

# The Cloud, the Crowd, and Public Policy

*A new age of more flexible, less expensive, and more secure computing  
will emerge soon if governments act wisely.*

**T**he Internet is entering a new phase that represents a fundamental shift in how computing is done. This phase, called Cloud computing, includes activities such as Web 2.0, Web services, the Grid, and Software as a Service, which are enabling users to tap data and software residing on the Internet rather than on a personal computer or a local server. Some leading technologists have forecast that within 5 to 10 years, 80% or even 90% of the world's computing and data storage will occur "in the Cloud."

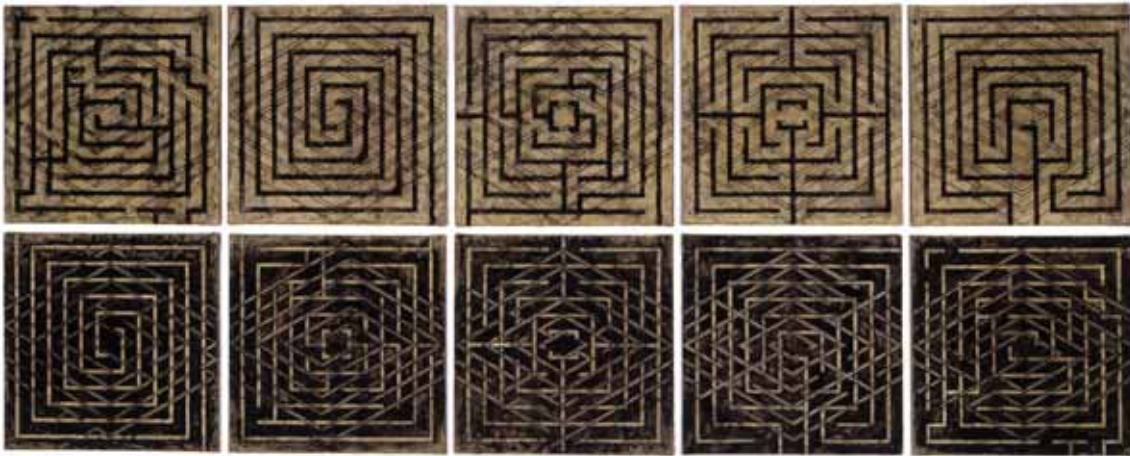
Although the move toward the Cloud is clear, the shape of the Cloud—its technical, legal, economic, and security details—is not. Public policy decisions will be critical in determining the pace of development as well as the characteristics of the Cloud.

The evolution of personal computing has occurred in three distinct phases. In phase 1, computers were stand-alone devices in which software and data were stored; typ-

ical applications were word processing and spread sheets. Phase 2 was marked by the emergence of the World Wide Web, which made it possible to access a wealth of data on the Internet, even though most users still relied on software that ran on individual machines; the quintessential application was the Web browser. In phase 3, most software as well as data will reside on the Internet; a wide variety of applications will proliferate because users will no longer have to install applications software on their machines.

Most of the work we do with computers is still done using phase 1 or phase 2 tools, but more and more people, especially among the younger generation, are starting to take advantage of the power of the Cloud, which offers:

- **Limitless flexibility.** By being able to use millions of different pieces of software and databases and combine them into customized services, users will be better able to find the answers they need, share their ideas, and enjoy online games, video, and virtual worlds.
- **Better reliability and security.** No longer will users



CHERYL GOLDSLEGER, *Sequence*, Wax, oil, and pigment on linen, 44 x 108 inches, 1998.

need to worry about the hard drive on their computers crashing or their laptops being stolen.

- **Enhanced collaboration.** By enabling online sharing of information and applications, the Cloud provides new ways for working (and playing) together.

- **Portability.** The ability of users to access the data and tools they need anywhere they can connect to the Internet.

- **Simpler devices.** Since both their data and the software they use are in the Cloud, users don't need a powerful computer to use it. A cell phone, a PDA, a personal video recorder, an online game console, their cars, even sensors built into their clothing could be their interface.

Cloud computing has the potential to reduce the cost and complexity of doing both routine computing tasks and computationally intensive research problems. By providing far more computing power at lower cost, Cloud computing could enable researchers to tackle hitherto impossible challenges in genome research, environmental modeling, analysis of living systems, and dozens of other fields. Furthermore, by enabling large distributed research teams to more effectively share data and computing resources, Cloud computing will facilitate the kind of multidisciplinary research needed to better understand ecosystems, global climate change, ocean currents, and other complex phenomena.

Combining the power of Cloud computing with data collected by thousands or even millions of inexpensive networked sensors will give scientists new and exciting ways to track how our planet and its ecosystems are changing. At the same time, such sensor nets will give entrepreneurs new

ways to provide new services, ranging from traffic monitoring to tracking livestock to improving surveillance on the battlefield or in high-crime neighborhoods.

