

Trustworthy Computing



Privacy in the Cloud

A Microsoft Perspective

November 2010

The information contained in this document represents the current view of Microsoft Corp. on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This whitepaper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2010 Microsoft Corp. All rights reserved.

Microsoft, Hotmail, Microsoft Dynamics, MSN, SharePoint, Windows Azure, Windows Live, and Xbox LIVE are either registered trademarks or trademarks of Microsoft Corp. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

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

Contents

Cloud Computing and Privacy	1
The Evolution of Cloud Computing	2
Foundations of Cloud Privacy at Microsoft.....	3
Privacy in Today's Cloud Services for Governments and Businesses.....	5
Legal and Regulatory Challenges.....	6
Conclusion.....	7

Cloud Computing and Privacy

A new generation of technology is transforming the world of computing. Advances in Internet-based data storage, processing, and services—collectively known as “cloud computing”—have emerged to complement the traditional model of running software and storing data on personal devices or on-premises networks. Many familiar software programs, from email and word processing to spreadsheets, are now available as cloud services. Many of these applications have been offered over the Internet for years, so cloud computing might not feel particularly new to some users.

Still, several aspects of cloud computing differ markedly from previous computing paradigms and offer distinct benefits. Today’s cloud services are highly scalable, which enables customers to pay only for the computing storage and power they need, when they need it. Datacenters in diverse geographies allow cloud providers to store and back up information in multiple locations, which enhances reliability and increases processing speed. And significant economies of scale generated by “server farms” that can simultaneously support scores of users mean major cost savings for customers. (For more information, please see the Microsoft whitepaper, *[The Economics of the Cloud](#)*.)

These advantages are leading governments, universities, and businesses of all sizes to move mission-critical services such as customer relationship management, enterprise resource planning, and financial data management into the cloud. At the same time, the unique attributes of cloud computing are raising important business and policy considerations regarding how individuals and organizations handle information and interact with their cloud provider.

In the traditional information technology (IT) model, an organization is accountable for all aspects of its data protection regime, from how it uses sensitive personal information to how it stores and protects such data stored on its own computers. Cloud computing changes the paradigm because information flows offsite to datacenters owned and managed by cloud providers.

Cloud customers remain ultimately responsible for controlling the use of the data and protecting the legal rights of individuals whose information they have gathered. But defining the allocation of responsibilities and obligations for security and privacy between cloud customers and cloud providers—and creating sufficient transparency about the allocation—is a new challenge. It is important for customers and their cloud providers to clearly understand their role and be able to communicate about compliance requirements and controls across the spectrum of cloud services.

Microsoft understands that strong privacy protections are essential to build the trust needed for cloud computing to reach its full potential. We invest in building secure and privacy-sensitive systems and datacenters that help protect individuals’ privacy, and we adhere to clear, responsible policies in our business practices—from software development through service delivery, operations, and support.

¹ <http://www.microsoft.com/presspass/presskits/cloud/docs/The-Economics-of-the-Cloud.xps>

As more data moves to the cloud, however, uncertainty about legal and regulatory obligations related to that data could limit the growth of cloud computing. The technology industry has an important responsibility to pursue initiatives that improve the privacy and security of cloud computing. The private sector, however, cannot build confidence in the cloud alone. A cooperative effort from all cloud stakeholders, including governments, is necessary. Elements of a strong legal and regulatory framework for cloud computing already exist, but many aspects of this framework were designed for earlier technologies and leave important gaps in protection.

Ultimately, the technology industry, users of cloud services, and governments must agree on certain core cloud privacy practices that span industries and are harmonized across borders. Such agreements will provide greater clarity and predictability for individuals, customers, and cloud providers. As that consensus evolves, Microsoft will be an active participant in the discussion, drawing on our extensive experience in providing cloud services and our commitment to helping create a safer, more secure Internet.

The Evolution of Cloud Computing

The increasing popularity of cloud computing is part of an ongoing evolution in how people manage information. Cloud services give organizations of all sizes access to virtually unlimited data storage while freeing them from the need to purchase, maintain, and update their own computer systems. Microsoft and other cloud providers offer “IT as a service,” enabling customers to quickly scale up or down as needed and only pay for the computing power and storage they use.

Cloud services are also capable of hosting applications, often working in tandem with programs that reside on laptop computers, smartphones, and other devices. These “client-plus-cloud” services offer consumers, governments, and businesses choice, agility, and flexibility while boosting efficiency and lowering IT costs.

Cloud applications generally fall into one of three categories:

- **Software as a Service (SaaS).** The cloud provider hosts a single application, such as Hotmail®, or a suite of programs such as Microsoft’s Office 365, which includes a mix of products such as Exchange Online and SharePoint® Online.
- **Platform as a Service (PaaS).** Users create and run their own software applications while relying on the cloud provider for software development tools as well as the underlying infrastructure and operating system. Microsoft’s Windows Azure™ is one such cloud platform.
- **Infrastructure as a Service (IaaS).** Users rent computing power—either actual hardware or virtualized machines—to deploy and run their own operating systems and software applications.

