Issues in TECHNOLOGY Innovation

Number 1 July 2010

Steps to Improve Cloud Computing in the Public Sector

Darrell M. West

EXECUTIVE SUMMARY

Government information technology is subject to a variety of rules, regulations, and procurement policies. Computing is treated differently depending on whether the platform is based on desktops, laptops, mobile devices, or remote file servers known as cloud computing. There are differences between the executive, legislative, and judicial branches of government, as well as in the level of privacy and security expected for various applications.

© Martin Barraud

Some people perceive higher security on desktop or laptop computers and lower security with the cloud because the latter's information is stored remotely through third-party commercial providers. In reality, though, there are serious security threats to all electronic information regardless of platform, and cloud server providers often take security more seriously than mass consumers or government officials employing weak passwords on their local computers.

In this paper, I review current federal IT policy and discuss rules, practices, and procedures that limit innovation. There are a variety of obstacles that make it difficult for policymakers to take full advantage of the technological revolution that has unfolded in recent years. After outlining these issues, I make recommendations on policy changes required to improve the efficiency and effectiveness of federal computing.

Issues in Technology Innovation

The Center for Technology Innovation at Brookings has launched its inaugural paper series to seek and analyze public policy developments in technology innovation.

The Center for Technology Innovation

Founded in 2010, the Center for Technology Innovation at Brookings is at the forefront of shaping public debate on technology innovation and developing data-driven scholarship to enhance understanding of technology's legal, economic, social, and governance ramifications.

My specific recommendations include:

1) Public officials should develop more consistent rules on computing across desktop, laptop, mobile, and cloud platforms.
2) The use of video, collaboration, and social networking should be authorized for congressional offices. This would make legislative branch policy consistent with that of the executive branch.
3) Judicial branch computing should be modernized, with greater emphasis on cloud computing.
4) There should be a more uniform certification process for federal agencies. Right now, each agency is responsible for certifying its own applications. It makes sense to have a "joint authorization board" with the power to review management services and certify particular products for use across the government.
5) Congress should update the Electronic Communications Privacy Act to change the process by which law enforcement agents obtain electronic information. Instead of using a prosecutor's subpoena, legislation should require a "probable cause" search warrant that is approved by a judge. This would provide greater safeguards in terms of online content, pictures, geolocation data, and e-mails.
6) Privacy rights should be placed on the same footing regardless of whether a person is using desktop or cloud computing. It makes little sense to have weaker standards on one platform than another. Consumers and government decision-makers expect the same level of protection whether they are accessing information on a desktop, laptop, mobile, or cloud storage system.
7) Congress should amend the Computer Fraud and Abuse Act to strengthen penalties for unwanted intrusion into computing systems. The law has inconsistent penalties and prosecutors have found that it is hard to prosecute cyber-crimes.
8) Apps.gov represents a big step forward and government use should be expanded because it makes procurement easier and speeds public sector innovation. It is a model of how the government can reinvent itself through digital technology in ways that improve efficiency and effectiveness.
9) Countries need to harmonize their laws on cloud computing so as to reduce current inconsistencies in regard to privacy, data storage, security processes, and personnel training,
10) There should be mechanisms for data exchange that encourage portability across platforms. We should avoid vendor lock-in that precludes data exchange.

Darrell M. West is the founding director of the Center for Technology Innovation at Brookings. He is also vice president and director of Governance Studies and a senior fellow.

11) Data on uptime, downtime, recover time, archiving, and maintenance schedules would help build public trust by providing information on computing performance.

Problems of Federal Computing Policy

The public sector makes relatively little use of cloud computing even though the private sector has achieved excellent cost savings and studies have suggested substantial government savings from a migration to the cloud.

The U.S. federal government spends nearly $76 billion each year on information technology, and $20 billion of that is devoted to hardware, software, and file servers (Alford and Morton, 2009). Traditionally, computing services have been delivered through desktops or laptops operated by proprietary software. But new advances in cloud computing have made it possible for public and private sector agencies alike to access software, services, and data storage through remote file servers.