### The government role

The pace of development and deployment of the Cloud will depend on many different factors, including how quickly the basic technology matures, how quickly the computer and telecommunications industries agree on standards, how aggressively companies invest in the needed infrastructure, how many cost-effective, compelling applications are developed, and how quickly potential users accept and adopt this new way of purchasing computing resources.

Government policy can influence each of these factors. And there are other ways in which governments can accelerate or hinder the growth of the Cloud. Just as the pace of development of the Internet has varied by country and industry, the pace of development of the Cloud will vary widely. The key policy factors that will influence the pace of progress include:

- **Research.** Giving researchers around the world access to Cloud computing services will lead to a further internationalization of science and a broadening of the base of first-class research. It will make it much easier to participate directly in multi-site projects and to share data and results immediately.

But how this happens will depend on decisions made by government research agencies. Will they make the investments needed to provide Cloud services to a large portion

of the research community? Or will separate Cloud initiatives be funded that are restricted to a narrow subset of researchers with especially large computational needs? Pre-commercial research is still needed on some of the building blocks of the Cloud, such as highly scalable authentication systems and federated naming schemes. Will there be sufficient funding for this critical R&D? Will government agencies (and the politicians who determine their budgets) be willing to fund Cloud services that will be increasingly international? Will they be willing to invest government money in international collaborative projects when the benefits (and funding) will be spread among researchers and businesses in several countries?

**Privacy and security.** Many of the most successful and most visible applications of Cloud computing today are consumer services such as e-mail services (Google Mail, Hotmail, and Yahoo Mail), social networks (Facebook and MySpace), and virtual worlds such as Second Life. The companies providing these services collect terabytes of data, much of it sensitive personal information, which is then stored in data centers in countries around the world. How these companies, and the countries in which they operate, address privacy issues will be a critical factor affecting the development and acceptance of Cloud computing.

Who will have access to billing records? Will government regulation be needed to allow anonymous use of the Cloud and to put strict controls on access to usage records of Cloud service providers?

Will government regulators be able to adapt rules on the use of private, personal information when companies are moving terabytes of sensitive information from employees and customers across national borders? Companies that wish to provide Cloud services globally must adopt leading-edge security and auditing technologies and best-in-class practices. If they fail to earn the trust of their customers by adopting clear and transparent policies on how their customers' data will be used, stored, and protected, governments will come under increasing pressure to regulate privacy in the Cloud. And if government policy is poorly designed, it could stymie the growth of the Cloud and commercial Cloud services.

**Access to the Cloud.** Cloud computing has the potential to dramatically level the playing field for small and medium-sized businesses (SMBs) who cannot currently afford to own and operate the type of sophisticated information technology (IT) systems found in large corporations. Furthermore, SMBs will also be in a position to offer their local knowledge and specialized talents as part of other companies' services. Likewise, researchers, developers, and entrepreneurs in every corner of the world could use Cloud com-



CHERYL GOLDSLEGER, *Caliper*, Wax, oil, pigment, and wood on linen, 18 x 18 inches, 2005.

puting to collaborate with partners elsewhere, share their ideas, expand their horizons, and dramatically improve their job prospects—but only if they can gain access to the Cloud. Telecommuters and workers who are on the road will also have access to the same software and data used by those in the office, provided that we increase broadband access in the home and over wireless connections.

As a result, development of the Cloud will increase pressure on governments to bridge the digital divide by providing subsidies or adopting policies that will promote investment in broadband networks in rural and other underserved areas. Unfortunately, the main impact of many previous efforts to promote network deployment has been to distort the market or protect incumbent carriers from competition. As Cloud computing become critical for a large percentage of companies, governments will need to find cost-effective ways to ensure that homes and businesses have affordable access to the Cloud no matter where they are located.

**E-government and open standards.** Cloud computing could provide huge benefits to governments. The Cloud is not a magic wand for solving hard computing and managerial problems, but it will reduce barriers to implementation, eliminate delays, cut costs, and foster interagency cooperation. A few pioneers, such as the government of Washington, DC, have already demonstrated the huge potential of Cloud computing for e-government. Vivek Kundra, then the chief technology officer for DC, led an effort to migrate thousands of DC government employees to Google e-mail and office software based in the Cloud. “Why should I spend millions on enterprise apps when I can do it at one-tenth the cost and ten times the speed?” he said in 2008. “It’s a win-win for me.”

Cloud computing will be particularly attractive to government users because of its increased reliability and security, lower maintenance costs, and increased flexibility. Running government operations on a unified Cloud infrastructure will be more secure and reliable, and less costly, than trying to maintain and manage hundreds of different systems. In addition, if done right, Cloud computing can help governments avoid being locked in to a small number of vendors.

