COMPUTER AND TECHNOLOGY SECTION

Circuits

Newsletter of the Computer & Technology Section
of the State Bar of Texas

Volume 2: Fall 2014

TABLE OF CONTENTS

Trade Secrets in the Cloud

By Patrick Keating

With the growing use of cloud data storage services, it is a good time to consider how to maintain trade secret protection over confidential business information stored in the cloud. To qualify as a trade secret under the Texas Uniform Trade Secrets Act ("TUTSA"), the owner of the information must have undertaken "efforts that are reasonable under the circumstances to maintain its secrecy." TEX. CIV. PRAC. & REM. CODE §134A.002(6)(B). Although Texas appellate courts have not yet applied this aspect of TUTSA to information stored in cloud computer servers, the issue is sure to arise in the future.

This article discusses a defense that may arise in trade secrets cases related to the standard terms of service governing the most popular cloud services and suggests a practical solution. Specifically, a defendant may argue that the plaintiff failed to use reasonable efforts to maintain the secrecy of information stored in the cloud because the terms of service governing that storage permit the service provider to access or disclose the information to third parties. Businesses can address this risk by encrypting the data they store in the cloud. Encryption is relatively inexpensive and will prevent the cloud service provider or other third parties from accessing the data. This will strengthen a claim that the business took reasonable steps to maintain the secrecy of proprietary information.

Terms of Service Examples

Some of the largest customers of cloud services have the clout to negotiate confidentiality restrictions into their contracts. Other customers use cloud services under the service provider's standard terms of services ("TOS"). The TOS do not always place confidentiality obligations on the service provider. Additionally, the most commonly used cloud service providers offer multiple categories of service (for example, "business" and "non-business" accounts) and the protection promised to the customer differs by category. Employees of a business may use free cloud storage services offered on non-business accounts, so all of the categories of cloud services are relevant to this issue.

i. Dropbox

Dropbox is a popular service used for storing data in the cloud. Dropbox's TOS for "Non-Business" accounts does not obligate Dropbox to protect the confidentiality of customer's data. The TOS includes a broad disclaimer stating that the customer takes Dropbox's services on an "as is" basis. Dropbox Non-Business TOS, https://www.dropbox.com/terms. Moreover,

Dropbox's general privacy policy authorizes Dropbox to share customer information with third parties working with Dropbox "to help [Dropbox] provide, improve, protect and promote [its] Services." Dropbox Privacy Policy, https://www.dropbox.com/terms#privacy. Read literally, this grants Dropbox authority to allow a third party to access customer data even if the access is not necessary for Dropbox to provide its services to the customer who owns the data.

The TOS governing Dropbox's "for Business" service provides more assurance to the customer that Dropbox will protect the confidentiality of customer information. That TOS includes a warranty that Dropbox will use industry standard measures to protect against unauthorized access to customer data. Dropbox for Business Agreement, §2(b) (https://www.dropbox.com/terms#business_agreement). As noted above, however, Dropbox's privacy policy permits Dropbox to grant some third parties access to the Customer's Data.

ii. Amazon Cloud Drive and Amazon Web Services

Amazon's Cloud Drive is another data storage service. Amazon's Cloud Drive TOS states that Amazon's use of customer data is subject to Amazon's general privacy policy, which permits Amazon to use any information it "stores" for customers to improve Amazon's "stores." Amazon Cloud Drive TOS, http://www.amazon.com/gp/help/customer/display.html?nodeId=201376540; Amazon Privacy Policy, http://www.amazon.com/gp/help/customer/display.html?nodeId=468496.

Amazon Web Services ("AWS") is Amazon's combined data storage and cloud-based computing service. The default AWS customer agreement contains two provisions that could be cited in a trade secret lawsuit. Section 3.1 states that, "without limiting Section 10," Amazon will "implement reasonable and appropriate measures designed to help you secure Your Content against accidental or unlawful loss, access or disclosure." AWS Customer Agreement, §3.1 (http://aws.amazon.com/agreement/). However, Section 10 states that Amazon offers its services "as is" and makes no warranty that "your content ... will be secure or not otherwise lost or damaged." AWS Customer Agreement, §10.

iii. Google Drive and Google Cloud Platform

Google Drive is Google's cloud storage service. Google expressly states on the frequently asked questions section of it website that (i) the user controls who can access the user's files stored in Google Drive and (ii) Google only shares files and data with others to the extent described in Google's privacy policy. Nevertheless, a defendant facing trade secret litigation might point to text in Google's TOS providing that the user grants "Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works ...

communicate, publish, publicly perform, publicly display and distribute [the user's] content ... for the limited purpose of operating, promoting, and improving our Services, and to develop new ones." Google TOS, http://www.google.com/policies/terms/.

Google provides cloud-based computing services through its Cloud Platform. Google's Cloud Platform TOS address more directly the issue of preventing third parties from accessing customer information. The terms of service state that (i) Google "will adhere to reasonable security standards no less protective" than the security standards Google applies to its own data and (ii) warrant that Google has implemented at least industry standard systems and procedures to ensure the confidentiality of customer data. Google Cloud Platform TOS, §1.3 (https://cloud.google.com/terms/).

This tells the customer that Google is working to prevent unauthorized disclosure of customer data to third parties. However, a defendant in trade secret litigation might argue that another portion of the TOS authorizes Google to use customer data. In this respect, Google's TOS state, "Google may use Customer Data and Applications ... to help secure and improve [Google's] Services." Google Cloud Platform TOS, §5.2.

Encryption

Because Texas appellate courts have not yet addressed what steps, if any, must be undertaken to protect the secrecy of information stored in the cloud, businesses may choose to use encryption as a proactive measure. This may also just be good business practice when dealing with proprietary information.

Encryption is a method of encoding data. Once the data is encoded with a strong encryption algorithm, a reader can only understand the data by possessing the key necessary to decrypt the data. In this sense, the data is locked. "Decryption" unlocks the data and turns the data back into its original, accessible format.

There are multiple companies that market encryption services. Those wishing to learn more about encrypting data stored in the cloud can try the services of several vendors at no charge.

Boxcryptor and Sookasa are separate companies that encrypt their customer's data before the data is transmitted to a cloud service provider. Sookasa currently only works with Dropbox, but Boxcryptor works with many cloud storage services.

Spider Oak provides another option for encrypting data. Spider Oak is a cloud storage provider who encrypts its customers' data before the data is uploaded to Spider Oak's servers. Thus,

Spider Oak offers a "one stop shop" for cloud storage and encryption services. Spider Oak does not, however, enable customers to encrypt data stored on another cloud service provider's servers.

Conclusion

The terms of service governing cloud services do not always expressly obligate the service provider to protect the confidentiality of customer data or prohibit use of customer data. Users of cloud services who are concerned about maintaining the secrecy of their information in the cloud can look to encryption as one tool to further that goal.

About the Author

Patrick Keating has represented clients in business litigation for nineteen years. He focuses his practice on (1) commercial litigation between businesses (for example, theft of trade secrets, other business tort disputes and breach of contract claims) and (2) lawsuits between co-owners of businesses and against officers, directors or managers of businesses (for example, breach of fiduciary duty cases). He is a partner in the Dallas office of Haynes and Boone, LLP. Patrick also is the author of a blog focusing on issues related to trade secrets in Texas at: http://www.pkeating.com.