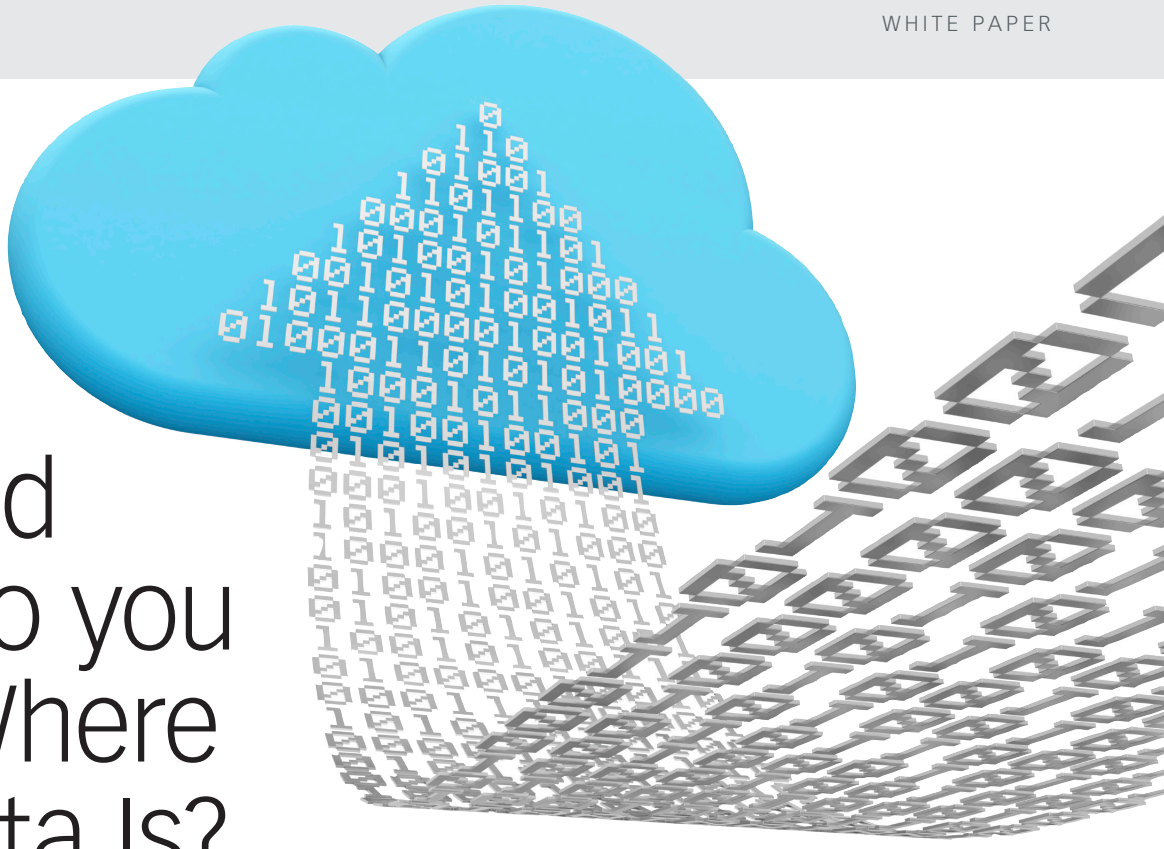
InfoWorld
Strategic Marketing Services

WHITE PAPER



It's Cloud Time, Do you Know Where Your Data Is?

Ensure secure cloud sharing benefits without exposing data to intrusive snooping

Executive Summary

Disclosures that spy agencies were able to tap into data transmitted by Internet service companies and telecom providers undermined confidence in the security of data housed by public cloud services. Even as enterprises are struggling to keep pace with technology and drive business forward, the disclosures call into question the sanctity of their intellectual property, confidential information and privacy guarantees—and they are wondering how to protect their information assets in the cloud environment.

SPONSORED BY ownCloud

The Snowden Effect

Big data has had a widespread impact on business in recent years. The act of collecting and analyzing data has resulted in game-changing insight, enabling entities of every size and shape to study trends, predict outcomes and even mitigate risk. Big data is literally changing the way companies—and countries—operate.