Right now, cloud computing constitutes a relatively small amount of federal IT spending. In 2008, for example, only $277 million of the federal government's IT budget was devoted to cloud computing (Wyld, 2009, p. 20). A recent Governmental Accountability Office study undertaken by Wilshusen (2010) found that only half of the 24 federal agencies surveyed employ any type of cloud computing. The public sector makes relatively little use of cloud computing even though the private sector has achieved excellent cost savings and studies have suggested substantial government savings from a migration to the cloud (West, 2010; Kundra, May, 2010).

With the convenience, scalability, and cost savings associated with the cloud, there are reasons to increase the federal effort devoted to cloud computing (Benioff, 2009). Public agencies can gain greater efficiency through cloud applications and storage devices. They can improve flexibility in serving agency needs. In requesting bids for enterprise e-mail and collaboration systems, a recent General Services Administration Request for Proposal (2010) recognizes the limitations of current e-mail systems and advantages of cloud-based services.

Despite the promise of cloud computing, there are four problems that result from the current computing environment. The government has inconsistent policies across computing platforms. In some respects, cloud applications are disadvantaged in current legal and procurement situations. For example, courts often support greater privacy rights with local rather than remote file storage.

Second, there is a need for greater performance transparency. With the considerable uncertainty that exists in regard to the reliability and security of information technology, officials need to think about how to instill greater confidence among consumers and taxpayers (Hart, 2008).

Third, there should be detailed conversations regarding the tradeoffs between privacy and security. There is some tension between these two goals. Potential security problems need to be addressed, but sometimes this involves increasing the level of real or imagined privacy threats.

Finally, the lack of uniformity in standards across nations has created a "Tower of Babel" atmosphere among cloud computing. Different nations have contrasting rules

on privacy, security, storage, and accessibility. This makes it difficult for cloud providers to deliver on the full promise of information technology.

Needed Policy Changes

To deal with these problems, I suggest a number of policy changes in order to improve the efficiency and effectiveness of federal IT policy. This includes shifts in federal practices, policies, and procedures.

Consolidate Number of Federal Data Centers

The federal government has over 1,100 federal data centers. This is up from 432 a decade ago (Kundra, July, 2010). The financial cost and energy requirements for maintaining this many data centers is enormous. Most data centers function at low-level storage capacity because agencies never want to run out of disk space. Some studies have estimated federal storage usage running as low as 7 percent (Bradshaw, 2010). Others have found storage capacity averaging from 7 to 15 percent (Goodrich, 2010).

Cloud storage and service utilization provide greater efficiency because users pay only for the server space they actually used (Federal Communications Commission, 2010). It is easy to scale up to higher storage as needs arise, so taxpayers can gain budget efficiencies in the process. With many government file servers currently under-utilized, we need to consolidate the number of federal data centers and migrate applications to the cloud (Office of Management and Budget, 2010). This would save money while also improving service delivery.

Allow Video, Collaboration, and Social Networking in Congressional Offices

Congressional offices have been slow to embrace many forms of technology innovation. Legislative policymakers still have rules that place limits on various types of digital communications. It has been only recently that rules were changed allowing the use of video and social networking sites, such as YouTube and Facebook.

Employment of phone conferencing applications such as Skype still are not allowed in House offices (Romm, 2010). Members can use this service on mobile or WiFi Internet networks, but not on desktop machines. Legislative leaders have labeled Skype as "unauthorized" because of fears the service would be vulnerable to security threats. If the phone conferencing feature is a security risk on desktops, why is its use allowed on mobile devices? These are the type of inconsistencies that make little sense in government computing policy.

Modernize Judicial Computing Usage

The judicial branch of government lags the executive or legislative branch in technology innovation. Past research undertaken by West (2008) shows that federal courts rank more poorly on many indicators of information technology than the rest of the public sector. They are less likely to feature online services, have interactive features, provide mechanisms for visitor feedback, or allow visitors to personalize the site to specific interests. Of the 61 federal sites rated, 13 of the bottom 16 performers were federal court sites, such as the Supreme Court or appellate courts from around the country.

