2010

Navigating the Challenges of the Cloud

Steven Ovadia
CUNY La Guardia Community College

Behavioral & Social Sciences Librarian, 29:233–236, 2010

ISSN: 0163-9269 print / 1544-4546 online
DOI: 10.1080/01639269.2010.498764

Routledge
Taylor & Francis Group

INTERNET CONNECTION

Navigating the Challenges of the Cloud

STEVEN OVADIA
LaGuardia Community College, Long Island City, New York

Cloud computing is increasingly popular in education. Cloud computing is "the delivery of computer services from vast warehouses of shared machines [that] enables companies and individuals to cut costs by handing over the running of their email, customer databases or accounting software to someone else, and then accessing it over the internet" ("Unlocking the Cloud" 2009). Simply put, this means software and data are accessed through the Internet rather than a local hard drive. Part of the popularity is the convenience cloud computing provides. It tends to make collaboration easier and often removes the need for specialized software. Most cloud systems simply require a Web browser to be accessed from any computer. But while the cloud has made many activities easier, it also has some serious, potentially negative implications that often are not fully addressed within the general conversations about cloud computing.

Before discussing the potential pitfalls of the cloud, it seems only fair to address the positive aspects. For instance, it is becoming an almost ubiquitous part of computing. Nelson (2009) estimates that more than 80% of the world's computing and data storage could occur within a cloud environment within the next five years.

Jaeger, Lin, and Grimes (2008) point out the computer processing power and data storage available within a cloud environment, making what was once an expensive investment proposition affordable to less resource rich groups like small businesses, nonprofits, and, of course, academics. They also point out that cloud services also serve as technical administrators, often eliminating the need for a local IT hiring line or helping to alleviate the workload on an existing IT department. Still, despite these benefits, there are some dangers when dealing with cloud computing that often are not fully addressed in the zeal to capitalize on its benefits.

Address correspondence to Steven Ovadia, LaGuardia Community College, Library Media Resources Center, 31-10 Thomson Avenue, Long Island City, NY 11101. E-mail: sovadia@lagcc.cuny.edu

When discussing the cloud, Doc Searls (2008) makes a distinction between infrastructure and commerce, pointing out that most cloud services exist as businesses, designed to make money, as opposed to public utilities providing a public service. With commerce as a *raison d'etre*, cloud computing companies need to make sound financial decisions that are not necessarily in the best interest of their users. For instance, a cloud computing business currently providing a free service may decide it needs to start charging for usage. What happens to users who cannot afford the service yet have become dependent on it?

Security is also always an issue when dealing with cloud computing. Not having to administer a cloud environment is convenient, but it also creates a level of separation between the company hosting the cloud and the organization using the cloud. The dangers of this separation became apparent when Google reported the theft of its password system (Markoff 2010). Google said they were making immediate changes to their password system to prevent the thieves from gaining access to private user information, including Google-hosted e-mail. The theft illustrates the security challenges of the cloud environment. Users relying on non-locally-hosted clouds do not have full control over the security protecting their data. Additionally, when using a large, well-known cloud host, such as Google, one's data becomes more of a target since there is more interest in exploiting the weaknesses of a high-visibility target.

So knowing all of this, what is a user to do? Ignore cloud applications? Push forward and hope for the best? Right now, there's no clear answer other than to assess each cloud application in terms or acceptable risk and acceptable data loss, either as an individual or an institution. But there are some intriguing ideas on the horizon that could positively impact cloud-hosted services.

One of the more intriguing ideas is the Open Cloud Manifesto, a document issued by a coalition of technology companies calling for a general openness within cloud computing environments, allowing users to easily switch cloud-based services without prohibitively detrimental service outages (Hamm 2009). Beyond that general statement of an ideal/goal, the Open Cloud Manifesto, whose list of supporters is now over 300 companies, has not produced specific documentation or standards on how to create an open cloud. Open cloud standards would be helpful for users, though, as they would allow users to more easily migrate data from one cloud platform to another, giving them more choices and forcing cloud hosts to be more responsive to user requirements since users could easily move their data to another host if a host was no longer providing an acceptable level of service.

