Issues in TECHNOLOGY Innovation

Number 3 October 2010

Privacy and Security in Cloud Computing

Allan A. Friedman and Darrell M. West

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.

EXECUTIVE SUMMARY

© Jupiter Images

Cloud computing can mean different things to different people, and obviously the privacy and security concerns will differ between a consumer using a public cloud application, a medium-sized enterprise using a customized suite of business applications on a cloud platform, and a government agency with a private cloud for internal database sharing (Whitten, 2010). The shift of each category of user to cloud systems brings a different package of benefits and risks.

What remains constant, though, is the tangible and intangible value that the user seeks to protect. For an individual, the value at risk can range from loss of civil liberties to the contents of bank accounts. For a business, the value runs from core trade secrets to continuity of business operations and public reputation. Much of this is hard to estimate and translate into standard metrics of value (Lev, 2003) The task in this transition is to compare the opportunities of cloud adoption with the risks. The benefits of cloud have been discussed elsewhere, to the individual to the enterprise, and to the government (West, 2010a, 2010b).

This document explores how to think about privacy and security on the cloud. It is not intended to be a catalog of cloud threats (see ENISA (2009) for an example of rigorous exploration of the risks of cloud adoption to specific groups). We frame the set of concerns for the cloud and highlight what is new and what is not. We analyze a set of policy issues that represent systematic concerns deserving the attention of policy-makers. We argue that the weak link in security generally is the human factor and surrounding institutions and incentives matter more than the platform itself. As long as we learn the lessons of past breakdowns, cloud computing has the potential to generate innovation without sacrificing privacy and

security (Amoroso, 2006; Benioff, 2009).

Defining Security in the Cloud

Allan A. Friedman is research director of the Center for Technology Innovation at Brookings. He is also a fellow in Governance Studies.

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.

If we wish to enable cloud-driven growth and innovation through security, we must have a clear framing on what is meant by security. Security has been notoriously hard to define in the general case (Avizienis et al, 2003). The canonical goals of information security are Confidentiality, Integrity, and Availability. We borrow from NIST to include Accountability and Assurance, and then add a sixth category of Resilience. We define these terms below and map them to the cloud context, with a few examples of how they can be supported by both technical and non-technical mechanisms.

Confidentiality refers to keeping data private. Privacy is of tantamount importance as data leaves the borders of the organization. Not only must internal secrets and sensitive personal data be safeguarded, but metadata and transactional data can also leak important details about firms or individuals. Confidentiality is supported by, among other things, technical tools such as encryption and access control, as well as legal protections.

Integrity is a degree confidence that the data in the cloud is what is supposed to be there, and is protected against accidental or intentional alteration without authorization. It also extends to the hurdles of synchronizing multiple databases. Integrity is supported by well audited code, well-designed distributed systems, and robust access control mechanisms.

Availability means being able to use the system as anticipated. Cloud technologies can increase availability through widespread internet-enabled access, but the client is dependent on the timely and robust provision of resources. Availability is supported by capacity building and good architecture by the provider, as well as well-defined contracts and terms of agreement.

Accountability maps actions in the system to responsible parties. Inside the cloud, actions must be traced uniquely back to an entity, allowing for integration into organizational processes, conflict resolution and deterrence of bad behavior. Accountability is supported by robust identity, authentication and access control, as well as the ability to log transactions and then, critically, audit these logs.

Assurance refers to the need for a system to behave as expected. In the cloud context, it is important that the cloud provider provides what the client has specified. This is not simply a matter of the software and hardware behaving as the client expects but that the needs of the organization are understood, and that these needs are accurately translated into information architecture requirements, which are then faithfully implemented in the cloud system. Assurance is supported by a trusted computing architecture in the cloud, and a by careful processes mapping from business case to technical details to legal agreements.

Resilience in a system allows it to cope with security threats, rather than failing critically. Cloud technology can increase resilience, with a broader base, backup data

and systems, and the potential identify threats and dynamically counteract. However, by shifting critical systems and functions to an outside party, organizations can aggravate resilience by introducing a single point of failure. Resilience is supported by redundancy, diversification and real-time forensic capacity.