There is far less cloud usage in the judicial than executive or legislative branches of government. Court officials need to consider ways to modernize judicial computing usage in general but cloud computing in particular. There are economies and efficiencies to be gained by migrating some court applications to the cloud. Some agencies have found cost savings of 25 to 50 percent from transferring e-mail services to cloud platforms (West, 2010).

Employ Government-Wide Contracts and Certification Processes

Many federal departments order software and hardware on an agency by agency (McClure, 2010). This makes it difficult for the federal government to take advantage of its huge purchasing power to gain economies of scale. Government-wide contracts would allow public officials to drive harder bargains and become more efficient in its use of federal resources.

We need a more uniform certification process for federal agencies. Right now, each agency is responsible for certifying its own applications (Kundra, July, 2010). Something approved by one department has no guarantee it will meet the certification standards of another department. This creates unnecessary inconsistency and delays in the procurement process as vendors go through multiple checkups for the same product.

It makes sense to have a "joint authorization board" with the power to review management services and certify particular products for use across the government. The new Federal Risk and Authorization Management Program (FedRAMP) represents a big advance toward a government-wide approach to certifying and accrediting particular applications. It should be used to expedite technology innovation in government.

Update Electronic Communications Privacy Act of 1986

Current privacy rules were written before the Internet was formally established and online content became ubiquitous. In 1986, most people did not use e-mail, the Internet, social networking, cloud, or file-sharing websites (Charney, 2010). As a result, when Congress approved the Electronic Communications Privacy Act (ECPA),

the law was vague or inconsistent in how it treated privacy provisions. For example, privacy advocates point out that electronic communications currently have stronger safeguards if stored on local than remote file servers. "The main thing that's broken about ECPA is that it penalizes you for using cloud computing," said Marc Zwillinger, a privacy law attorney (McCullagh, 2010).

The reason for differential privacy protection is that a number of court cases in recent years have witnessed judges deciding that people who share information with third parties have a diminished expectation of privacy and therefore do not have the same Fourth Amendment guarantees against unreasonable search or seizure by government authorities. By definition, material stored on a cloud involves voluntarily sharing material with a third party. In the eyes of judges, that puts privacy on cloud platforms on a lower level than that associated with desktop, laptop, or mobile devices. This means that when law enforcement agents request e-mails, Internet usage, or other electronic communications, they can satisfy a lower threshold for accessibility with cloud applications.

It is not clear that cloud servers face more serious security risks than local ones.

We need to place privacy on the same footing whether a person is using desktop or cloud computing. It makes little sense to have weaker standards on one platform than another. Consumers and government decision-makers expect the same level of protection whether they are accessing information on a desktop, laptop, mobile, or cloud storage system. The platform does not affect their personal practices or expectations of privacy.

One change that would be desirable concerns the process by which law enforcement agents can obtain electronic information. Instead of using a prosecutor's subpoena, legislation should require a "probable cause" search warrant that is approved by a judge (Helft, 2010). This would provide greater safeguards in terms of online content, pictures, geolocation data, and e-mails.

Protect Security on Government Cloud Platforms

Security represents a major consideration in cloud migrations for government agencies (Furlani, 2010). Indeed, a Government Accountability Office study undertaken by Wilshusen (2010) found that "22 or 24 major federal agencies reported that they are either concerned or very concerned about the potential information security risks associated with cloud computing. Risks include dependence on the security practices and assurances of a vendor, and the sharing of computing resources."

People sometimes perceive higher security on desktop and laptop computers because they physically control those devices and lower security with the cloud because information is stored remotely through third-party commercial providers and public clouds feature multi-tenancy. In reality, though, there are serious security threats to all electronic information regardless of platform. It is not clear that cloud servers face more serious security risks than local ones. After all, the federal government currently relies on 4,186 different contractor systems, many of which are

commercial-based systems featuring desktop, laptop, or mobile computing.

