



Privacy Recommendations for the Use of Cloud Computing by Federal Departments and Agencies

**Privacy Committee
Web 2.0/Cloud Computing Subcommittee**

August 2010

Introduction

Good privacy practices are a key component of agency governance and accountability. One of the Federal government's key business imperatives today is to maintain the privacy of personally identifiable information (PII) we collect and hold. The Office of Management and Budget (OMB) Memorandum 07-16¹ defines PII as "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

As business systems and processes become more complex and sophisticated, agencies are collecting an increasing amount of data, including more PII. As a result, agencies are struggling to keep pace with their needs for storage in a manner that minimizes costs. Cloud computing presents a possible solution. Cloud computing is internet-based computing whereby shared resources, software, and information are provided to computers and other devices. While this provides a flexible solution for complex information technology needs, cloud computing poses additional privacy challenges to those using the "cloud." Federal agencies need to be aware of the significant privacy concerns associated with the cloud computing environment where PII will be stored on a server that is not owned or controlled by the Federal government. That solution may result in holding or processing data without complying with Federal privacy requirements in a multi-jurisdictional environment. The framework below provides guidance on the privacy considerations posed by moving computer systems that contain PII to a Cloud Computing Provider (CCP). Agencies should also consult their own legal counsel and privacy offices to obtain advice and guidance on particular laws and regulations governing their own information systems containing personal information.

The purpose of this paper, and of privacy interests in general, is not to discourage agencies from using cloud computing; indeed a thoughtfully considered cloud computing solution can enhance privacy and security. Instead, the purpose is to ensure that Federal agencies recognize and consider the privacy rights of individuals, and that agencies identify and address the potential risks when using cloud computing.

Summary of the Privacy Risks Posed by Some Cloud Computing Platforms

The need to maintain the rights established by the Privacy Act of 1974² and the E-Government Act of 2002, including clearly defined uses for the information Federal agencies collect, rules governing retention , agreements controlling internal and external sharing and disclosure, and procedures governing notice, access, redress, and security.

¹ Available at: <http://www.whitehouse.gov/omb/assets/omb/memoranda/fy2007/m07-16.pdf>

² 5 U.S.C. § 552a. The Act applies to agency systems of records about individuals, when such records are retrieved by the individual's name or identifying number, symbol, or other identifying particular assigned to the individual. The Act applies no matter where the agency maintains such records.

Once an agency chooses a CCP to collect and store information, the individual is no longer providing information solely to the government, but also to a third party who is not necessarily bound by the same laws and regulations. The government and CCP must agree to strictly adhere to the Privacy Act to ensure the protection and safety of the information.

Risks Include:

- The permitted use for the information the CCP collected from the Federal agency may not be clearly defined in the Terms of Service/Contract, enabling the CCP to analyze or search the data for its own purposes or to sell to third parties.
- The data could become an asset in bankruptcy, particularly if the Terms of Service or contract do not include retention limits.
- Depending on the location of the CCP's servers or data centers, the CCP might allow or be required to permit certain local or foreign law enforcement authorities to search its data pursuant to a court order, subpoena, or informal request that would not meet the standards of the Privacy Act of 1974.
- The individual providing the information has no notice that explains that his or her information is being stored on a server not owned or controlled by the U.S. Government. Thus, when the individual person attempts to access his or her data, he or she is unable to do so and is left without proper redress.
- The data stored by the CCP is breached and the CCP does not inform the government or any of the individuals affected by the incident.
- The CCP improperly implements Federal security requirements (i.e., finds them cost-prohibitive or cumbersome) and thus inadvertently allows the data it is storing in the cloud to be viewed by unauthorized viewers.
- The CCP fails to keep access records that allow agencies to conduct audits to determine who has accessed the data.
- The Federal government cannot access the data to perform necessary audits. The data has been moved to a different country and a different server and the government suffers a loss in reputation and trust.
- The Federal government fails to keep an up-to-date copy of its data. The CCP accidentally loses all of the government's data and does not have a back up.

Certain privacy laws may affect the ability of some Federal organizations considering wishing to use CCPs.

Some types of information may trigger procedural or substantive barriers that prevent or limit the disclosure of some records to third parties, including CCPs. The Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191) (HIPAA) and its implementing regulations, for example, may require a formal agreement before any sharing of records with a CCP is lawful. Other laws may similarly limit or prevent such arrangements. In addition, records management and disposal laws may limit the ability of a government agency to use CCPs for official records.

Where the information is stored and processed may have significant effects on the privacy and confidentiality protections of information that apply.

Organizations need to consider the laws and policies of the country where the data processing machines are located. For example, a CCP may without notice to the organization, move the organization's information from one jurisdiction to another, from provider to provider, or from machine to machine thus creating different legal problems. Personal information that ends up maintained by a CCP in a European Union (EU) Member State could be subject to domestic privacy laws that must follow specific EU standards. It may not be clear how the privacy laws and protections apply given these complex relationships.