Threat Vectors – What to Worry About

How does the landscape of threats to security and privacy change as organizations shift to cloud-based systems, storage and applications? New vectors are introduced, and old ones can be exploited in new ways. Below we briefly discuss some of the threats, highlighting what is genuinely different and new in a world of cloud hosting, what threats are similar to the dominant model of local applications and in-house IT management but will manifest in different ways.

If data are kept in the cloud, for example, then a lost or stolen laptop is much less likely to put sensitive information at risk.

Before categorizing new threats, it is important to acknowledge that the structure of many cloud architectures can mitigate or negate some current security threats. If data are kept in the cloud, for example, then a lost or stolen laptop is much less likely to put sensitive information at risk. Standardized interfaces could make security management easier (ENISA, 2009), while the scale of a provider hosting many parties can generate more information for better threat monitoring. Centralized security management and monitoring can be more effective than local efforts by IT professionals with limited security experience.

Still, moving critical systems and data to a network-accessible framework introduces new classes of vulnerabilities in and of itself, by creating new surfaces to attack and new interfaces to exploit. When those network resources are built on systems, platforms and applications shared with others, another set of threat vectors is introduced. The control mechanism itself can be attacked, breaking down isolation between users, potentially allowing another user to access data or resources. Even without direct access, a providers' other clients can learn valuable transaction data about an organization (Ristenpart et al, 2009). The shared architecture also puts a cloud user at risk from other cloud users if their bad behavior draws attention from either law enforcement or media, leading to hardware seizure or bad publicity (Molnar and Schechter, 2010).

Some threat vectors are not new to cloud, but have somewhat different dynamics. In a classic IT architecture, PCs inside the organization may be at risk of compromise through a host of attack vectors exploiting local applications such as browsers or document viewers. If less data is stored locally, less is immediately at risk, but now the attacker could compromise credentials to gain access to the user's cloud privileges. A compromise to an entire Gmail database probably began with a compromised PC (Zetter, 2010). Similarly, in an attack on the Twitter management team in 2009, a compromised email password lead to exposure of a wide range of other important documents in other cloud infrastructures (Lowensohn and McCarthy, 2009). Shared authentication tokens can lead to brittle defenses.

Organizations must be careful to safeguard data as they move it around their

organization, even without the benefit of cloud computing. When they no longer need data, it must be properly deleted, or else risk leaking sensitive data to the outside (Garfinkel and Shelat, 2003). When relying on a cloud service to handle data, appropriate care must be made to arrange for appropriate security management practices, such as encryption and appropriate deletion.

Similarly, all organizations are vulnerable to an insider attack from a trusted insider, but moving things to the cloud can raise the costs of misplaced trust. A cloud system with a well-thought out identity interface and a clear access control system can restrict access and foster accountability. However, a unified data system with more people accessing more different types of data through more applications can actually make it harder to appropriately limit access and detect misuse (Sinclair and Smith, 2008).

Trends – What Might Get Better Over Time

Cloud technologies are clearly still evolving, and it is important to avoid setting policies today in reaction to an immature market. Based on observations from diffusion and maturation of other technologies, we might anticipate some threats diminishing naturally over time. Both market evolution and a growth of experience will settle some of the issues discussed above.

Economics drives much of our reaction to security and privacy threats (Anderson and Moore, 2006). If demand grows, firms will at least pay more attention to customer concerns about security. Many security mechanisms, such as encryption, network auditing tools, isolation architectures and even hired expertise have a high fixed cost, but add little marginal cost to each client. Once investment has been made, costs can be recouped across all clients without one bearing the complete cost, even if the features were initially demanded by only a subset of the client base.

Experience will also help. On the technical level, as tools and administrator skills mature, threats to availability through under-provision or bad scalability should decrease. Back-end fraud detection will improve with more data, preventing unauthorized access while reducing false positives. The risk of losing access and data from a law enforcement investigation should diminish as both the firm and the agency develop more efficient mechanisms for law enforcement compliance (Molnar and Schechter, 2010). Experience will also help the user and the provider develop a more symbiotic relationship, as each gets acclimated to what might be expected of the other.