In the wake of the devastating "9/11" attack on Sept. 11, 2001, the passage 45 days later of the USA PATRIOT Act heralded a new era in government use of technology to intercept and analyze communications. The culling of big data in the name of national security was conceived as a vital intelligence tool to help thwart terrorist activities. Few at the time, though, recognized the global ramifications beyond the war on terrorism and into the realms of personal privacy and corporate security.

When news organizations in 2013 began publicizing secret documents[1] provided by Edward Snowden, a contract employee working with the U.S. National Security Agency (NSA), it quickly became apparent that the intelligence agency was intercepting huge amounts of data from online service providers.[2] At the heart of the NSA disclosures is a program code-named PRISM that collects "the contents of emails, chats, VoIP calls, cloud-stored files, and more."[3]

The NSA, according to many published reports, collected massive amounts of data from service providers, based on the premise that much of the world's Internet traffic passes through servers housed in the U.S. And the U.S. isn't the only country to do so. According to *The Guardian*, the Snowden disclosures reveal that "The German, French, Spanish and Swedish intelligence services have all developed methods of mass surveillance of internet and phone traffic over the past five years in close partnership with Britain's GCHQ eavesdropping agency."[4]

The prospect of intelligence agencies being able to see data on public hosted cloud services calls into question the presumed security of public cloud infrastructure. It raises the issue of how to deal with policies and governance over employees who may leverage such services on an ad hoc basis. Further, many data owners are unaware of the pertinent guiding legislation when they first store their files in the cloud.

With executives and users demanding more and quicker access to cloud services, it is difficult for IT to enforce policies that restrict the use of public cloud services, including consumer-grade services for syncing and sharing files. Many cite the need for control, because when accessing off-premise data through CDN, WebDAV or other Web protocols, data is not encrypted and may be co-mingled with the data of other companies. This may expose data to unwanted snoopers—from hackers to government investigators, lawyers or even file-sharing vendors. Additionally, once data is on those third-party servers, it often stays there even after it's deleted. In short, IT organizations are no longer in control of their data.

Global Implications

Reaction to the disclosure of PRISM and other data interception efforts varies greatly, depending on factors such as country, cultural sensitivity to privacy and confidentiality issues, and relative fears of terrorism threats.

"In the U.S., the reaction to PRISM was more subdued than it was in Europe," says Markus Rex, CEO and co-founder of ownCloud Inc., the provider of enterprise file sync and share software that offers the benefits of cloud services while ensuring proper management and control of sensitive data stored on-premise. "Because U.S.-based providers dominate so much of the cloud services industry, their U.S.-based customers may be somewhat complacent about data 'staying' in the U.S."

That segmentation of data within definable borders isn't always the case. According to *Computerworld*, in a routine audit, one large Fortune 500 company discovered that its cloud provider "had become merely a shell" and had actually outsourced the provision of the service to an offshore company.[5] Similarly, *Network World* reported that service providers may operate "a network of data centers that work in tandem to provide high availability and security of customer data. Sometimes that means data will be moved around the country based on disasters, service levels, demand of resources and cost, among other factors."[6]

"Because U.S.-based providers dominate so much of the cloud services industry, their U.S.-based customers may be somewhat complacent about data 'staying' in the U.S."

—Markus Rex, CEO and co-founder of ownCloud Inc.

Consumer-grade services from Dropbox and Google remain the most popular cloud storage services used in businesses, despite the availability of more secure enterprise-level alternatives.

SOURCE: "Enterprise cloud storage still losing out to Dropbox in the workplace," April 10, 2014. TechRepublic. www.techrepublic.com/blog/european-technology/enterprise-cloud-storage-still-losing-out-to-dropbox-in-the-workplace/#

For companies dealing with compliance or legal issues that require data be kept within domestic borders, such ambiguity can be troubling. Cloud service providers, whether U.S.-based or elsewhere, may or not may not provide specific information about where a customer's data is stored. Metadata, encryption keys and access trails all may follow the data. And service providers doing business in another country may still be subject to, or susceptible to, the surveillance laws and/or practices of their home country.

