Microsoft

Trustworthy Computing

Privacy in the Cloud Computing Era

A Microsoft Perspective

November 2009

Microsoft Corp. • One Microsoft Way • Redmond, WA 98052-6399 • USA

Contents

Cloud Computing and Privacy

A new generation of technology is transforming the world of computing. Internet-based data storage and services—also known as "cloud computing"—are rapidly emerging to complement the traditional model of software running and data being stored on desktop PCs and servers. In simple terms, cloud computing is a way to enhance computing experiences by enabling users to access software applications and data that are stored at off-site datacenters rather than on the user's own device or PC or at an organization's on-site datacenter.

E-mail, instant messaging, business software, and Web content management are among the many applications that may be offered via a cloud environment. Many of these applications have been offered remotely over the Internet for a number of years, which means that cloud computing might not feel markedly different from the current Web for most users. (Technical readers will rightly cite a number of distinct attributes—including scalability, flexibility, and resource pooling—as key differentiators of the cloud. These types of technical attributes will not be addressed here because they are outside the scope of this document.)

Cloud computing does raise a number of important policy questions concerning how people, organizations, and governments handle information and interactions in this environment. However, with regard to most data privacy questions as well as the perspective of typical users, cloud computing reflects the evolution of the Internet computing experiences we have long enjoyed, rather than a revolution.

Microsoft recognizes that privacy protections are essential to building the customer trust needed for cloud computing and the Internet to reach their full potential. Customers also expect their data and applications stored in the cloud to remain private and secure. While the challenges of providing security and privacy are evolving along with the cloud, the underlying principles haven't changed—and Microsoft remains committed to those principles. We work to build secure systems and datacenters that help us protect individuals' privacy, and we adhere to clear, responsible privacy policies in our business practices—from software development through service delivery, operation, and support.

Enterprise customers typically approach cloud computing with a predefined data management strategy, and they use that strategy as a foundation to assess whether a given service offering meets their specific needs. As a result, privacy protections might vary in different business contexts. This is not new or unique to the cloud environment. Ultimately, we expect the technology industry, consumers, and governments to agree on baseline privacy practices that span industries and countries. As that consensus view evolves, Microsoft will remain an active voice in the discussion—drawing on our extensive experience and our commitment to helping create a safer, more secure Internet that enables free expression and commerce.

The Evolution of Cloud Computing

Services that operate in the cloud often work in tandem with a client application operating on the desktop computer. For example, instant messaging and e-mail applications running on a computer rely on the cloud infrastructure for their connected features and also require a client download. The combination of "client

plus cloud" offers consumers, governments, and businesses greater choice, agility and flexibility while also greatly increasing efficiency and lowering information technology (IT) costs. It gives customers access to information, software, and services on a range of intelligent devices, at a lower cost. As a result, this next generation of computing has enormous potential to create new business opportunities and economic growth.

As with other major technological transitions, the evolution of cloud computing has drawn widespread attention and scrutiny in the news media. It has also raised policy questions concerning how people, organizations, and governments handle information and interactions in this environment. These questions are not unlike those raised during other technology-driven transitions, such as the shift from records, cassettes, and compact discs to MP3 files and from printed newspapers to online news. In these examples, the unique properties of a new medium triggered a period of adjustment that involved realigning usage practices, policies, and even regulatory approaches.

In the case of the cloud, this shift has been under way for a number of years as part of an ongoing evolution from processing information on paper and storing it in filing cabinets to storing it on computer servers outside of the user's immediate physical control. A key distinction of cloud computing is that information storage and usage need not be limited by space or geography. Indeed, cloud computing users typically don't even need to know how many "virtual filing boxes" they will need because the available space scales to meet their needs. Further, the cloud does far more than just store data. It also hosts applications and enables cheaper, more flexible uses of the cloud's contents.

Privacy Questions in Cloud Computing

These properties of client-plus-cloud computing raise valid questions about security and privacy, such as:

- Are hosted data and applications within the cloud protected by suitably robust privacy policies?
- Are the cloud computing provider's technical infrastructure, applications, and processes secure?
- Are processes in place to support appropriate action in the event of an incident that affects privacy or security?

Security is an essential component of strong privacy safeguards in all online computing environments, but security alone is not sufficient. Consumers and businesses are willing to use online computing only if they trust that their data will remain private and secure. (See the related paper titled "Securing Microsoft's Cloud Infrastructure."[1]) The ability of cloud computing providers to live up to these expectations is critical not only for the future of cloud computing but also for protecting fundamental rights of privacy and freedom of expression.

