curve Toys, Inc. v. Playwood Toys, Inc., 342 F.3d 716, 726 (7th Cir. 2003), there are no hard-and-fast rules for determining whether an owner has taken reasonable steps to protect the secrecy of its information. That said, courts evaluating reasonableness commonly consider whether the owner has taken steps that include the following:

- Limiting who has access to trade secrets. See, e.g., Lincoln Park Sav. Bank v. Binetti, No. 10 CV 5083, 2011 WL 249461, at *2 (N.D. Ill. Jan. 26, 2011).

- Requiring third parties with access to trade secrets to sign confidentiality agreements. See, e.g., PRG-Schultz Int'l, Inc. v. Kirix Corp., No. 03 C 1867, 2003 WL 22232771, at *6 (N.D. Ill. Sept. 22, 2003).

- Requiring employees to sign nondisclosure agreements (NDAs) and participate in training and exit interviews. See, e.g., Matter of Innovative Constr. Sys., Inc., 793 F.2d 875, 884 (7th Cir. 1986); Hexacomb Corp. v. GTW Enters., Inc., 875 F. Supp. 457, 465 (N.D. Ill. 1993).

- Affixing confidentiality labels to trade-secret documents and files See, e.g., Huawei Techs. Co., Ltd. v. Motorola, Inc., No. 11-cv-497, 2011 WL 612722, at *9 (N.D. Ill. Feb. 22, 2011).

- Enforcing known violations of confidentiality agreements. See, e.g., Diamond Power Int'l, Inc. v. Clyde Bergemann, Inc., 370 F. Supp. 2d 1339, 1348 (N.D. Ga. 2005).

- Taking prompt action to halt any public exposure of trade secrets, such as by sending cease-and-desist letters or initiating litigation. See, e.g., Lockheed Martin Corp. v. L-3 Commc'ns Corp., No. 1:05-CV-902-CAP, 2008 WL 4791804, at *12 (N.D. Ga. Sept. 30, 2008); Alamar Biosciences, Inc. v. Difco Labs., Inc., No. CIV-S-94-1856 DFL PAN, 1995 WL 912345, at *6 (E.D. Cal. Oct. 13, 1995).

With more and more companies storing sensitive information in the cloud, the need to practice diligence in protecting that information is as important as ever.

Potential Challenges and Tips for Storing and Protecting Trade Secrets in the Cloud

Unlike confidential information locked in file cabinets and stored on desktop computers in the days when it was relatively easy to limit the universe of people with access, information stored in the cloud is potentially accessible to anyone with Internet access, at any time, and from anywhere in the world. While hackers are often thought of as the primary threat to secrecy, that is not the case in most situations. In fact, a hacker's attack may not deprive an owner of legal trade-secret protection, as long as reasonable steps and proper precautions were taken by the owner, including prompt remedial measures to halt and limit disclosure. Third-party cloud service providers and company employees often pose the greatest threats to secrecy (sometimes as a result of seemingly innocuous conduct). Accordingly, this section addresses the reasonableness of steps taken to limit access and maintain the secrecy of information stored in the cloud, and identifies steps to consider for avoiding or minimizing risks.

Cloud service providers.

Reasonable steps should be taken to ensure that a cloud service provider has only as much access to company information stored in the cloud as is necessary, and that both the company and provider are doing everything possible to maintain the information's secrecy. Companies that store trade-secret information in the cloud face certain risks related to the use of a third-party provider, including (1) boilerplate terms of service that allow providers to access any information uploaded to the cloud and (2) rogue employees of the provider.

For example, cloud providers often ask users to agree to terms of service that grant the provider access to any information stored in the cloud. This means that the security of the company's information is only as strong as the security offered by the provider, and even some of the best-known and widely used providers have suffered information leaks.