Structural Problems That Won't Go Away on Their Own

Many security and privacy threats, such as malware or the risk of a malicious insider, appear to be omnipresent aspects the information technology landscape today, and must be addressed as part of a larger national and international cybersecurity agenda.

Beyond this background cyber-threat cloud services, however, still pose several structural and institutional problems. These will require communication and collaboration between the involved players, and possibly government involvement.

In turning over control of some aspects of their information systems to a cloud provider, cloud users face what economists call a "principal agent" problem. When a principal hires an agent, that person cannot be certain that the agent is acting completely in the principal's best interest, particularly where the two interests (such as profits) diverge. This is a problem of information asymmetry. How does the client know what the provider is doing? This is further complicated by the fact that security is not an absolute property, and that metrics to compare the relative attributes of different systems and approaches has proven quite difficult (Bellovin, 2006).

Privacy advocates point out that electronic communications currently have stronger safeguards if stored on local than remote file servers, dating from earlier distinctions between personal and public information.

A provider cannot offer an absolute guarantee against a bad outcome, so it must convince the client that it has taken adequate but economically sensible precautions. This trust must also be extended to third parties contracted by the provider, over which the original client has even less control, and little to no information. However, a study of the Terms and Conditions offered by cloud providers found that they frequently disclaim any responsibility for the security of the data (Bradshaw, Millard and Walden, 2010). Responsibility for security lies with the user, even in instances where the user cannot be expected to take any constructive or defensive action. Instead, users must rely on the best efforts of the provider, without necessarily having adequate information about what these precautions comprise. This information asymmetry is even more important in consumer-level applications, where users may have even less awareness of the limited responsibility of the provider, and have less information about the risks.

The principal agent problem is evident in other areas as well. A client may have privacy preferences, for example, for the provider to challenge law enforcement demands for data, and insist upon challenging these demands to the full extent of the law. The provider, on the other hand, may have an interest in developing a long-term positive relationship with law enforcement agencies. This might be even more problematic when dealing with a foreign government (Goodman, 2005).

The legal front presents several other concerns for cloud privacy. Many have commented on the challenge of keeping law current with information technology, and how citizens use that technology. Privacy advocates point out that electronic communications currently have stronger safeguards if stored on local than remote file servers, dating from earlier distinctions between personal and public information. Through cloud technologies, individuals and organizations safeguard more private information on third-party systems, but see these systems as extensions of their own computational environment. A number of court cases in recent years have seen 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 some judges, that puts privacy on cloud platforms on a lower level than that associated with desktop, laptop, or mobile devices (Oza, 2008). This affords much less protection, allowing law enforcement access to information without 4th Amendment warrant requirements, and creates uncertainty the power of the U.S. government over cloud data.

Uncertainty also exists about the power of other sovereign powers. The decentralized nature of cloud architecture might create a useful fiction that data's location is irrelevant to the platform, but that data does exist in the very real space of bits on a platter spinning in a server located under *someone's* jurisdiction. What that state might see as an opportunity for law enforcement or public safety intervention could very well be viewed as a flagrant violation by the data owner, used to operating under a different set of laws.

Some nations are becoming increasingly protective in their treatment of cloud computing. In the name of national security, they only want to store data within their own national borders and take the view that the only system they trust is one operated within their own jurisdictions (Blumenthal, 2010). Inside the United States, some jurisdictions have put restrictions in place. Cloud agreements negotiated in some cities have included a promise to store government cloud data within the continental U.S. Government officials justified this on security grounds, but it limits the efficiency of cloud computing systems.

Europeans have a data protection directive that precludes data transfers from the European Union to countries with privacy and confidentiality rules it views as inadequate (World Economic Forum, 2010). Since this includes places such as the U.S., this limits the ability of American cloud providers to build cross-national networks and take advantage of the economies of scale that are a strong feature of cloud computing.