Desktop, laptop, and mobile devices face security threats owing to theft, loss, or compromised information (Bradshaw, 2010). Since individuals are in charge of password protection on these devices, security often is weak because people don't want to be bothered with "strong" passwords and instead use passwords linked to their pet, birthday, anniversary, education, or sports team. With the advent of social networking sites, this "personal" information frequently is shared with strangers, which makes it difficult to maintain the integrity of desktops, laptops, or mobile devices.

Even though the cloud often is perceived as less secure because it is outside the physical control of the user, in many cases, cloud service providers employ much more rigorous security standards than local computers. Many use encrypted or highly-secure passwords featuring complex combinations of letters, numbers, and characters. Most providers also insist on highly-secure facilities having armed guards, limited access, and detailed employee background checks.

Despite this reality, the major federal law in this area, the Computer Fraud and Abuse Act of 1986, is unclear in its definition of presumed losses through cloud computing. It sets forth definitions of cyber-crime and establishes penalties based on unauthorized access and presumed losses.

However, it is vague on whether the maximum penalty of up to five years in jail and as much as a $250,000 fine for unwarranted intrusions applies to the cloud data center as a whole or each individual and business account that is accessed. Ideally, penalties should apply to each cloud account that is compromised. Otherwise, the penalties for unwanted cloud intrusions are artificially low given the magnitude of the possible losses.

Congress should amend the Computer Fraud and Abuse Act to strengthen penalties for unwanted intrusion into computing systems. The law now has inconsistent penalties and prosecutors have found that it is hard to prosecute cyber-crimes. We need to close that loophole in order to assure effective enforcement of the law.

The National Institute of Standards and Technology and General Services Administration currently are developing security standards for low, moderate, and high-risk applications (Mell and Grance, 2009). Organizations that have highly sensitive or classified information obviously require greater safeguards, both in terms of monitoring and firewalls. The federal government currently has rolled out "low-risk" cloud solutions and soon will be doing the same thing for "moderate-risk" applications.

To assure security, the General Services Administration (2010) standard for e-mail is that we need systems that are stored in at least "two different data center facilities at two different and distant geographic locations." Eventually, the federal government aims to meet "high-risk" security needs for agencies such as the Department of Defense. It plans to roll out these applications for software, platform, and infrastructure needs this year (Lewin, 2009).

Government agencies need to develop safeguards appropriate to the mission of each organization (Hoover, 2010). With concern over cyber-security threats, there are pressures to increase security safeguards and maintain secure facilities (Amoroso, 2006). But officials need to be cognizant of the costs and benefits of enhanced security safeguards. It is clear that the greater the need for highly secure storage and applications, the higher the cost of the cloud and the less the possible cost savings that may come from cloud migration. Agencies with high security needs generally require that information be stored in secure facilities within the continental United States and operated by individuals with high-level security clearances who have passed background checks.

Expand Apps.gov

Government procurement of electronic services is a long and cumbersome process. There is a lengthy review process by specific agencies and it takes a considerable amount of time to certify and authorize new products. This hinders innovation and makes it difficult to acquire new services in a timely manner.

Recently, the federal government has streamlined the provision of cloud solutions through www.Apps.gov. This site allows agency officials to purchase cloud computing services in 33 different categories such as management, productivity, and social media applications. Among the business apps are ones for asset management, business processes, dashboard, data management, geographic information, surveys, and travel. Productivity apps include video conferencing, office tools, project management scheduling, and workflow. Social media possibilities include search tools, blogs, videos, and contests.

Many of these fall within the Federal Information Security Management Act certification for "low-risk" solutions. Some are free applications from providers who accept "government friendly" terms of service (McClure, 2010). Apps.gov represents a big step forward because it makes procurement easier and speeds public sector innovation. It is a model of how the government can reinvent itself through digital technology in ways that improve efficiency and effectiveness.

