



**Building Confidence in the Cloud:
The Need for Prompt Industry and Government Action
for Cloud Computing**

At the Brookings Institution Policy Forum,
"Cloud Computing for Business and Society"
Washington, D.C.
January 20, 2010

Brad Smith
General Counsel, Microsoft Corporation

It's a pleasure this morning to join leaders from our industry and academia to talk about cloud computing.

This is an important and timely topic. It seems that almost every week there is a new development relating to information technology and the issues it raises. Last week was no exception. The issues raised by Google relating to security and free expression are clearly important.

The world needs a safe and open cloud – a cloud that is protected from the efforts of thieves and hackers and also that serves as an open source of information to all people around the world. Neither goal may be fully achieved today – but we have to keep striving to achieve them over time.

These issues are important in countries around the world. I'd like to talk this morning about issues here in the United States.

The computing experience is undergoing a powerful transformation. Increasingly consumers and businesses alike are harnessing computing power in the cloud. We're running applications and storing documents on powerful servers located in massive data centers. We're using more powerful client devices. And we're creating, accessing, and sharing more of our personal information more frequently and with more people than ever before.

For information technology, the cloud represents a major extension of computing models. In this sense, it really has become the next frontier.

The benefits of this transformation are immense. But we need to overcome new obstacles and address new challenges as well.

As last week's issues continue to illustrate, we should not take the benefits of technology for granted. We can't afford to close our eyes to new obstacles we need to overcome. We need to build confidence

in the cloud. And that requires a new conversation about the opportunity – and need – for industry and government each to take new steps to move forward.

It's this opportunity to move cloud computing forward that I'd like to address this morning. I'd first like to touch upon the recent evolution of cloud computing and then turn to new steps that the industry and government need to take.

The label "cloud computing" reflects an attribute common to information technology. In the early stages of a new technology, we have a habit of taking everyday terms and using them in a way that most people can't possibly understand. It's perhaps not surprising that an industry that borrowed from terms as diverse as the mouse, windows, spam, and viruses should now turn to the weather to describe another big development.

It also shouldn't surprise us that the rest of the world sometimes has little idea what the heck we're talking about. A survey commissioned by Microsoft and conducted earlier this month by Penn Schoen & Berland, or PSB, showed that 76 percent of Americans either hadn't yet heard the term "cloud computing" or only knew the name and nothing else.

Despite the lack of familiarity with the term, most Americans already use technologies that constitute forms of cloud computing. The PSB survey showed that 84 percent of the general population use some sort of web mail service; 57 percent store or share information using a social media site; and 33 percent now store their photos online.

This will continue to grow. The PSB survey found that 58 percent of consumers and 86 percent of senior business leaders are excited about the potential of cloud computing to change the way they use technology. The majority of consumers and business leaders believe these technologies have the potential to help government operate more efficiently and effectively as well.

Virtually all of the leaders in our industry agree that this enthusiasm is well placed.

Cloud computing, properly implemented, provides users with greater flexibility, portability, and choice in their computing options. By running software located in a data center, users can choose to utilize applications provided by the cloud service provider itself. They can choose to develop or run their own applications while relying on the service provider for the servers, operating systems, or storage. Or they can choose to deploy and run whatever software they wish on the service provider's infrastructure, but retain control over the applications as well as things like operating systems and storage.

Users can choose to rely on a private cloud operated only for one organization. Or they can choose a public cloud, which is open to the public and may have multiple enterprises, organizations, and individuals that use the same infrastructure. There are additional alternatives as well.

In other words, together with smart client devices you can rely on the cloud for as little or as much of your computing needs – and keep as much data and computing functions locally on site – as you want.

Cloud computing offers new benefits for almost every part of society. It will lead to better delivery of health care and will help control its costs. It will provide teachers with new tools that will make classrooms more vibrant. It will contribute to economic growth and job creation. Small and medium-sized businesses are especially likely to benefit from public clouds and the computing power they offer.

And there are clear opportunities for the government itself. As the Administration's Chief Information Officer, Vivek Kundra, recently noted, "With more rapid access to innovative IT solutions, agencies can spend less time and taxpayer dollars on procedural items and focus more on using technology to achieve their missions."

These are among the many reasons we at Microsoft are excited about the potential benefits of cloud computing. We've invested billions of dollars to create a global breadth of cloud offerings. These include consumer offerings such as cloud-based email and collaboration products that have been in use around the world for over a decade, as well as new business online services that are already being used by 1.5 million people in 36 countries.

We've built large data centers around the world and have launched our new Windows Azure application platform for the cloud. We're committed to world-leading, enterprise-class services that are second to none in reliability, interoperability, and security. And we're backing this with a strong partnership ecosystem that now numbers over 7,000 partners, including companies such as HP, Accenture, Vodafone, and many others.

We also recognize that cloud computing creates the opportunity for us to pursue more open and interoperable solutions. As Ray Ozzie, our Chief Software Architect, said when we launched this new platform, "we've designed Windows Azure to be one of the most open cloud platforms on the market, and we are working hard to make Azure a great platform for all users and developers – including those who want to write or run open-source applications."