Similarly, the backend systems that deliver cloud services are generally deployed in one of four ways:

- **Public cloud.** Customers access cloud services and store documents in large datacenters equipped with hundreds of virtualized servers that house data from multiple organizations.
- **Private cloud.** A single organization uses a dedicated cloud infrastructure.
- **Community cloud.** A private cloud is shared by a group of organizations with common missions, interests, or concerns.

- **Hybrid cloud.** Two or more cloud types are linked to enable data and applications to flow between them in a controlled way.

Which cloud model is most appropriate depends on the customer, the sensitivity of the data, and the type of processing required. For highly sensitive information, a private cloud can provide the greatest control and security, although at higher cost and with lower scalability and redundancy than a public cloud.

As government agencies and businesses migrate to the cloud, they are asking many of the same questions about capabilities of cloud providers. Among them:

- Are cloud-hosted data and applications protected by suitably robust privacy and data management policies? How are the policies enforced?
- Are cloud providers' technical infrastructure, applications, and processes secure?
- Are processes in place to minimize the risk and impact of any incidents that might affect privacy or security?

Security is an essential component of strong data safeguards in all online computing environments. (See the related paper titled *Information Security Management System for Microsoft Cloud Infrastructure*².) But security alone is not sufficient. Consumers' and businesses' willingness to use cloud computing also depends on their ability to trust that the privacy of their information will be protected.

Foundations of Cloud Privacy at Microsoft

Microsoft has been a leader in addressing privacy issues associated with online services since the launch of the MSN[®] network in 1994. Today, we manage a cloud-based infrastructure and platform that supports more than 200 online services and websites. We operate one of the largest online email systems, Hotmail, with more than 368 million active accounts. Xbox LIVE[®] enables more than 25 million gamers to compete against one another online.

Our experience has enabled us to develop industry-leading business practices, privacy policies, compliance programs, and security measures that we are now applying across our cloud computing ecosystem. We recognize that cloud services pose unique security and privacy challenges, and we believe that our time-tested policies and practices provide a solid foundation for addressing customer concerns and enabling greater trust in cloud computing going forward.

Microsoft has long maintained that in order for individuals and organizations to take full advantage of 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 it will be used and managed appropriately.

² <http://www.globalfoundationservices.com/security/documents/InformationSecurityMangSysforMSCloudInfrastructure.pdf>

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 have 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

Our approach to privacy and data protection is built on a commitment to empower people to 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.

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

As part of our [Trustworthy Computing](#) initiative, Microsoft employs more than 40 full-time privacy professionals across the company. Four hundred more help ensure that our privacy policies, procedures, and technologies are applied across our products, services, processes, and systems.

The Microsoft Privacy Standard for Development (MPSD) helps ensure that privacy and data protection are systematically incorporated—from the ground up—into Microsoft products and services. The MPSD includes detailed technical guidance on creating customer notification and consent procedures, providing sufficient data security features, maintaining data integrity, managing user access, and supplying controls when developing software products and websites. As part of our commitment to sharing best practices with the technology industry and the privacy community, we have released a public version of our [Privacy Guidelines for Developing Software Products and Services](#).

We regularly review the privacy policies and codes of conduct that govern our online applications, and we update them periodically if changes are needed to address consumers' evolving needs and expectations.

Privacy in Today's Cloud Services for Governments and Businesses

We are currently adapting many of the privacy policies and technologies developed for our early online services and applying them to our cloud computing solutions for governments, schools, and businesses. Both public and private organizations typically approach cloud computing with a predefined data management strategy, and they use that strategy to assess whether a given cloud service offering meets their needs. As a result, cloud privacy protections might vary depending on the business context. This situation is not new or unique to the cloud.

Regardless of the service model or type of cloud deployment, security and privacy challenges must be addressed. Cloud providers and enterprise customers have distinct responsibilities and, in some cases, shared obligations as they work to reap the benefits of cloud computing.

Microsoft addresses these challenges through a holistic approach to security and privacy that meets or exceeds the requirements of most of our customers. Our approach includes three interrelated functions to manage physical, personnel, and IT security:

- A risk-based information security program that assesses and prioritizes security and operational threats to the organization
- A detailed and continually updated set of security controls that mitigate risk
- A compliance framework that helps ensure that security controls are designed appropriately and operate effectively

Unlike businesses such as Hotmail or Xbox LIVE, in which Microsoft has direct relationships with customers and controls the policies that govern their personal data, our cloud services for organizations are designed to plug into the customer's privacy policies. The customer organization, rather than Microsoft, controls and sets policies relating to how its customers' or employees' data is handled in the cloud.

This division of responsibility is similar to when a company rents physical warehouse space to store hard-copy customer files. Even though someone else owns the building, the company that rents the space sets the policies governing access to the files and the use of the information they contain. The same principle applies in the cloud.