The privacy and confidentiality risks vary significantly with the terms of service and privacy policy established by the CCP.

Those risks may be magnified when the CCP has reserved the right to change its terms and policies at will. The secondary use of an agency's information by the CCP may violate laws under which the information was collected or are otherwise applicable to the original agency. Enforcement may be difficult due to conflicting laws and policy applications. A CCP will also acquire transactional and relationship information by virtue of its services that may raise privacy concerns. Agencies may not be aware of the specific details in the terms of service or of the consequences of sharing information with a CCP.

Government Clouds versus Private Vendor Clouds

Agencies may contract with CCPs; however, some Federal agencies have begun or are considering supplying cloud computing services. While many of the concerns and recommendations in this paper may be addressed by Federal agency cloud services, it is still incumbent upon the contracting agency to ensure that the agency's contract complies with Federal statutes and policies regardless of the source from where an agency selects its cloud computing services. Federal agencies must follow National Institute of Standards and Technology (NIST) Special Publications 800-53 and 800-60 and various OMB memoranda to protect PII. Private cloud vendors should be aware of these publicly published controls and should offer them as enhancements.

Contracts Favored Over Terms of Service Amendments

Given the potential risks and privacy considerations described in this paper, the question remains as to how Federal agencies should best enforce compliance with the public's privacy rights and other government requirements in this area.

Contracting with CCPs rather than trying to modify CCPs' terms of service agreements may allow agencies greater ability to comply with and audit the privacy concerns outlined in this paper. In cases where cloud computing will include the transmittal and storage of PII, amending a CCP's terms of service may not adequately cover all of the agency's requirements, as they are

not typically written with Federal privacy and security requirements in mind. Privacy and security risks are magnified when the CCP has reserved the right to change its terms and policies at will which is a common provision in some terms of service. If the use of cloud computing does not involve storage or transmittal of PII, terms of service may adequately cover agency concerns.

Appropriate contract language can help ensure that CCPs are transparent about other possible users. Without precautions, there is no way an agency can ensure that CCPs do not use subcontractors or that information is not transferred to other third parties without the knowledge and approval of the contracting agency.³

Privacy Threshold Analysis

Before determining which actions are most appropriate in protecting privacy in the cloud environment, agencies should first conduct an assessment of the data and systems proposed for cloud storage. Section 208 of the E-Government Act of 2002 (*44 U.S.C 3501 note*), and OMB Memorandum 03-22,⁴ define the circumstances under which agencies should conduct a Privacy Impact Assessment (PIA). Many agencies conduct a Privacy Threshold Analysis (PTA) first, to determine whether a PIA is warranted. In general, a thorough threshold analysis should determine whether or not a new system, or a change to a system, creates new privacy risks and whether that system will require a full PIA. Additionally, a properly executed PTA may be incorporated into the Certification & Accreditation (C&A) process and has proven to be an effective tool for analyzing and documenting the potential privacy concerns for systems.

Examples of changes that are possible in the cloud environment, and which should be addressed in a PTA before moving data to a cloud include (as defined by OMB Memorandum 03-22):

- Significant System Management Changes - when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system
- Significant Merging – when agencies adopt or alter business processes so that government databases holding PII are merged, centralized, matched with other databases or otherwise significantly manipulated: For example, when databases are merged to create one central source of information, such a link may aggregate data in ways that create new privacy concerns

³ The Privacy Committee is currently developing contract language that may be promulgated through the Federal Acquisition Regulation, which would address the concerns identified in this section. Should such a regulation issue, we recommend using the language. Many agencies already have such clauses.

⁴ Available at: http://www.whitehouse.gov/omb/memoranda_m03-22/

- New Public Access – when user-authenticating technology (i.e., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public
- New Interagency Uses - when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, both agencies should complete a PIA
- Internal Flow or Collection - when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form
- Alteration in Character of Data - when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information)

After completing the threshold assessment, an agency should conduct a PIA on those systems that require a PIA to better understand and document the specific privacy and security risks involved. For situations in which legacy systems and information were previously exempted from the PIA process, the switch to cloud computing could now trigger the need for a PIA.

If the PIA threshold set forth in the assessment is not met, agencies may still decide to conduct a PIA as a best practice. This process will help ensure that agencies identify privacy risks and always consider the potential disclosure or other statutory requirements (such as the Freedom of Information Act or the Federal Records Act) that may apply when using a CCP.