Seek International Agreements on Cloud Computing Rules and Norms

Another problem crucial for long-term cloud development is the lack of uniformity of national laws across borders (Thibodeau, 2010). Many countries have different rules or norms on cloud computing, privacy, data retention, security processes, and personnel training. It is hard to get the full efficiency of cloud computing when laws are inconsistent or contradictory. Sometimes, countries require data disclosure even if the cloud data center is not located within their national boundaries.

Rules on cross-border transactions via the cloud should be clarified and harmonized where possible in order to facilitate innovation and get the greatest economies of scale from new technology. We need international agreements

harmonizing national rules so that the current "Tower of Babel" doesn't undermine fiscal efficiencies or utilization of cloud platforms.

A World Economic Forum study (2010) ranked collaboration with other governments to reduce the complexity of compliance requirements as the most important priority. Leaders in a number of different countries see cross-border differences as problematic and in need of resolution.

Data on uptime, downtime, recover time, archiving, and maintenance schedules would help build public trust in the cloud, as would information on what providers are doing to safeguard security standards.

Make Sure Information is Portable Across Platforms

We need mechanisms for data exchange that encourage portability across platforms. This includes desktop to cloud, cloud to desktop, and cloud to cloud transfer. We especially need portability when people shift cloud platforms. We should avoid vendor lock-in that precludes data exchange (Burton, 2010). This means there needs to be recognized procedures for file structure and metadata (Ganger, 2010). The creation of cloud import and export tools would help to expedite the portability of information across platforms.

Improve Transparency of Cloud Performance

Taxpayers are understandably nervous about security, privacy, and performance with cloud applications. They worry whether confidential information stored by federal agencies on everything from taxes and health care to retirement pensions will be protected. Many do not understand cloud computing and are concerned that the metaphor of a wispy and ever-moving cloud will not protect their private information.

In this situation, public officials need to bend over backwards to assure skeptical citizens regarding the reliability of cloud storage (Combs, 2010). We need effective service level agreements that make clear what the performance expectations are and whether providers meet those expectations. Data on uptime, downtime, recover time, archiving, and maintenance schedules would help build public trust in the cloud, as would information on what providers are doing to safeguard security standards.

For example, when the General Services Administration moved its portal site USA.gov to the cloud, officials found that it "was able to reduce site upgrade time from nine months to one day; monthly downtime improved from two hours to 99.9% availability; and GSA realized savings of $1.7M in hosting services," (McClure, 2010). Indeed, most commercial providers commit to 99.9 percent availability in their service level agreements. Having this type of information about computing performance reassures taxpayers and helps legislators understand the advantages of cloud computing.

The Center for Technology Innovation
The Brookings Institution
1775 Massachusetts Ave., NW
Washington, DC 20036
Tel: 202.797.6090
Fax: 202.797.6144
http://www.brookings.edu/techinnovation

Editor
Christine Jacobs

Production & Layout
John S Seo

Tell us what you think of this *Issues in Technology Innovation*.

E-mail your comments to techinnovation@brookings.edu

References

Note: I would like to thank Jenny Lu for providing research, writing, and editing assistance on this project.

Alford, Ted and Gwen Morton, "The Economics of Cloud Computing: Addressing the Benefits of Infrastructure in the Cloud," Booz, Allen, and Hamilton, 2009.

Amoroso, Ed, Cyber Security, Silicon Press, 2006.

Benioff, Marc., Behind the Cloud, Jossey-Bass, 2009.

Bradshaw, Mike, "Cloud Computing: Benefits and Risks of Moving Federal IT into the Cloud," statement at hearing of House Committee on Oversight and Government Reform, Subcommittee on Government Management, Organizations, and Procurement, Washington, D.C., July 1, 2010.

Burton, Daniel, Mike, "Cloud Computing: Benefits and Risks of Moving Federal IT into the Cloud," statement at hearing of House Committee on Oversight and Government Reform, Subcommittee on Government Management, Organizations, and Procurement, Washington, D.C., July 1, 2010.