Microsoft has developed data handling processes in its agreements with business and government customers for popular cloud services such as [Microsoft Dynamics® CRM Online](#), [SharePoint Online](#), and [Exchange Online](#). We also provide enterprise customers with flexible management tools that help protect sensitive data and support compliance with government privacy and security guidelines.

Such transparent policies and strong tools are essential for enterprises as they deal with the privacy and security questions that arise from their use of cloud services.

Legal and Regulatory Challenges

Cloud services can thrive when cloud providers are able to provide services efficiently and assure customers that their data will remain private and secure. This has been the focus of the approach Microsoft has built over the years, and the success of that approach is reflected in our rapidly growing list of government, corporate, nonprofit, and small business customers who are using cloud services. However, as more and more data moves to the cloud, uncertainty about the legal and regulatory obligations related to that data could limit the benefits of cloud computing.

To ensure that cloud computing can reach its full potential, we need a multinational conversation on privacy and security in the cloud. One particularly complicated issue is the regulation of cross-border data flows. As cloud computing evolves, traditional geographical limits on the movement of data are changing. Information might be created in France using software hosted in Ireland, stored in the United States, and accessed in Singapore.

To optimize the efficiency of cloud services and deliver the performance and reliability customers expect, cloud providers must be able to operate datacenters in multiple locations and transfer data freely among them. Unhindered data flows allow cloud providers to optimize the efficiency of their services and deliver the performance and reliability customers expect. Regulations that restrict cross-border data transfers, or create uncertainty by failing to clearly articulate the rules that apply to such transfers, can limit the benefits of cloud computing.

Similarly, cloud providers are put in a difficult position when different governments impose conflicting legal obligations and assert competing claims of jurisdiction over data held by cloud providers. Divergent rules on privacy, data retention, law enforcement access 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 apply in a given context. However, those rules might be in direct conflict with the privacy laws of another country that has a strong claim of jurisdiction over the same data.

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

Microsoft supports efforts to develop globally consistent policy frameworks that recognize the worldwide nature of data flows while at the same time providing strong privacy protections. Governments must help craft clear rules and processes to resolve conflicting obligations in ways that protect privacy and security.

In the U.S., for instance, we believe an important first step would be for Congress to reform the principal statute for protecting user privacy in electronic communications, the Electronic Communications Privacy Act (ECPA).

ECPA was enacted in 1986 to provide a comprehensive privacy framework for data shared or stored in various types of services. ECPA grants certain protections to customer data when it is transferred across or stored in such systems and establishes rules that law enforcement must follow to access such data.

However, ECPA has been overtaken by technological change, and it no longer strikes the right balance between consumers' privacy interests and the U.S. government's legitimate need to access user information.

For example, under ECPA, e-mails stored for less than 180 days receive greater privacy protections than e-mails stored for a longer period. And while information stored on an individual's hard drive in his or her home or office would be fully protected by the Fourth Amendment to the U.S. Constitution, under ECPA a single e-mail might be subject to multiple legal standards depending on whether it is stored and waiting to be read or has been opened.

Europe's data retention framework is also inconsistently applied. EU member states have taken divergent views as to whether cloud service providers need to retain data and, if so, for how long. EU member states also disagree on what Internet-based services constitute "electronic communications services" regulated by the 2006 Data Retention Directive.

Governments around the world can enhance cloud security by increasing law enforcement resources and strengthening criminal and civil enforcement mechanisms against malicious hacking of cloud services. Although the cloud is being built with unprecedented security, the aggregation of data in cloud data centers presents new and rich targets for hackers and thieves. To combat such criminals, legislation is needed to enhance criminal enforcement of crimes targeting cloud data centers and to allow cloud service providers to sue violators directly.

Governments can also help users make informed choices by promoting transparency around cloud providers' privacy and security practices. It should not be for cloud providers to claim that their services are private and secure. Customers should be provided with information detailing why this is the case. To improve transparency, legislation should require that cloud service providers maintain comprehensive written information security programs with safeguards appropriate to the use of their services; provide summaries of those programs to potential customers, and disclose their privacy practices to any individual or customer from whom personal information is collected.

Conclusion

Cloud computing offers organizations and individuals the promise of enhanced choice, flexibility, and cost savings. To realize such benefits, however, users must have reliable assurances from cloud providers regarding the privacy and security of their personal data. Regulators and lawmakers around the world can help fulfill the potential of cloud computing by resolving legal, jurisdictional, and public policy uncertainties surrounding cloud services.

Microsoft has been addressing security and privacy issues associated with cloud computing since 1994, when we delivered our first online services for consumers and enterprises. Since then, our experience has shaped our corporate privacy policies, our product and service development guidelines, and our business practices, all of which we are now adapting to our newer cloud services.

We are committed to maintaining high the highest standards of privacy and security in our online services, and we look forward to partnering with industry leaders, governments, and consumer organizations to develop globally consistent privacy frameworks that will maximize the economic and social benefits of cloud computing.