While an evolving and competitive marketplace should drive better security, it also presents several concerns for safeguarding data. As some companies win and others lose in the market place, a client may find its provider shuttered. Absent the ability to extract one's data, the losses could be enormous. Moreover, it is critical that a bankrupt firm not see its clients' data as an asset to be sold.

The ability to extract ones data is also critical for enabling competition in the cloud by ensuring that customers and users are not locked in or captured by a single vendor. Lock-in can leave the client vulnerable to increased prices and reduced features or service. Moreover, reducing the risk of lock-in through data portability can serve to enhance competition based on quality and features (Armbrust et al, 2009), which could in turn drive security as a market differentiator.

Predictions about the shape of any market is a risky business. If early adopters do not highlight security as a key feature needed from providers, it will not be a priority for investment. Security must often be balanced against other desirable attributes such as speed, usability, information sharing, and, of course, cost. Google encrypted its cloud mail service Gmail login process, but did not publicly offer the option encryption of mail sent to the user's browser until 2008 (Rideout, 2008). A year later, a

team of security experts complained this option was far from obvious to the layman, and it should be on by default (Singel, 2009). Google reached the conclusion that the latency costs of encryption were outweighed by security concerns to set encryption as the default in early 2010 (Schillace, 2010).

Finally, data aggregation poses its own privacy risks. Among the benefits of a cloud architecture are the collection and aggregation of data from disparate sources. Once collected for some primary use, such as portability of electronic health records, or shared access to government databases, it will be tempting to exploit this collected information in new ways. This can be incredibly powerful tool, but brings a host of privacy concerns about how to use data without violating privacy.

One of the virtues of the cloud is its potential for real-time performance data and on-demand transparency.

A recent Institute of Medicine report on privacy and research found that the current regulations hinder research without protecting privacy (IOM, 2009). To enable research, the report calls for the linking of data from multiple sources. Paul Ohm (2010) observes, however, that is this very linkage that poses the largest threat to individual privacy by enabling re-identification across contexts.

Inside the government, aggregating information across different databases and between agencies allows government administrators to operate more efficiently, and make more informed decisions. However, it is critical to understand who should have access to what to comply with privacy legislation.

Recommendations

Transparency A key to improving consumer confidence in cloud privacy and security is transparency and disclosure. Providers need to improve disclosure of privacy notices and business practices so that users know what is being offered. Prospective clients and users should be able to understand the security precautions take by a given provider, and have enough information to make an informed choice between two alternatives about their risk exposure. Even sharing how a cloud provider recruits its employees that administer key systems would be useful information.

Absent any formal liability for security incidents, current and potential clients need to have as much information about risks of cloud services use as possible. One of the virtues of the cloud is its potential for real-time performance data and on-demand transparency. For example, companies can offer real-time information on cloud down-time and data breaches. There is also some limited evidence that public disclosures of data breaches lead to a financial penalty in the form of reduced stock prices (Acquisti, Friedman, and Telang, 2006) that, in turn, might lead to risk mitigation. On-demand transparency gives consumers instantaneous information. This is an advantage that was not available in the era of paper-based records or some types of desktop computing.

Competition Beyond transparency, the greatest promise for a more secure set of cloud infrastructures is a competitive marketplace. A diverse enough pool of market actors will allow security to be a credible path to differentiating service. This will engender a positive feedback loop, where firms will market themselves, and even the

least secure provider will have to raise their level of security. Moreover, a larger number of platforms and systems will increase the number of potential targets for attackers, preventing malware specialization and reducing systematic social risk (Geer et al, 2003). However, providers must be large enough to leverage the economies of scale discussed above, including security investment, information sharing, and usable interfaces.

One key mechanism in this equation is exportability of data and code. Exportability would reduce switching costs, enabling clients to shift to more secure providers. The marketplace can be further tended by rewarding smaller or newer players with government contracts, or at very least guaranteeing open forums for industry collaboration and standard setting. A diverse marketplace allows natural selection to reward successful market participants with greater market share. This selection can be artificially guided through blunt instruments such as liability, or more subtle mechanisms such as federal guidelines or security certifications.

