February 2013

Privacy in the Cloud: Office 365

Key Points

- The advances and increased adoption of cloud computing raise important policy considerations, including shared data storage, geographic location, transparency, access, and security.
- Microsoft understands that strong privacy protections are essential for building trust in the cloud and helping cloud computing reach its full potential. So Microsoft built its Office 365 online collaboration service from the beginning with strong data protection in mind, including the dedication of a team of privacy professionals.
- Conflicting legal obligations and competing claims of governmental jurisdiction over data usage continue to limit cloud computing services and their adoption. Divergent rules on privacy, data retention, and other issues cause ambiguity and create significant legal challenges.

BACKGROUND

Cloud computing—Internet-based data storage, processing, and services—is now both a viable alternative and a complement to the traditional model of running software and storing data on premises or on personal devices. Although cloud computing provides convenient, shared access to apps and online services, servers, networks, and storage, this data model raises important privacy and security policy considerations:

- **Shared data storage.** When the data from many customers is stored at a shared physical location, cloud providers must take appropriate steps to segregate that data to protect it from inappropriate use or loss. Additional safeguards include providing strong levels of encryption and proper controls for administrative access.
- **Transparency and access.** Customers want to know where their data is stored, who has access to it, how it is used and shared, and what safeguards are protecting it. Cloud providers can address these concerns—and build trust, too—by implementing transparent policies and communicating them clearly to customers and regulators.
- **Geographic location of data.** As cloud computing evolves, traditional geographical limits on data storage and movement also shift. For instance, data created in France using software hosted in Ireland could be stored in the Netherlands and accessed from the United States. Consequently, regulators and cloud computing customers want clearly defined policies and disclosures regarding the physical location of their data.
- **Security.** Customers rely upon their cloud service providers not only to store their data securely but also to keep it safe from loss, theft, or misuse.

MICROSOFT APPROACH

Microsoft offers a number of cloud-based products, including Microsoft Office 365, a service that provides access to cloud-based email, web conferencing, file sharing, and Office Web Apps.

Microsoft understands that strong privacy protections are essential for building trust in cloud computing, and implements them in Office 365 as follows:

Data use. Microsoft explains clearly how it manages and uses customer data, including explicit statements that Microsoft uses it only for maintaining and securing Office 365 services. Office 365 does not use customer data—for example, by scanning email or documents stored in the cloud—to create advertisements.

Shared data storage. To enable cost savings and efficiencies for data storage, Microsoft stores customer data from multiple customers on the same equipment (known as a *multi-tenant format*). However, the company goes to great lengths to help ensure that multi-tenant deployments of Office 365 logically separate the data (and processing) of different accounts and support the privacy and security of the data stored.

Data portability. Microsoft enables Office 365 customers to export any or all of their data at any time and for any reason, without any assistance from Microsoft. Even after an Office 365 account expires or is closed, customers by default have limited access for an additional 90 days to export data.

Transparency. The Office 365 Trust Center details the policies and practices that the Office 365 service uses to protect customer data.

Security. Microsoft helps protect Office 365 with a security regimen that includes daily monitoring.

Access. Microsoft identifies any of its subcontractors who can access customer data and the circumstances under which they can access it. The company also logs and reports any access to critical data. Additionally, Microsoft and its third-party auditors conduct sample audits to help ensure that the customer's data is accessed only for appropriate business purposes.

Geographic location of data. For customers interested in knowing where their data is stored, including the assignment of private storage locations, Microsoft tells customers where the major data centers are located, and how it determines where data is stored. Office 365 administrators can also choose to receive updates to changes in data center locations.

POLICY CONSIDERATIONS

- Conflicting legal obligations and competing claims of governmental jurisdiction over the use of data continue to limit cloud computing services and their adoption. Divergent rules on privacy, data retention, and other issues cause ambiguity and create significant legal challenges.
- Microsoft supports privacy legislation that facilitates the free flow of information, builds trust, and encourages innovation. Because data flows are global, the company strives to harmonize privacy regulations, policies, and standards worldwide.
- As governments develop policies that address the privacy and security concerns associated with such emerging technologies as cloud computing, they should continue to support technological innovation and its adoption. Working together, government and industry can establish appropriate privacy principles that protect data in the cloud.

Helpful Resources

An overview of Microsoft privacy policies and initiatives
www.microsoft.com/privacy

Microsoft Office 365
office365.microsoft.com

Privacy and cloud computing at Microsoft
www.microsoft.com/privacy/cloudcomputing.aspx

The Office 365 Trust Center
www.trust.office365.com