Governments have the potential to be model users of Cloud computing. As the largest economic entity in most countries, government has the leverage to set standards and requirements that can influence actions throughout the economy. Just as U.S. federal government Web sites demonstrated the power of the Web and inspired state and local governments and companies to create online presences, national governments can be early adopters of Cloud computing, which would demonstrate and publicize the technology. But

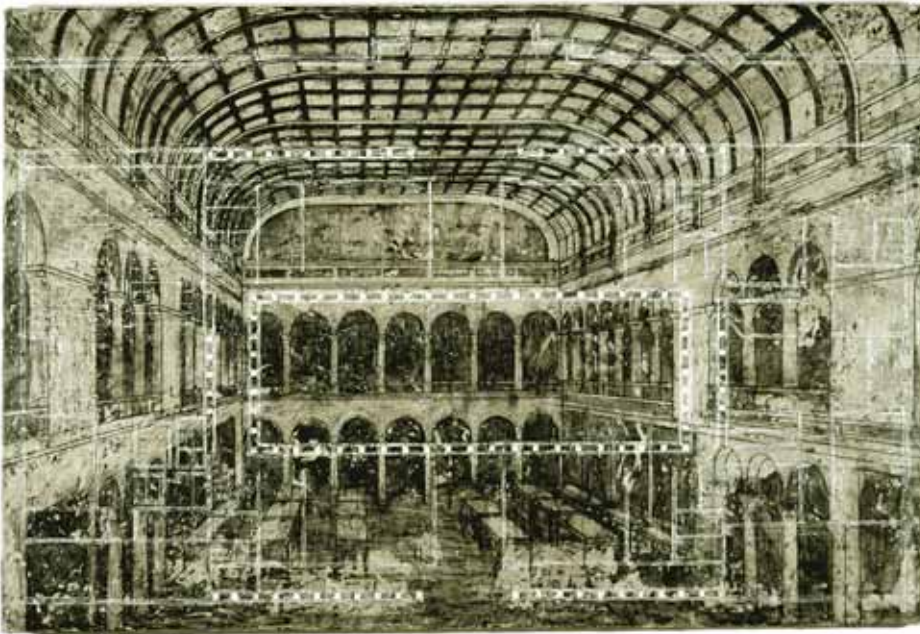
if governments are going to become early adopters of Cloud services, they must overcome bureaucratic, regulatory, and cultural barriers to resource sharing that could slow the adoption of Cloud computing. Government IT procurement rules covering purchase of hardware and software must be updated to enable purchase of Cloud services.

U.S. government procurement decisions in the 1980s, which led to the widespread use of the Internet Protocol to link together previously unconnected agency networks, were a critical driver at a crucial time in the development of the Internet. Likewise, major government users could play an important role by compelling industry to quickly reach consensus on open, international Cloud standards so that government suppliers, contractors, and partners would be able to easily tap into government-funded Cloud services.

Today, many different grid and Cloud architectures rely on incompatible proprietary software. Achieving the full potential of Cloud computing will require a “Cloud of Clouds”: different network-based platforms all linked together by common middleware, so that data and applications software residing on one company’s piece of the Cloud can be seamlessly combined with data and software on systems run by another Cloud service provider.

**Competition and antitrust.** The structure of the Cloud will be defined over the next few years as key players establish the standards and technologies for Cloud services and as business models and business practices evolve. Perhaps the most important factor determining how the Cloud evolves is whether one company or a handful of companies are able to achieve a dominant position in the market for Cloud services or whether the Cloud becomes an open interoperable system where hundreds or even thousands of different companies are able to build and run part of an interlinked, interoperable Cloud capable of running different applications developed by millions of developers around the globe.

With the Internet, strong economic benefits and customer demand both pushed network service providers to link their different networks and create a network of networks. The situation may not be as clear-cut with the Cloud, and some companies building the infrastructure of the Cloud may be able to use economies of scale, ownership of key intellectual property, and first-mover advantage to block or slow competitors. Governments will need to watch carefully to see that companies do not use their dominant position in one sector of the IT or telecommunications market to gain an unfair advantage in the market for Cloud services. A Cloud built by only one or two companies and supporting only a limited set of applications would not be in the best interest of either individuals or corporate customers.



CHERYL GOLDSLEGER, *Woman's Building*, Wax, oil, and pigment on linen, 54 x 80 inches, 2003.

Governments need to take cautious rather than radical actions at this time, and to promote open international standards for the Cloud so that users will be able to switch Cloud service providers with a minimum of cost and risk. Flexible, far-sighted government policy and procurement decisions could promote interoperability, without dictating a particular architecture or set of standards for the Cloud. Since the Cloud is still evolving rapidly, governments need to allow and encourage different companies and groups to experiment. For instance, in government procurements for cloud services, governments can require interoperability and migration plans in case an agency wishes to change Cloud service providers at a later date, without specifying a particular standard or a particular company's service. In the 1980s and 1990s, when personal computers were being widely adopted, some governments took the wrong approach; they chose Microsoft Word as their government-wide word-processing standard, rather than embracing an open standard such as the Open Document Format and requiring all vendors to support it. Later, some of those same governments had to resort to antitrust actions against the Microsoft monopoly they helped create.