Privacy Impact Assessments

The PIA process is designed to ensure that Federal agencies comply with applicable privacy laws and regulations governing an individual's privacy and to ensure confidentiality, integrity, and availability of an individual's personal information at every stage of development and operation. Typically, agencies conduct a PIA during the Certification and Accreditation (C&A) process and update it every three years, unless there is a change in the privacy or information security posture. Currently, two CCP vendors are going through the C&A process. Future C&A reviews of cloud providers will be facilitated through the Cloud Computing Security Working Group Program Management Office with participation from the General Services Administration, Department of Homeland Security, and Department of Defense as Authorizing Officials. Typically, PIAs will continue to be the responsibility of the contracting agency.

In addition to the existing PIA requirements, a PIA for cloud computing should assess:

- What information the agency will collect and put into the cloud (e.g., nature and source)

- Why the agency is collecting the information (e.g., to determine eligibility for a benefit or service)
- Intended use of the information (e.g., to verify existing data)
- With whom the agency will share the information (e.g., another agency for a specified programmatic purpose)
- What opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent
- How the agency and CCP will secure information in the cloud (e.g., administrative and technological controls)
- Whether the agency is creating a system of records under the Privacy Act and if so, drafting the mandated notice for publication in the *Federal Register*.
- Where the server on which the data will be stored is physically located⁵

A major benefit to conducting a PIA in association with cloud computing, regardless of whether or not use of the CCP passes the privacy assessment threshold, is that it will ensure that agencies examine the privacy considerations posed by this action. Even if the system in question is covered by an existing PIA, agencies should review the document to be certain that the privacy risks have not changed.

Regardless of the cloud service delivery model (Platform as a Service, Infrastructure as a Service, or Software as a Service) used, each agency will be responsible for completing its own privacy threshold analysis and if warranted, a PIA.

Privacy Act Considerations

The Privacy Act of 1974, as amended, requires that personal information Federal agencies collect is accurate, timely, relevant, and complete. The Privacy Act governs the executive branch and it may also reach non-Federal CCPs if they are considered government contractors and fall under subsection (m) of the Act. “When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function,

⁵ CCPs may not typically disclose where their data centers are physically located. For a general sense of where data centers used for cloud computing are typically located and how they operate, see Tom Vanderbilt, “Data Center Overload,” New York Times Magazine, June 8, 2009 available at <http://www.nytimes.com/2009/06/14/magazine/14search-t.html>.

the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system.”⁶

Agencies will have to address a number of Privacy Act issues before data contained in systems of records are placed onto a server not owned or controlled by the U.S. Government. These requirements include providing accurate notice, rights of access, redress, description of the location of records, choice and consent, data quality and accuracy, collection, use, retention, and disposal.⁷

Agencies must consider the right of individual access to and amendment of records pertaining to the individual and make those known to potential CCPs. In addition, agencies may wish to proactively inform the public that their information is being stored in a cloud environment, which would most likely be done through revision of the appropriate Privacy Act system of records notice⁸.

Contracting agencies must be certain that the routine uses for information under the Privacy Act are identified and apply to disclosure they make to potential CCPs. In cases where agencies will require the information on a timely basis, such as in searching for a fugitive or a missing child, agencies should establish procedures to ensure timely retrieval of the required data.

Location of the data is a key issue, not only in terms of access and retrieval under the Privacy Act, but also in consideration of other issues such as application of foreign privacy laws, the requirements of E-Discovery,⁹ and in any Privacy Act statements on forms used to collect information from the individual.

⁶ Privacy Act, as amended, 5 U.S.C. § 552a(m)(1). For guidance concerning this provision, see OMB Guidelines, 40 Fed. Reg. 28,948, 28,951, 28,975-76, (July 9, 1975), available at http://www.whitehouse.gov/omb/assets/omb/inforeg/implementation_guidelines.pdf.

⁷ See 5 U.S.C. § 552a(e)

⁸ The minimum amount of time it takes to publish a SORN is 30 days. If a notice and/or comment period is required, and if multiple layers of agency departmental review are required the publication can be several months.

⁹ Electronic discovery (E-discovery) refers to the process of identifying and producing electronically stored information (ESI) in response to civil and criminal litigation, including metadata and electronic backup materials that may be relevant to that litigation. Once such litigation is reasonably anticipated (e.g., receipt of a letter threatening a lawsuit), a party has a legal obligation to suspend destruction of such ESI, by issuing a “litigation hold” to all individuals and entities maintaining ESI on the party’s behalf. Failure to take proper and adequate steps to preserve such ESI can result in serious legal sanctions against a party. These risks may be significantly greater when using a cloud computing service, since the service provider may be unable or unwilling for technical, cost, legal or other reasons to halt routine destruction of responsive ESI, which may be maintained or commingled with data of other clients of that service for records management and disposal purposes. Likewise, the nature of cloud storage (e.g., widely dispersed servers or databases located domestically or even overseas) may complicate the ability to identify, preserve, and retrieve responsive ESI in a timely fashion, further jeopardizing the agency’s ability to meet its legal e-discovery obligations. With regard to data stored in foreign jurisdictions, see generally The Sedona Conference Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy & e-Discovery – Public Comment Version, available at http://www.thesedonaconference.org/dltForm?did=WG6_Cross_Border.