Charney, Scott, "Cloud Computing: Benefits and Risks of Moving Federal IT into the Cloud," statement at hearing of House Committee on Oversight and Government Reform, Subcommittee on Government Management, Organizations, and Procurement, Washington, D.C., July 1, 2010.

Combs, Nicklous, "Cloud Computing: Benefits and Risks of Moving Federal IT into the Cloud," statement at hearing of House Committee on Oversight and Government Reform, Subcommittee on Government Management, Organizations, and Procurement, Washington, D.C., July 1, 2010.

Federal Communications Commission, Connecting America: The National Broadband Plan, Washington, D.C., 2010.

Furlani, Cita, "Cloud Computing: Benefits and Risks of Moving Federal IT into the Cloud," statement at hearing of House Committee on Oversight and Government Reform, Subcommittee on Government Management, Organizations, and Procurement, Washington, D.C., July 1, 2010.

Ganger, Gregory, "Cloud Computing: Benefits and Risks of Moving Federal IT into the Cloud," statement at hearing of House Committee on Oversight and Government

Reform, Subcommittee on Government Management, Organizations, and Procurement, Washington, D.C., July 1, 2010.

General Services Administration, "Statement of Objectives for Enterprise E-Mail and Collaboration Services," Washington, D.C., June, 2010.

Goodrich, Michael, "GSA Presentation on the Federal Cloud Computing Initiative," 2010.

Hart, Kim, "Google Goes to Washington, Gearing Up to put Its Stamp on Government," Washington Post, September 29, 2008.

Helft, Miguel, "Technology Coalition Seeks Stronger Privacy Laws," New York Times, March 30, 2010.

Hoover, J. Nicholas, "GSA Shifts Cloud Computing Strategy," Information Week, March 1, 2010.

Kundra, Vivek, "Cloud Computing: Benefits and Risks of Moving Federal IT into the Cloud," statement at hearing of House Committee on Oversight and Government Reform, Subcommittee on Government Management, Organizations, and Procurement, Washington, D.C., July 1, 2010.

Kundra, Vivek, "State of Public Sector Cloud Computing," Washington, D.C.: CIO Council, May 20, 2010.

Lewin, Katie, "Federal Cloud Computing Initiative Overview," June 18, 2009.

McClure, David, "Cloud Computing: Benefits and Risks of Moving Federal IT into the Cloud," statement at hearing of House Committee on Oversight and Government Reform, Subcommittee on Government Management, Organizations, and Procurement, Washington, D.C., July 1, 2010.

McCullagh, Declan, "Tech Coalition Pushes Rewrite of Online Privacy Law," CNET News, March 29, 2010.

Mell, Peter and Tim Grance, "NIST Definition of Cloud Computing v15," National Institute of Standards and Technology, October 7, 2009.

Office of Management and Budget, "Federal Data Center Consolidation Initiative," Washington, D.C.: CIO Council, February, 2010.

Romm, Tony, "GOP Hypes Skype for Congress's Computers," Politico, July 1, 2010, p. 13.

Thibodeau, Patrick, "Microsoft Seeks Legal Protections for Data Stored in Cloud," CompterWorld, January 20, 2010.

West, Darrell, "Saving Money Through Cloud Computing," Washington, D.C.: Brookings Institution, 2010.

West, Darrell, "State and Federal Electronic Government in the United States," Washington, D.C.: Brookings Institution, 2008.

Wilshusen, Gregory, "Governmentwide Guidance Needed to Assist Agencies in Implementing Cloud Computing," statement at hearing of House Committee on Oversight and Government Reform, Subcommittee on Government Management, Organizations, and Procurement, Washington, D.C., July 1, 2010.

World Economic Forum, "Exploring the Future of Cloud Computing," Geneva, Switzerland, 2010.

Wyld, David, "Moving to the Cloud: An Introduction to Cloud Computing in Government," IBM Center for the Business of Government E-Government Series, 2009.