Needless to say, we're hardly alone. Everyone, it seems, is taking new steps and investing in the cloud these days.

As we move to embrace the cloud, we should ensure that we preserve the benefits of the present along the way.

We should keep in mind that one of the fundamental benefits of the personal computer revolution has been that it has made computing *more personal* in nature. It has empowered individuals to use technology in the *way* they choose. It has enabled individuals to store their information *where* they choose. It has given individuals the freedom to share their information *when* they choose and *with whom* they choose.

No technology is perfect. Nothing is perfect. But unquestionably the PC revolution has empowered individuals and democratized technology in new and profoundly important ways. As we increasingly connect smarter client devices with the resources in the cloud, our challenge is to build on these successes and make them greater still. We should not and need not sacrifice the personalization of technology in order to benefit from computers in the cloud.

These very issues are on the minds of Americans as they think about their future use of the cloud. As the PSB survey found, more than 75 percent of senior business leaders believe that safety, security, and privacy are top potential risks of cloud computing. And as they think about storing their own data in the cloud, more than 90 percent of the general population and senior business leaders are concerned about the security and privacy of personal data.

Not surprisingly, the American public expects us to take action. The majority of all audiences PSB surveyed wants us to consider the ramifications of the use of the cloud. They want us to be thoughtful

as we move forward. And they believe the U.S. Government should establish laws, rules, and policies for cloud computing.

They are right. In order to make the cloud a success, those of us in industry need to pursue new initiatives to address issues such as privacy and security. At the same time, the private sector cannot meet all of these challenges alone. We need Congress to modernize the laws, adapt them to the cloud, and adopt new measures to protect privacy and promote security.

We need a Cloud Computing Advancement Act that will promote innovation, protect consumers, and provide the Executive Branch with the new tools needed for a new technology era. We need Congress and the Administration to address three issues in particular – privacy, security, and international sovereignty.

As we think about the future of the cloud, it's only fitting that we start by thinking about the future of privacy. The protection of privacy has long been a fundamental American right, tracing its origins to the Bill of Rights and the Fourth Amendment to the Constitution.

More recently, a hallmark of the personal computer revolution has been the privacy protection afforded by the PC. In the 1980s consumers started to move their information from their desk drawer to their hard disk. They regarded their PC a bit like the advertising saying about Las Vegas – what happened on their hard disk stayed on their hard disk.

In contrast, one obvious attribute of the cloud is that information typically is stored on a server computer that is controlled by a third party. This makes it all the more important for service providers to be thoughtful and clear in deciding and communicating what they will do with this information.

Equally important, we need government action to ensure that as information moves from the desktop to the cloud, we retain the traditional balance of individual privacy vis-à-vis the state.

Americans take for granted that, except in the plots on popular television shows, the government typically cannot come into their homes without showing them a valid search warrant. But the courts have cast doubt on whether the Fourth Amendment to the Constitution, which provides this protection, applies to information that is transferred to a third party for storage or use.

The rise of cloud computing should not lead to the demise of the privacy safeguards in the Bill of Rights. The public needs prompt and thoughtful action to ensure that the rights of citizens and government are fairly balanced so that these rights remain protected.

Changes in communication technology have led to this type of situation before. Recognizing a Constitutional hole, Congress acted in the 1980s to adopt the Electronic Communications Privacy Act, or ECPA, to fill the gap. This law has played a vital role by providing Americans with statutory privacy protection for electronic and stored communication and clarifying when and how law enforcement can access such data.

But ECPA was enacted before the popularization of the Internet. Over the past two decades technology has continued to move forward, and this law has become increasingly antiquated as a result. We need new action by Congress to modernize the protection of privacy and fill in these legal gaps. This is why we at Microsoft support the efforts in this area led by the Center for Democracy and Technology, or CDT.

The protection of personal information is about more than privacy protection. We therefore need to focus on the second issue – security – as well.

Unfortunately there are and always will be bad actors interested in stealing digital information from others. At times this is because the information is valuable. At other times it is because individuals or groups are simply malicious or up to no good.

Across our industry we are building data centers with more powerful security safeguards than anything seen before. Cloud computing already has a high level of security and is ready for adoption. That's good news for consumers and businesses.

But the cloud also creates a bigger and more inviting target for hackers and thieves. We cannot close our eyes to that reality. There's no benefit in underestimating the savvy of potential attackers, now or in the future.

Across the industry we need to continue to dedicate ourselves both separately and together to strengthening the security of the cloud. We need to recognize that this will remain a daily fact of life.

As we develop new cloud services, we need to continue to take new steps to implement new security standards, such as those from the International Standards Organization and under the Federal Information Security Management Act. As the Federal Government moves information into the cloud, it needs to continue to adhere to procurement policies that ensure that it too implements these types of security standards.

We also need new steps by Congress.