Federal Information Security and Management Act (FISMA)

FISMA (Title III of the E-Government Act) was enacted in 2002 to "provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets."¹⁰

FISMA requires agencies to identify their major systems, and then assess risk and recommend controls based on the individual system and the information contained within that system. NIST provides standards for these assessments in its Federal Information Processing Standards Publication 199 (FIPS 199). The very first security objective listed in FIPS 199 is confidentiality of information and prevention of unauthorized disclosure of that information.

Agencies report to OMB (at a minimum) annually documenting their compliance with FISMA requirements. This report includes sections on both the privacy and security of the major systems.

Agencies need to consider if a CCP is in compliance with FISMA requirements, especially if agencies plan to collect and store information categorized at a "moderate"¹¹ level at a CCP facility. Moderate level information includes PII and agencies need to work with CCPs to address issues of access control, what type of privacy and security training will be provided to those granted access, and a background investigation for those individuals who are given access to personal information the Federal government has collected.

Agencies must consider incident reporting obligations imposed by FISMA and related Federal policy, which would apply in the event that data maintained by the agency on the cloud are compromised. Currently, Federal agencies must report certain information security incidents, to the U.S. Computer Emergency Readiness Team (US-CERT) at the Department of Homeland Security. OMB Memorandum M-06-19 requires agencies to report all incidents involving personally identifiable information to US-CERT within one hour of discovering the incident. Agencies must either have or adopt adequate and appropriate controls (including contractual, see attached) to ensure that CCPs detect and provide notice of incidents to the agency in a timely manner. These controls must also address other incident-related issues, including the cost and responsibility for containing or mitigating harm and for notifying affected individuals where required and where applicable identity protection/credit monitoring services.¹²

¹⁰ Federal Information Security and Management Act (44 U.S.C. 3541)

¹¹ Federal Information processing Standards Publication "Standards for Security Categorization of Federal Information and Information Systems – FIPS Pub 199) can be found at <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>

¹² See generally OMB Memorandum 06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments (July 12, 2006), <http://www.whitehouse.gov/OMB/memoranda/fy2006/m06-19.pdf>; OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007), <http://www.whitehouse.gov/omb/assets/omb/memoranda/fy2007/m07-16.pdf>; and NIST Special Publication 800-61,

Health Insurance Portability and Accountability Act (HIPAA)

Agencies that provide healthcare services or otherwise handle protected health information (PHI) should also consider, and make CCPs aware of, the possible HIPAA implications involved. HIPAA rules contain privacy and security requirements which apply to covered entities¹³ as well as business associates of covered entities.

While a business associate is not directly subject to the HIPAA law, an agreement between the business associate and the covered entity essentially makes the business associate subject to the same standards as the covered entity. Covered entities, therefore, must have a business associate agreement with the CCP that complies with HIPAA.

Previously, if a CCP simply acted as a conduit of PHI the business associate requirements did not apply. This relationship has changed, however, under the provisions of the Health Information Technology for Economic and Clinical Health Act (HITECH Act) (Title XIII of the American Recovery and Reinvestment Act of 2009). Also, penalties and enforcement for non-compliance have been increased.

Under these new guidelines agencies and CCPs should assume that a business associate agreement is required if PHI is being transmitted and stored on a cloud.¹⁴

Conclusion and Recommendations

Agencies should include the Senior Agency Official for Privacy (SAOP) or his or her appropriate designees early in the development process to ensure that agencies recognize the privacy rights of individuals and identify and address the potential risks when using cloud computing. . The SAOP or other delegated privacy staff should be part of the board or committee that will evaluate information moving information to the cloud, the proposed service delivery model, the CCP's proposal before a contract award takes place, and all other areas of concern mentioned in this paper. Agencies should weigh the security threats and opportunities that are present for public, private, and community clouds when PII is involved. As with many technological innovations, cloud computing presents challenges and possible rewards for Federal agencies. Cloud computing can be a cost-saving and efficient option for Federal agencies when agencies properly recognize the rights of individuals and identify and address the potential risks.

Computer Security Incident Handling Guide (Jan. 2004), <http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>.

¹³ Covered entities are defined in the HIPAA rules as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which the Department of Health and Human Services has adopted standards.

¹⁴ Refer to the HIPAA Privacy Rule, at 45 CFR Part 160 and Part 164, Subparts A and E.