**Wiretapping and electronic surveillance.** One of the thorniest issues related to the Cloud may be electronic surveillance, particularly when it spans international borders. In the United States, citizens are protected by the Constitution against unreasonable search and seizure. In most cases, the police must get a search warrant to examine data on someone's home computer. It is not at all clear that the

same data are protected if they are backed up in a data center in the Cloud, particularly if that data center is in another country. And if the situation within the United States is unclear, it is even less clear how and when U.S. or other intelligence services can access data from noncitizens stored in the Cloud. If users believe that governments will be monitoring their activities, their willingness to use the Cloud for important functions will surely decrease.

**Intellectual property and liability.** Related to the question of wiretapping is whether governments will try to enforce laws against online piracy in ways that limit or slow the development of Cloud services. By giving customers access to almost unlimited computing power and storage, Cloud services could make it even easier to share copyrighted material over the Internet. Will Cloud service providers be required to take special measures to prevent that? Will they be liable for illegal activities of their customers? Would doing so make it impractical for companies to provide Cloud services to the general public?

**Consumer protection.** If companies and individuals come to rely on Cloud services such as e-mail, word processing, and data backup, and then discover that the services are down for a protracted period of time, or worse, that their data are lost, they will seek recourse—most likely in court. If the reliability of Cloud services becomes a serious problem, state and national governments may step in to ensure that customers get the service they expect.

What kind of liability will a company that provides Cloud services be expected to assume in the event that there are

serious outages? If a program running in the Cloud malfunctions, it could affect other users. Yet tracking problems in the Cloud and assigning responsibility for failures will be difficult. The Internet is already causing telecommunications companies and the courts to adopt new approaches to assigning liability for outages and security breaches.

Crafting a consistent global approach to this problem will not be easy, but if it can be done, it could increase consumer trust and significantly accelerate the adoption of Cloud services. Given the difficulty of finding an international governmental approach to consumer protection in the Cloud, a global self-regulatory approach based on best practices, insurance, and contract law may be faster, more flexible and adaptable as technology evolves and new services are offered, and more effective.

### **Taking the lead**

Governments will play a critical role in shaping the Cloud. They can foster widespread agreement on standards, not only for the basic networking and Cloud communication protocols, but also for service-level management and interaction. By using the power of the purse in their IT procurement policies, governments can pressure companies to find consensus on the key Cloud standards.

Governments need to assess how existing law and regulations in a wide range of areas will affect the development of the Cloud. They must both “future-proof” existing law and ensure that new policy decisions do not limit the potential of this revolutionary new approach to computing.

The greatest concern would be premature regulation. The Cloud will be a fundamental infrastructure for the economy, national security, and society in general. A natural reaction would be to demand uniformly high quality and to regulate a number of features and services that use it. But without a lot more experience, we simply do not know enough about what the right set of underlying services will be, what are appropriate differences in price and quality of services, what techniques will be best for providing reliable service, and where the best engineering tradeoffs will be.

Governments can add value by encouraging experimentation and new services. They must avoid locking in the wrong technology, which will either put a country at a competitive disadvantage or reduce the value of the Cloud as a whole. Governments must follow industrial practice as much as possible rather than mandating untried solutions.

Like the Internet itself, the Cloud is a disruptive technology that challenges existing business models, institutions, and regulatory paradigms. As a result, there is likely to be resistance from many different quarters to the widespread deployment of Cloud technologies. Governments must be willing to challenge and change existing policies that could be used to hinder the growth of the Cloud. Simply trying to adapt existing regulations to the Cloud might allow entrenched interests to significantly delay the investment and effort needed for widespread use of Cloud computing. Because Cloud computing is a fundamentally different approach to computing and communications, governments should consider fundamentally new approaches to telecommunications and information policy.

Many of the public policy issues, including privacy, access, and copyright protection, raised by Cloud computing are similar to Internet policy issues that governments have been struggling with for at least 15 years. However, addressing these issues for the Cloud will be at least twice as difficult—and five times more important. Because the Cloud is inherently global, policy solutions must be cross-jurisdictional. Because the Cloud is a many-to-many medium, it is not always easy to determine who’s responsible for what. And because the Cloud technology and Cloud applications are evolving so quickly, government policy must be flexible and adaptable. Because the challenges are so great and the opportunities so widespread, it is imperative that policymakers and the technologists developing the Cloud start now to look for innovative technical and policy solutions.

*Michael R. Nelson (mnelson@pobox.com), a visiting professor at Georgetown University in Washington, DC, is the former director of Internet technology and strategy at IBM.*