Government enforcement will play a critical role in stopping and deterring attacks on the cloud, but only if Congress adapts the law to new security challenges. This is why Congress should modernize and strengthen the Computer Fraud and Abuse Act, or CFAA, to help law enforcement officials address security in the cloud.

Currently, it is sometimes difficult for federal prosecutors to establish the monetary thresholds needed to impose felony penalties. This is because it's often unclear how to place a specific monetary value on the theft of content such as documents, emails, or digital photos. A better approach would be for Congress to give prosecutors the option of applying a specified statutory amount, such as \$500, for each individual victim and then multiply this by the number of victims affected.

In addition, Congress should amend the CFAA to increase the level of fines levied against hacking into a datacenter. Today they effectively are the same as for a perpetrator who hacks into a single PC.

Congress should also strengthen the legal ability of cloud service providers to pursue their own civil claims against security violators. At Microsoft we have a Digital Crimes Unit that works with law enforcement on criminal cases and supports our own civil litigation on Internet safety issues. In some areas of the law, such as under the CAN-SPAM Act, it's clear that service providers have a private right of action. Congress should amend the law to provide service providers with a similar private right of action for security attacks on the cloud.

Ultimately, stronger laws need to be effective in practice as well as on paper. As security attacks have become more sophisticated, they have become more difficult to investigate. Effective security

protection will require new technologies to help connect all the dots. It will require even closer coordination between law enforcement agencies in single countries and across borders. And it will require even closer coordination in appropriate ways between law enforcement agencies and cloud service providers.

Congress needs to provide the Executive Branch with the resources needed for this challenge. Law enforcement will need to use these expanded resources effectively. And those of us in the private sector will need to do even more to provide our support.

In addition, both privacy and security will benefit if we as an industry follow principles that ensure clear and complete communication with consumers. We're familiar in the financial sector with "truth in lending" principles.

We need new "truth in cloud computing" principles so consumers and businesses have full knowledge of how their information will be accessed and used by service providers and how it will be stored online.

These principles should ensure that there is transparency over how data is protected. They should ensure that service providers maintain a comprehensive written information security program and disclose whether a service provider's architecture, infrastructure, and controls satisfy well-recognized and verifiable security criteria. They should convey in plain language how their information will be accessed and used by service providers, and how they can reclaim their documents and data in the future.

Simply put, it should not be enough for service providers simply to say that their services are private and secure. There needs to be some transparency about why this is the case.

One possible approach is for the industry to come together around a new self-regulatory code. Alternatively, if there is going to be law in this area – and being realistic, this seems likely – the industry and public will both benefit if this law is created at the federal rather than state level, administered by an agency such as the Federal Trade Commission. Cloud computing is national and even global in character, and it will not help if the law changes each time one crosses a state line.

Finally, in addition to privacy and security, we need Congress and the Executive Branch to address a third issue: this involves emerging issues that impact national sovereignty in the global context of cloud computing.

In recent years there has emerged a global thicket of competing and sometimes conflicting laws impacting cloud computing. For example, recent cases in Belgium, Brazil, and Italy have all sought to impose their laws on U.S. service providers even for data stored in the United States. These types of cases increasingly have raised the prospect of civil and even criminal penalties for service providers.

This is creating a catch-22 situation for the cloud. Where different laws conflict, a decision to comply with a lawful demand for user data in one jurisdiction may place a provider at risk of violating laws elsewhere. This also makes it more difficult to provide consumers with accurate information about when and how their personal information might be accessed by law enforcement.

Cloud computing will benefit the most if governments can establish a multilateral framework that provides legal clarity in the form of a treaty or similar international agreement. One such approach

would ensure a free trade zone, so to speak, for data packets. While a multilateral framework would require substantial diplomatic leadership and resources, it's a cause worth embracing.

Experience suggests, however, that a formal agreement will first require steps to lay the foundation for international consensus. There is a need for both bilateral and multi-lateral discussions between the U.S. and other governments on new procedures for resolving conflicts around data access and other legal issues. This should be complemented by a push for enhanced mutual legal assistance treaties, which would help harmonize domestic legislation regarding data privacy issues.

The Executive Branch will need to take the lead in this area. But Congress should ensure that there are adequate resources for this work and should engage in the types of international discussions that help build consensus with legislators in other countries.

As we look to the future, new steps to address privacy, security, and national sovereignty will play a vital role in helping to advance cloud computing. Those of us in industry will need to continue to be proactive, not just in developing new technology but in deploying it with a sense of responsibility and in identifying issues that merit broader consideration by others. Government will play a key role, not only in using cloud computing to enhance transparency and improve its services, but in moving the law forward to keep pace with technology.

While cloud computing continues to move forward – and to help it move forward – we need a new conversation about these new issues. It needs to be a broad conversation that includes technologists, legal experts, and representatives from industry, consumer groups, and other parts of civil society. It needs to take place in Washington, D.C., but it needs to include individuals from across the country and in many other countries as well.

This is an important topic, and it merits an important discussion. We at Microsoft look forward to taking part.

Thank you.