Another risk is that a rogue cloud employee, upon discovering that a popular company uses the provider's services to store sensitive information, could succumb to curiosity and snoop around the company's files. If the employee discovers sensitive or potentially valuable information, there is no telling whether the employee will exercise proper judgment and keep the information private or publicly disclose the information. Either way, the company's information is no longer within its sole control. While the risk of a rogue cloud employee stealing and disclosing trade secrets is admittedly low, it is a potential risk to consider.

If you decide to store trade secrets in the cloud, there are several steps you can take to limit potential risks associated with entrusting a third-party provider with your information:

- Do your homework before selecting a cloud provider. Research all of the providers you are considering to understand where and how your information will be stored, whether advanced security features are available (such as encryption, two-phase authentication, and cryptographic protocols), whether the provider has suffered security lapses and, if so, what measures were taken to address the lapses.

- Negotiate terms of service that maximize protection for your information. Boilerplate terms of service often fail to protect the owner's interests sufficiently. For example, cloud providers are often granted full access to any information stored on their servers. Consider negotiating terms that limit the provider's rights to access your files, and require the provider to delete all of your information at the end of contract.

- Require a confidentiality agreement. The provider and any of its employees who have access to your information should sign a confidentiality agreement prohibiting use and disclosure of that information.

- Purchase an insurance policy for your information. Because a provider's terms of service may limit the provider's liability for damages caused by the loss of information, consider purchasing an insurance policy to protect your company against potential losses in the event of an information leak.

Hackers and other outside threats

After information is uploaded to the cloud, it is a potential target for hackers and others with illicit motives. Security breaches and information thefts are becoming increasingly common. For example, one of the country's largest retail chains recently saw its customer information fall into the hands of a group of hackers. Information pertaining to 70 million customers was downloaded from the store's database, including names, addresses, phone numbers, and credit/debit card numbers. For a company that values the privacy of its customer information, this was a major loss of protected information.

To limit the potential risks of exposure from hackers and other outside threats, consider the following steps:

- Investigate and implement security measures offered by cloud providers. Do not be afraid to ask your cloud provider about past attacks and how the provider has responded to them.

- Encrypt trade-secret files stored on the cloud. Encryption provides an extra layer of protection in the event your information is hacked. In addition, encrypting files allows a company to further limit which employees have access to certain files.

- Use multiple-phase authentication before granting file access. This makes it more difficult for hackers to obtain your information by requiring them to get through multiple layers of security. For example, authentication measures may require both a username/password combination and an additional "token code" that constantly changes (usually every minute).

Company employees

Another concern raised by storing trade secrets in the cloud is the ease of employee access to confidential files. For example, with the best intentions, a telecommuting employee can access highly confidential trade-secret information in the cloud from her home computer. That employee has been loyal, trustworthy, and the company has no qualms about giving her access to highly confidential information in the cloud. Though the information is otherwise secure, once the employee accesses that information from her computer, a copy of that file resides on the employee's computer and is no longer controlled by the company.

Similarly, the same trustworthy employee could set up her own cloud storage site (e.g.,Dropbox or Google Docs) to easily access files from her various work locations. This setup could even be known to the company and accessed by a manager. But once information is stored in the cloud, there is an increased risk of unauthorized access to and use of that information.

In both examples, as long as the trustworthy employee maintains the confidentiality of the documents, even on her home computer, the trade secrets may be safe. But what happens if the company downsizes and the employee is let go? Typical security protocols may include confiscating the employee's company computer and ensuring that the employee does not leave the company with any disks, drives, or devices that contain company information. But where information already exists in the cloud, the employee can simply go home, access that information, and use it to her advantage. A sales person with a company's customer list could cause substantial harm. Alternatively, the former employee could start her own company to compete with the trade-secret information in hand. Simply put, even benign use of cloud solutions can compromise the secrecy of a company's trade-secret information.

To limit these potential risks, consider the following steps:

- Limit access to trade-secret files to employees on a need-to-know basis. The fewer people with access to trade secrets, the more likely the information will remain secret.

- Limit access to cloud-based solutions on company computers and prohibit any use of personal cloud solutions for company materials. Consider installing software to limit access to any cloud solutions that are not approved by the company.