Legal Clarifications This approach to cloud privacy should be clarified because it is not clear that consumers have a clear sense of which platforms they are using and how privacy protections vary across domains. During the course of a day, people shift quickly from cloud to desktop to flash drives without thought to how confidentiality rules differ. When they shift from a desktop to the cloud, most consumers are unaware that their privacy rights drop precipitously. Ideally, congress should act to require a "probable cause" search warrant that is approved by a judge. This would provide greater safeguards for online content, pictures, geolocation data and emails. Such legislation is supported by a broad coalition of cloud providers, technology firms and advocacy groups from across the political spectrum (Helft, 2010).

In addition to updated privacy protections, the law must also reflect how cloud-based data and systems will become a new target for online criminals. The Computer Fraud and Abuse Act of 1986 should be updated to clarify its definition of presumed losses through cloud computing. The law 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.

Stakeholder Engagement

Strong privacy and security protections should be important to all parties, but some

effort will be necessary to identify mutually beneficial paths towards mitigation of threats in the cloud. The technical costs may not be the stumbling block, since building them in early and raising demand for a baseline of protection could apply across the industry. Harder to internalize are the changes that must happen outside of the cloud industry itself and in the larger community of cloud computing stakeholders: consumers, firms, investors, regulators and lawmakers.

Users and cloud providers will have to mutually discover the willingness to pay for security features and privacy protection, particularly as they trade off against other attributes. Moreover, the providers and users will have to work together to establish mechanisms to promote trust, as well as make the business case for security investment. Currently, the onus seems to be on the client to seek answers to a host of security and privacy-related questions from service providers (Hathaway, 2010). We cannot take for granted that answers are readily available, let alone consistent with an organization's or individual's approach to risk.

There is reason to be optimistic about the gains to be had from a transition of many information services to a cloud architecture.

The lack of liability claims stronger than "best effort" make it difficult to build in a security model that maps to a mature risk posture. Other options include standardized and reliable auditing reports, compliance certifications and best practices. These should be developed with as wide a set of stakeholders as possible, with particular attention to privacy advocates.

The users of cloud services must also work together to further promote interoperability. Governments should make efforts to develop cross-border agreements on cloud computing. If nations can reach agreement on basic privacy, security, and access control rules, it would pave the wave for cloud networks and data-sharing on an international scale. This is not a trivial task, but by starting small and focused on particular areas of compromise, progress could be made towards a broader domain of sharing that would head off a cloud-balkanization. Absent national legislation, states could work through standards bodies to build sharing frameworks that comply with diverse data demands while still allowing some of the benefits of cloud portability and distributed access.

Conclusion

There is reason to be optimistic about the gains to be had from a transition of many information services to a cloud architecture. Cloud computing makes possible cost savings, scalability, and more efficient use of IT resources, among other things. However, the risks to privacy and security from cloud computing cannot be ignored. Not all these risks are new, and some of them can be mitigated through technology investment and due diligence from the client. But others are systematic in nature, and may not be solvable through unilateral innovation.

Uncertainty dominates the client's ability to forecast risk and the data subject's expectation of privacy. Transparency would support selection towards a more security-conscious cloud universe, and market competition can enable that shift. While some uncertainty will always be present in a world of network threats, clarified

regulations and cooperation among the relevant stakeholders can put these platforms on an assured footing moving forward.

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

Acquisti, Alessandro, Allan Friedman and Rahul Teland. "Is There a Cost to Privacy Breaches? An Event Study," International Conference of Information Systems (ICIS), 2006.

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

Anderson, Ross and Tyler Moore, "The Economics of Information Security," Science 314. October 27, 2006.

Armbrust, Michael, Armando Fox, Rean Grif fith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia. "Above the Clouds: A Berkeley View of Cloud Computing" Technical Report EECS-2009-28, EECS Department, University of California, Berkeley. 2009.