Microsoft has been examining and addressing privacy challenges in the evolving cloud computing realm for well over a decade. Our extensive experience has helped us develop well-defined business practices, privacy policies, and security measures that govern our cloud computing ecosystem. Recognizing that the cloud poses some new security and privacy challenges, we believe that our current policies and practices provide a solid foundation for addressing privacy issues and enabling greater trust in the Internet going forward.

---

[1] www.globalfoundationservices.com/security/documents/SecuringtheMSCloudMay09.pdf

Consumer-Oriented Cloud Computing Today

Over the past decade, rapidly growing Internet-based services such as e-mail, blogging, social networking, search, and e-commerce have substantially redefined the way consumers communicate, access content, share information, and purchase products. Since the launch of the MSN® network in 1994, Microsoft has actively addressed privacy and security considerations in its online services. Today, we manage a cloud-based infrastructure and platform for more than 200 online services and Web portals for consumers, including Windows Live™ Hotmail®, Windows Live Messenger, and Bing™ search. Because Microsoft has a direct relationship with consumers for these services, we establish and directly manage the privacy policies that govern data associated with these services.

Microsoft Privacy Principles

- **Accountability** in handling personal information within Microsoft and with vendors and partners
- **Notice** to individuals about how we collect, use, retain, and disclose their personal information
- **Collection** of personal information from individuals only for the purposes identified in the privacy notice we provided
- **Choice and consent** for individuals regarding how we collect, use, and disclose their personal information
- **Use and retention** of personal information in accordance with the privacy notice and consent that individuals have provided
- **Disclosure or onward** transfer of personal information to vendors and partners only for purposes that are identified in the privacy notice, and in a security-enhanced manner
- **Quality assurance** steps to ensure that personal information in our records is accurate and relevant to the purposes for which it was collected
- **Access** for individuals who want to inquire about and, when appropriate, review and update their personal information in our possession
- **Enhanced security** of personal information to help protect against unauthorized access and use
- **Monitoring and enforcement** of compliance with our privacy policies, both internally and with our vendors and partners, along with established processes to address inquiries, complaints, and disputes

Microsoft has long maintained that in order for individuals and organizations to fully utilize the power of computers and the Internet, the overall ecosystem must be more secure and reliable. We also believe that individuals and organizations must have greater control over their information and be able to trust that this information is being used and managed appropriately.

The foundation of Microsoft's approach to privacy and improved data protection is a commitment to empowering people to help control the collection, use, and distribution of their personal information. Microsoft was one of the first organizations to embrace the Safe Harbor privacy principles developed by the U.S. Department of Commerce and the European Commission. These tenets provided a framework for the development of Microsoft's own privacy principles, which guide our use and management of customer and partner information. (See sidebar at left.)

Together, our privacy principles and corporate privacy policy govern the collection and use of all customer and partner information and provide Microsoft employees with a clear and simple framework to help ensure privacy compliance companywide.

As a part of our Trustworthy Computing initiative, Microsoft employs more than 40 full-time privacy professionals across the company, with several hundred

more employees responsible for helping to ensure that privacy policies, procedures, and technologies are applied within the company's products, services, processes, and systems.

Further, the Microsoft Privacy Standard for Development (MPSD) framework helps ensure that customer privacy and data protections are systematically incorporated into the development and deployment of Microsoft products and services. The MPSD includes detailed guidance on creating customer notification and consent procedures, providing sufficient data security features, maintaining data integrity, offering user access, and supplying controls when developing software products and Web sites. In an effort to share best practices with the broader technology industry and privacy community, Microsoft has publicly released a version of its Privacy Guidelines for Developing Software Products and Services.[2]

We continually review and refine the privacy policies and codes of conduct that govern our online applications in order to address consumers' evolving needs and expectations.

Cloud Computing for Governments and Businesses

Many of the same privacy policies, principles, and technologies that govern our delivery of consumer-oriented cloud computing services also apply to cloud computing for governments and businesses. Adoption of cloud computing in these sectors has accelerated as organizations have recognized its compelling potential to reduce capital and staffing costs by moving e-mail and other services into a cloud environment. Cloud-based services can also be quickly implemented and modified to meet customer demand anytime and anywhere. This allows governments and businesses to add or reduce computing capacity nearly instantaneously and pay only for the services they need. These advantages are leading organizations to put mission-critical services such as customer relationship management, enterprise resource planning, financial data management, e-mail, and document management into the cloud.

Unlike our consumer business, in which Microsoft has a direct relationship with consumers and directly controls the policies that govern their data, our cloud services for business customers defer to the policies of those customers. In this case, Microsoft has no direct relationship with the business's employees or the customers to whom the hosted data may pertain. Policies relating to the business's handling of this data in the cloud environment are controlled and set by that business rather than by Microsoft. Our role is to handle and process the data on behalf of the business, much like third-party telephone call centers process customer inquiries, orders, and data for their business customers.

