



# Open Government *and* Privacy Protections

---

*2010 Office Environmental  
Information Symposium*

---

*Office of Information Collection,  
FOIA & Privacy Branch*

---

*May 11, 2010*

# Agenda

---

- Open Government Memo
- Basic Objectives of the Privacy Act
- Social Networking
- Social Networking Risks
- Cloud Computing
- Electronic Government Act (E-Gov)
- Privacy Act
- Required Privacy Protections
- Cloud Computing Providers (CCPs)
- Cloud Computing Risk
- Contracting with CCPs
- Other Federal Policy Issues
- Considerations





# Open Government Memos



**President Obama** – January 21, 2009

Transparency

Participatory

Collaborative

**Administrator Jackson** – April 23, 2009

Transparency and inclusiveness in decision-making

Conduct business openly and fairly

**Deputy Assistant Administrator (OEI)**

– March 5, 2010

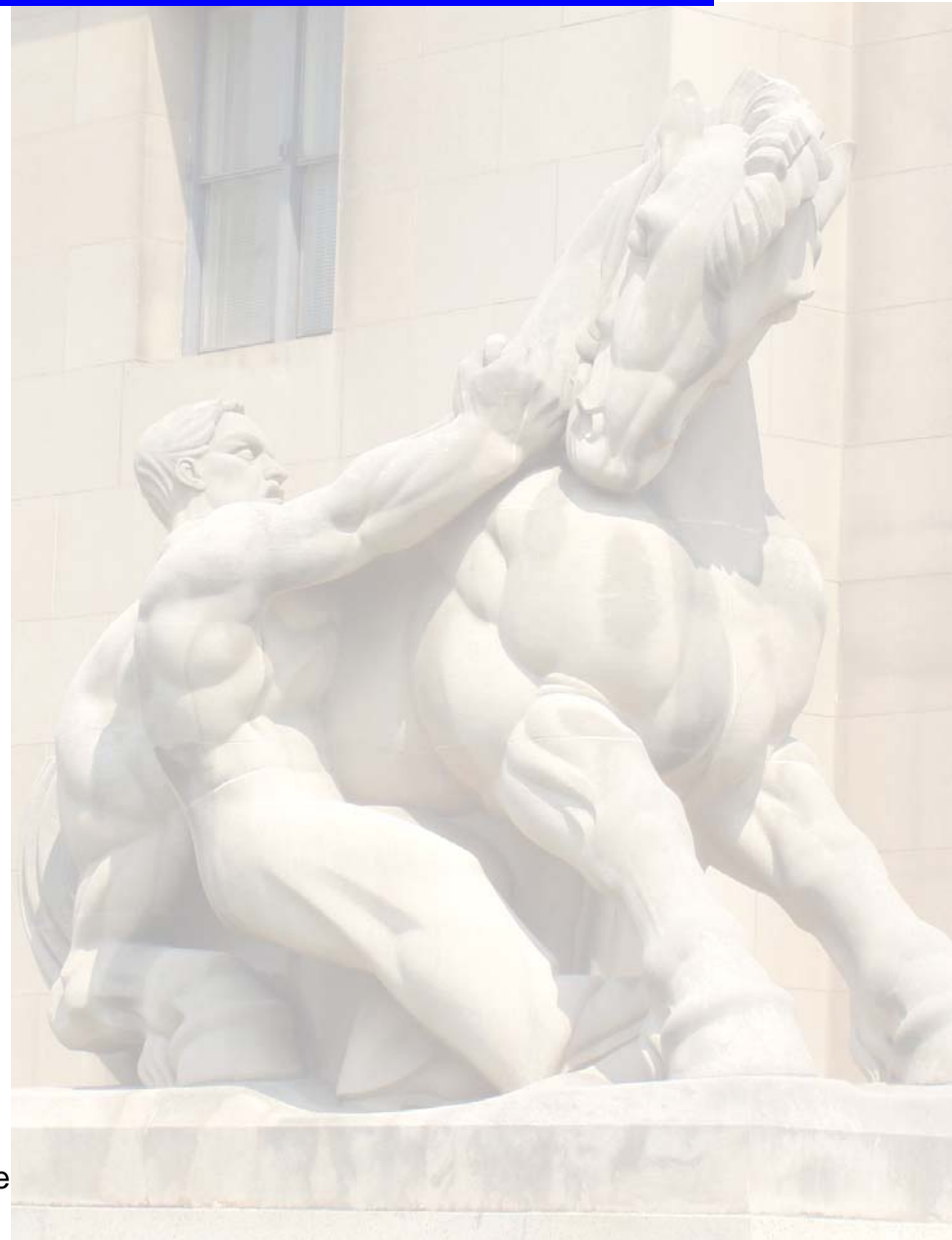
[Agency Implementation](#)