Avizienis, Algirdas, Jean-Claude Laprie, Brian Randell, and Carl Landwehr. "Basic concepts and taxonomy of dependable and secure computing" IEEE Transactions on Dependable and Secure Computing 1:1, 2004

Bellovin, Steve. "On the Brittleness of Software, and the Infeasability of Security Metrics" IEEE Security and Privacy 4:4. July 2006.

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

Blumenthal, Marjory, "Is Security Lost in the Clouds?", Telecommunications Policy Research Conference, Oct 2, 2010.

Bradshaw, Simon, Millard, Christopher and Walden, Ian, Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. Queen Mary School of Law Legal Studies Research Paper No. 63/2010. Available at SSRN: http://ssrn.com/abstract=1662374

Economist "Selling people's secrets," The Economist (blog) July 13, 2010. http://www.economist.com/blogs/babbage/2010/07/privacy_protection

European Network and Information Security Agency (ENISA), "Cloud Computing: Benefits, Risks and Recommendations for Information Security," Report. November, 2009.

Garfinkel, S. and Shelat, A., "Remembrance of Data Passed: A Study of Disk Sanitization Practices," IEEE Security and Privacy, January/February 2003.

Geer, Dan. Charles Pfleeger, Bruce Schneier, John Quarterman, Perry Metzger, Rebecca Bace, Peter Gutmann,"Cyberinsecurity: The Cost of Monopoly—How the Dominance of Microsoft's Products Poses a Risk to Security," Computer and Communications Industry Association, September 24, 2003

Goodman, Peter. "Yahoo Says It Gave China Internet Data" Washington Post, September 11, 2005.

Hathaway, Melissa. "Beyond Availability: Melissa Hathaway on the Cloud." GovInfoSecurity.com, June 10, 2010.

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

Institute of Medicine (IOM), "Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research," Report. February, 2009.

Lev, Baruch. "Remarks on the Measurement, Valuation, and Reporting of Intangible Assetts." FRBNY Economic Policy Review, September 2003.

Lowensohn, Josh and Caroline McCarthy. "Lessons from Twitter's Security Breach," CNet, July 15, 2009.

Molnar, David and Stuart Schechter, "Self Hosting vs. Cloud Hosting: Accounting for the Security Impact of Hosting in the Cloud," Workshop on the Economics of Information Security, 2010.

Ohm, Paul. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, UCLA Law Review 57:6, 2010

Oza, Achal, Amend the ECPA: Fourth Amendment Protection Erodes as E-Mails Get Dusty. Boston University Law Review, Vol. 88, No. 4, 2008. Available at SSRN: http://ssrn.com/abstract=1288344

Rideout, Ariel. "Making Security Easier." Gmail Blog. July 24, 2008. http://gmailblog.blogspot.com/2008/07/making-security-easier.html

Ristenpart, T., Tromer, E., Shacham, H., and Savage, S. 2009. "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds." In *Proceedings of the 16th ACM Conference on Computer and Communications Security*

Sinclair, Sara, and Sean W. Smith. “Preventative Directions for Insider Threat Mitigation Using Access Control.” Chapter 11 of Salvatore Stolfo, Steven M. Bellovin, Shlomo Hershkop, Angelos D. Keromytis, Sara Sinclair, and Sean W. Smith, eds. Insider Attack and Cyber Security: Beyond the Hacker. Springer, April 2008.

Schillace, Sam. “Default https acces for Gmail.” Gmail Blog. January 12, 2010. http://gmailblog.blogspot.com/2010/01/default-https-access-for-gmail.html

Singel, Ryan. "Encrypt the Cloud, Security Luminaries Tell Google." Wired Threat Level, June 19, 2009. http://www.wired.com/threatlevel/2009/06/google_ssl/

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

West, Darrell, “Steps to Improve Cloud Computing in the Public Sector”,” Washington, D.C.: Brookings Institution, 2010b.

Whitten, Alma, “Consumer Online Privacy,” statement at hearing of Senate Committee on Commerce, Science, and Transportation, Washington, D.C., July 27, 2010.

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

Zetter, Kim. “Google Hackers targeted source code of more than 20 companies.” Wired Threat Level. January 13, 2010.