- Implement policies and train employees about the use (or non-use) of cloud solutions and, more generally, about the protection of confidential information. Employee handbooks, new-employee orientations, posted company policies, and annual employee training sessions all provide opportunities to address these issues.

- Monitor when files are accessed or downloaded, and by whom. This will allow the company to take immediate action in the event it discovers suspicious activity.

- Require employees to sign NDAs. All employees should sign NDAs prohibiting them from taking or using company information for any purpose other than their work for the company. These obligations should extend beyond termination.

- Conduct exit interviews. This will allow the company to explore whether the employee retained any confidential information and to instruct him or her that any such information should be immediately returned or destroyed.

- Collect and secure computers used by terminated employees. By examining the computer of a former employee, a company can often determine if any information was taken before the employee's departure and what that information was.

- Label or name files containing trade secrets as "Confidential" or "Trade Secret." While this probably will not prevent unauthorized use or access, it may help a company to persuade a court that any misappropriated information still qualifies for trade-secret protection. This is because confidentiality labels help show that the company took reasonable steps to maintain secrecy by notifying the employee as to the sensitivity of the information.

Of course, many of these limitations are easier to implement for large corporations with significant IT staffs. Nevertheless, given the potential implications, all companies should consider taking at least some of these precautions, especially because courts often consider the size and resources of the information's owner in evaluating the reasonableness of steps taken to maintain secrecy.

Maintaining Trade-Secret Protection in the Face of Unauthorized Disclosure

Because even the best-laid plans sometimes go astray, it is important to be prepared in the event you discover unauthorized use or disclosure of your trade secrets. For example, if you learn that a former employee has used or disclosed your trade-secret information, it is important to act quickly in taking corrective action. Because reasonable steps to maintain secrecy do not require "perfection," Learning Curve Toys, 342 F.3d at 725, an owner can often preserve trade-secret status by acting quickly to halt any public or unauthorized use or disclosure, and limit further exposure. Though secrecy is the touchstone of trade-secret protection, "[a]bsolute secrecy is not required." Wyeth v. Natural Biologics, Inc., 395 F.3d 897, 900 (8th Cir. 2005).

To minimize the risk of losing trade-secret protection because of unauthorized use or disclosure, consider taking the following steps:

- Immediately remove any trade-secret information from the cloud and make efforts to investigate the source of the information leak.

- Send cease-and-desist letters or initiate litigation against the offending party.

- Enforce known violations of confidentiality agreements or NDAs.

In short, it is imperative that you act quickly in the event of unauthorized use or disclosure because courts often refuse to allow parties to claim trade-secret protection where they knew that their information's secrecy was at risk, but failed to take prompt remedial action.

Protecting Trade Secrets During Litigation

Litigation does not relieve a trade-secret owner of the obligation to take reasonable steps to protect its information. In fact, litigation presents its own set of risks because court filings and discovery disclosures may become public absent necessary precautions. Though the court system is in place to right legal wrongs, if a company does not take steps to make sure its confidential information remains secret during legal proceedings, it could lose trade-secret protection for that information. For example, if the trade secret is disclosed in a publicly filed complaint or in an interrogatory answer served before a protective order is in place, a company may inadvertently lose trade-secret protection for the very information it was seeking to protect.

To minimize these risks, an owner should consider taking the following precautions to maintain secrecy during litigation:

- File under seal any materials containing trade-secret information and avoid disclosing any trade-secret information in public filings.

- Enter into an appropriate protective order before producing any discovery containing trade secrets.

- Seek in-camera hearings for matters involving trade-secret information.

Conclusion

As cloud services continue to grow in popularity, companies must remain diligent in taking the necessary precautions to ensure that their confidential and trade-secret information stored in the cloud remains protected. By following the steps outlined above, companies can feel more confident that their information will never be seen raining from the cloud.

Benjamin J. Bradford is a partner and Justin A. Maleson and Michael T. Werner are associates at Jenner & Block's Chicago, Illinois, office.