While European enterprises have been more guarded about their proprietary information residing on U.S.-hosted systems, their efforts may not be enough. As *The Washington Post* reported, intelligence agencies were also able to collect data from transmission links connecting data centers around the world, including those that Google and Yahoo each maintain to serve their customers.[7]

Irresistibility of the Public Cloud

With more than 1 billion files saved every day to Dropbox alone,[8] consumers have latched onto public cloud services eagerly, "owing to the improved simplicity associated with being able to connect multiple devices through the cloud, making file-sharing and synchronization less of a hassle."[9]

"File sync and share has taken the consumer world by storm because it is an easy way to share photos, documents and more using any device, any time," says Terri McClure, senior analyst with Enterprise Strategy Group (ESG), a leading IT research, analysis and strategy firm. "Unfortunately, many employees have brought these consumer apps into the workplace and are using them to store and share business data, giving corporate IT huge headaches as sensitive—and sometimes even regulated—corporate data is being stored in consumer cloud services."

Enterprise use of public cloud is being promoted as inevitable, relying on the concept of "hybrid cloud" to tie together private and public cloud resources, which Gartner forecasts will be deployed by almost half of large enterprises by 2018.[10]

Bring Cloud Services Out from the Shadows

Many providers that started with consumer service offerings now claim "enterprise-grade" business versions of their services, but in general that extra level of enterprise-readiness primarily relies on encryption of data; service providers still utilize common storage resources to store data from multiple customers. Others may require data be moved or duplicated rather than left as is under the governance of the security policies implemented by IT. And there is no way to ensure that enterprise data can be deleted once users upload it to a public cloud-based service. What's more, workers can inadvertently violate nondisclosure agreements, and cloud vendors may be subject to subpoenas that require them to surrender the enterprise's data.

Another complication for enterprises is that the cloud industry is still relatively new and evolving rapidly, making it difficult to anticipate changes that may impact security and privacy. "What enterprises need is flexibility, and certainty that the technology they acquire today [works] for future use cases for which they are not yet even aware," says Rex. "This is a challenge if you totally depend on some external cloud systems. Technology is fast-moving and it is hard to say what service providers will look like in two years, let alone 10 years."

Many emerging service providers face the ongoing challenge of maximizing market opportunity as well as optimizing and changing their business models to find their optimal role.

What are the Options?

"Recent NSA disclosures have added significantly to a sense of urgency to get control over corporate data," says ESG's McClure. "Many companies are concerned about putting their corporate file data in the cloud, seeking instead a hybrid solution that gives employees the tools they need to be productive and IT the ability to secure and control sensitive and regulated corporate file data behind their own firewall."

Flexibility Meets File Share

The task force on data storage solutions for TERENA—the Trans-European Research and Education Networking Association—looked at many file sync and share alternatives and determined that its community is best served by solutions that are open source, integrated software that can be operated on-premise and are agnostic to storage solutions.

"Research and educational institutions have unique privacy and regulatory concerns, and only by having an open and flexible solution can they best take advantage of file sync and share," says Péter Szegedi, project development officer at TERENA.

"The approach behind ownCloud's enterprise server architecture, which is based on the popular ownCloud open source file sync and share community project, is to enable enterprises to examine, audit and modify ownCloud to meet their requirements," says ownCloud CEO Markus Rex.

The organization developed a solution that returns control of sensitive data to IT—combining greater flexibility, openness and extensibility with on-premise servers and storage. The server can utilize storage physically located in an enterprise data center or "mounted" to third-party storage providers. Either way, IT can manage and protect enterprise files as with any other element of the infrastructure.

From the user perspective, ownCloud provides access to share, roll back and manage files through a standard browser as well as the desktop client. This ensures the user is always working with the latest file. Further, users can optimize their productivity with the ability to browse, download, edit and upload files while on a mobile device or tablet.

Enterprises should not be forced to choose between on-premise and cloud-based solutions, says Rex. The key is making sure that IT can secure the use of sensitive data, provide secure file sync and share services, and even enable user access to services like Dropbox for nonsensitive information. ownCloud allows businesses to leave data where it is. IT remains in full control with auditing and logging features while data lives within the security and governance policies determined by the enterprise.

There's more to security issues than the lack of encryption and co-mingling of data. IT needs to be able to track, protect and manage files from software running on servers it can control safely, and to establish policies—using physical, virtual or private cloud servers, with on-premise or third-party storage.