The division of responsibility between an enterprise or government and its cloud services provider is similar to that of a company that rents physical warehouse space from a landlord for storing boxes of customer or company files. Even though someone else might own the building, access to those files and the use of information within them is still governed by the policies of the company that rents the space. These same principles should apply in the cloud environment.

---

[2] http://www.microsoft.com/downloads/details.aspx?FamilyId=C48CF80F-6E87-48F5-83EC-A18D1AD2FC1F&displaylang=en

Documents stored on an organization's own internal servers have a measure of built-in security and privacy based on the physical boundaries and access controls that the company can impose directly. As data moves into the cloud, these natural protections no longer apply in the same way. Assurance of privacy and security will require firm policies on data access, usage, and transfer that will remain in force no matter where the data travels or how it is used. Some companies will prefer to store and manage their documents and data on their own servers, while others will prefer a cloud environment or some combination of the two approaches. Microsoft offers customers all three options, which are backed by a range of security tools to help customers protect documents and data against theft, security breaches, and other types of compromise.

To prepare for the growth of cloud computing, Microsoft has developed clear and transparent data handling processes in its hosted-services agreements with enterprise customers for Microsoft Dynamics® CRM Online, Microsoft® Business Productivity Online Standard Suite, and many other services. Microsoft also provides enterprise customers with a set of flexible management tools in its enterprise platform offerings that help to protect sensitive and confidential data and support compliance with related government guidelines.

These types of transparent policies and strong protective tools are essential for enterprises as they deal with the additional privacy and security questions that arise from their use of the cloud environment to store, organize, and share data—questions that go beyond those associated with consumer-oriented cloud computing services.

Microsoft is working closely with its enterprise customers to help address these considerations through well-defined policies governing cloud-based management, use, and protection of data. This includes making sure that as enterprises increasingly move from storing data in-house to contracting with cloud-services providers for hosted management, clear privacy guidelines define what the provider can and cannot do with data it is safeguarding.

Legal and Regulatory Challenges

Cloud services can thrive when companies are able to provide these services in an efficient way and assure customers that their data will remain private and secure. But as more and more consumer and enterprise data moves into the cloud, increasing uncertainty about the legal and regulatory obligations related to that data could jeopardize the benefits of cloud computing.

To offer the full benefits of cloud computing, online computing providers must be able to operate datacenters in multiple locations and transfer data freely between them. This allows a provider to optimize efficiency and deliver the performance and reliability that customers expect. Regulations that restrict cross-border data transfers, or create uncertainty or disharmony with respect to such transfers, can hamper these benefits.

Similarly, providers can be caught in an impossible position when governments impose conflicting legal obligations and assert competing claims of jurisdiction over user data held by these providers. Divergent rules on data privacy, data retention, law enforcement access to user data, and other issues can lead to ambiguity and significant legal challenges. For instance, one country might insist that its rules regarding mandatory data retention or law enforcement access to data apply in a given context. However, this could result in a situation

where there is a direct conflict with the privacy laws of another country that also has a strong claim of jurisdiction over that same data.

While IT companies will face the brunt of these problems first, their effects will increasingly be felt across the economy. If businesses are forced to store data locally in order to mitigate these jurisdictional conflicts, the costs of investment and innovation in cloud computing will increase. As a result, many of the efficiency and performance benefits of cloud computing may be lost and the benefits to business and consumers will be reduced.

The IT industry has been working hard to address these challenges, but it cannot solve them alone. Microsoft supports efforts to develop globally consistent privacy frameworks that recognize the worldwide nature of data flows while at the same time providing strong privacy protections for the people to whom the data pertains. More generally, governments must help craft clear rules and processes to resolve these conflicting obligations in a way that protects privacy and security.

Conclusion

Client-plus-cloud computing offers enhanced choice, flexibility, operational efficiency and cost savings for businesses and consumers. To take full advantage of these benefits, users must be given reliable assurances regarding the privacy and security of their online data. In addition, a number of regulatory, jurisdictional, and public policy issues remain to be solved in order for online computing to thrive.

Microsoft has been addressing many of these issues since 1994, when we delivered our first online services for consumers and enterprises. Our breadth of experience has shaped our company's privacy principles, corporate privacy policy, product and service development, and overall business practices. These components anchor our commitment to maintaining the highest standards of privacy and security in our online services and to partnering with other industry leaders, governments, and consumer organizations to develop globally consistent privacy frameworks that enable the expansion of the economic and social value of cloud-based computing.