Another interesting project is EyeOS, an open-source cloud computing framework. The EyeOS project allows users to create their own cloud environment, with users able to word process, create spreadsheets, use calendars,

and send and receive e-mail (EyeOS 2010). But while cloud services are traditionally hosted by a third party on servers not owned or controlled by the user or their organization, the EyeOS allows users and/or organizations to install a cloud-computing service on their own servers, letting an organization create their own cloud. Users can also develop custom cloud-hosted applications, assuming, of course, they have the technical skills to do so.

This is an interesting proposition in that it provides the convenience of a cloud and the control of a locally hosted application or service. However, getting a service like EyeOS running and functioning could require a lot of time and effort, depending on the skills and personnel of the organization interested in using it.

Microsoft SharePoint represents a more established cloud-based, locally hosted solution. SharePoint is a cloud-based service that allows users to manage calendars, documents, and even provides Wiki functionality. Unlike third-party cloud-based services, though, SharePoint is installed on a locally controlled server, thus, like EyeOS, it gives users administrative control over their own cloud. Like EyeOS, the organization using SharePoint is gaining both control and additional administrative responsibilities.

This column is not intended to dissuade readers from using third-party cloud-based services. In many applications, a third-party cloud is entirely appropriate. However, there are dangers, ramifications, and complications caused by giving one's data over to someone with whom a user has not explicitly negotiated the terms of the data storage. The cloud is convenient and can represent short-term cost savings, but organizations must consider their long-term needs and determine if their cloud-based hosts can grow with an organization's needs over time.

In general, information technology experts tend to think in terms of data security, but it is up to librarians to remind users about the importance of data portability. Secure data in a cloud is a very useful thing, but it does not do users much good if they have no way to move their secure data to a different environment. What good is security if users have no choice in where they can move their data?

Services like Google Docs, Flickr, and even Facebook help prevent local computer failures from becoming the catastrophic loss of data. But once those files no longer exist locally, users and organizations need to think about their long-term access needs. Easy access to a third-party cloud now does not guarantee that same kind of access tomorrow. Librarians need to make sure users understand the enduring responsibility that is access and data portability. Teaching users to navigate and understand hosted, cloud-based services is not helpful if they are also not taught how best to preserve their data over time.

As clouds become a more common phenomenon, users become more and more used to the idea of uploading important data into the cloud. As users upload more data into the cloud, they become more dependent on

the cloud, and as users become more dependent on the cloud, they become more vulnerable to any failure or changes within the cloud. A generation of students and faculty with empty document folders is not so far away. It is a good idea to remind users of the importance of information redundancy as a means of protecting data, to prevent a generation of users who are utterly dependent on the whims of a cloud host.

In order to make sure users are never too dependent on non-locally-hosted clouds, librarians also need to become more aware of cloud projects that allow institutions and individuals to create their own clouds, giving them the convenience of the cloud coupled with the security and data portability of a locally hosted application.

Jaeger, Lin, and Grimes (2008) also discuss the policy issues of cloud computing, breaking it down into three areas that must be considered when deciding whether to migrate data and/or services into a cloud. The three main ideas they describe are reliability and liability; security, privacy, and anonymity; and access and usage restrictions. They also bring up the issue of standardization of data to promote "data flows in clouds." There is not enough space here to extensively explore those ideas, but any user contemplating some kind of move to the cloud probably should consider his expectations for how the cloud host can address each of those three ideas. Cloud computing can be a wonderful thing as long as all parties are clear on their responsibilities as users and as administrators.

REFERENCES

EyeOS. 2010. What is eyeOS?http://eyeos.org/index.php?p=whatiseyeos_overview (accessed May 2, 2010).

Hamm, Steve. 2009. Meet the open cloud manifesto. *BusinessWeek Online*, March 30. http://www.businessweek.com/technology/content/mar2009/tc20090329_463505.htm (accessed May 2, 2010).

Jaeger, Paul T., Jimmy Lin, and Justin M. Grimes. 2008. Cloud computing and information policy: Computing in a policy cloud? *Journal of Information Technology and Politics 5*(3): 269–283.

Markoff, John. 2010. Cyberattack on Google said to hit password system. *New York Times*, April 19. http://www.nytimes.com/2010/04/20/technology/20google.html.

Nelson, Michael. 2009. Building an open cloud. *Science 324*: 1656.

Searls, Doc. 2008. Stallman vs. clouds. *Linux Journal*. http://www.linuxjournal.com/content/stallman-vs-clouds.

Unlocking the cloud. 2009. *Economist 391*(8633): 18.