To start, an enterprise must identify its risk tolerance in determining how it will let users sync and share files. That means striking a balance between convenience and the issues of privacy and security, says Rex. "There are tools like encryption algorithms that make it literally impossible to get to data, but they are too cumbersome for most users."

At its core, secure enterprise file sync and share must integrate with existing IT systems and policies such as authentication systems, user directories, governance workflows, intrusion detection, monitoring, logging and storage management. It should preserve existing business processes and provide a choice to the administrators about where and how they store data. And to avoid user defections, IT needs to be able to extend functionality of the enterprise file sync and share solution, utilizing APIs and mobile libraries to customize system capabilities, meet unique service requirements, and accommodate changing user needs.

This leaves many enterprises favoring private cloud options over public cloud or even hybrid cloud implementations in which administrators retain control over enterprise data where it currently resides, while end users are able to access files through secure cloud portals from the devices they use daily.

Karl-Eugen Binder, retired CIO of Stuttgart Insurance Group in Germany, realized the company needed its own cloud solution after marketing and sales employees began using Dropbox on their own. The potential exposure of confidential files was not an acceptable risk. Instead, the company developed its own private cloud, using software from ownCloud. Now it operates a fully private cloud for sharing documents internally, a second for selectively sharing information on intellectual property laws, and a third for externally focused marketing information.

"We had to find a solution better than Dropbox," he says. "We dropped Dropbox from internal networks and were able to offer users good services and the opportunity to support their other devices; they accepted it readily."

Bottom Line: Some Data Needs to Stay Private

Storing data off-premise may strip an organization's ability to manage and control its data, or to ensure that data can be deleted. Few enterprises, however, are willing to forgo the benefits that cloud services provide in the advancement of agility and improved business processes. That leaves them struggling with how to leverage these technologies without importing security risks. They also recognize that end users are increasingly able to migrate to external services that provide them greater flexibility and mobility than that offered by the enterprise.

By retaining on-premise manageability of file sync and share services, though, IT can utilize a private cloud solution to reconcile the need for cloud technology with the requirements for security and privacy, and regain control of sensitive data without unwanted exposure. With the ability to enhance control and govern access to files, IT administrators can set sophisticated rules for user and device connections and prevent access based upon those rules. Further, the capabilities and extensibility of on-premise file sync and share match the ease of use and complete access that first drove consumption of cloud services, yet IT controls sensitive assets in its own cloud environment.

Please visit www.owncloud.com for information about ownCloud, links to download the software, and detailed product documentation.

InfoWorld
Strategic Marketing Services

ownCloud

[1] Mirrien Gidda, "Edward Snowden and the NSA files – timeline," July 25, 2013, The Guardian. www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline

[2] Eric Schmitt, David E. Sanger and Charlie Savage, "Administration Says Mining of Data Is Crucial to Fight Terror," June 7, 2013, The New York Times. www.nytimes.com/2013/06/08/us/mining-of-data-is-called-crucial-to-fight-terror.html?pagewanted=all

[3] Verge Staff, "Everything you need to know about PRISM," July 17, 2013. The Verge. www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet

[4] Julian Borger, "GCHQ and European spy agencies worked together on mass surveillance," November 1, 2013. The Guardian. http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden

[5] Stacy Colett, "Do you know where your cloud data is?", December 16, 2011. Computerworld. www.computerworld.com/s/article/357979/Securing_the_daisy_chain

[6] Brandon Butler, "Do you know where your cloud data is?," April 25, 2012. Network World. www.networkworld.com/article/2188011/cloud-computing/do-you-know-where-your-cloud-data-is-.html

[7] Barton Gellman and Ashkan Soltani, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say," October 30, 2013. The Washington Post. www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

[8] Stephen Shankland, "Dropbox clears 1 billion file uploads per day," February 27, 2013. CNET.

[9] Charlie Osborne, "Report tags top consumer trends for 2013," Dec. 13, 2012. CNET. www.cnet.com/news/dropbox-clears-1-billion-file-uploads-per-day/

[10] "Gartner Says Nearly Half of Large Enterprises Will Have Hybrid Cloud Deployments by the End of 2017," Oct. 1, 2013. Gartner, Inc. www.gartner.com/newsroom/id/2599315