[www.epa.gov/open](http://www.epa.gov/open)

[www.openepa.ideascale.com](http://www.openepa.ideascale.com)

# Basic Objectives of the Privacy Act

- To restrict disclosure of personally identifiable records maintained by executive branch agencies;
- To grant individuals increased rights of access to agency records maintained on themselves;
- To grant individuals the right to seek amendment of agency records that are not accurate, relevant, timely, or complete; and
- To establish a code of “fair information practices” that regulates the collection, use, maintenance and disclosure of PII.





# Social Networking



## Social Networking

- Web-based services for building online communities of people who share same interests or activities;
- Social networks provide a variety of ways for people to interact and share content; and
- Social networks are “invitational” in that users control or limit access to their content.

## Examples of Government Use

- Dissemination and collaboration of both public and private information using commercial sites such as Face Book and YouTube.



## Using a commercially hosted application:

- Payment processing
- Emergency notification systems
- HR applications
- Government travel management services

For Conference Purposes Only

# Social Networking Risks

---

- Open collaborative web applications are difficult to protect.
- New technologies are continuously introduced and users may not understand the extent of sharing of information.
- Most sites require registration with a private company.
- Companies may track usage across the site with a “cookie” or other tracking mechanism.
- Inappropriate sharing of personal or other sensitive information.
- Possible workplace distraction.
- Staffing and budgeting concerns.





# Cloud Computing

## ■ What is Cloud Computing?

- Cloud computing is a set of pooled computing resources delivered over the Internet. The cloud (or internet) delivers a hosting environment that doesn't limit an application to a specific set of resources. Depending on the platform, an application can scale dynamically and increase its share of resources.

## ■ Why use Cloud Computing?

- The cloud can quickly access thousands of servers to make resources available as they're needed.

## ■ Types of hosting products:

- Cloud Servers – for on-demand computing power
- Cloud Sites – for robust web hosting
- Cloud Files – for elastic online file storage`



# Electronic Government Act (E-Gov.) 2002

---

- **Agencies should first conduct an assessment of the data and systems proposed for cloud storage.**
  - **A PIA for cloud computing should assess:**
    - What information is to be collected and put into the cloud (e.g., nature and source);
    - Why the information is being collected (e.g., to determine eligibility for a benefit or service);
    - Intended use of the information (e.g., to verify existing data);
    - With whom the information will be shared (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 information will be secured in the cloud (e.g., administrative and technological controls); and
    - Whether a system of records is being created under the Privacy Act and published in the *Federal Register*.



# Privacy Act

**Some of the Privacy Act requirements that will have to be addressed before Federal systems of records are put into the cloud include:**

- Accurate notice;
- Right of access;
- Redress;
- Location of records;
- Choice and consent;
- Data quality and accuracy; and
- Collection, use, retention, and disposal.





# Required Privacy Protections

---



## Government will:

- Establish a Terms of Service (TOS) for the use of the collected information;
- Be allowed access to the data to perform necessary audits;
- Include breach language in the TOS that informs the provider of their responsibility for incident handling;
- Identify retention and destruction limits for the data; and
- Notify individuals that their information is “going into the cloud.”



## Cloud Provider will:

- Allow individual access to his or her data and/or redress;
- Not conduct searches and analyses through the data to sell to marketers;
- Implement the Federal security requirements to prevent the data in the cloud from being viewed by unauthorized persons;
- Obtain a court order to search through the cloud; and
- Not move the data to a different country, or cloud without government approval.

# Cloud Computing Provider (CCP)

## **Cloud Provider should:**

- Establish an agreement with the government;
- Strictly adhere to the Privacy Act requirements; and
- Ensure the protection and safety of the information.

## **Government should:**

- Conduct a risk assessment;
- Identify appropriate security controls to protect against the risk, and implement those controls; and
- Provide a point of contact for any questions from users.



# Cloud Computing Risks

---

## CCPs could:

- Hold or process data without complying with Federal privacy requirements;
- Allow secondary use of the information which may violate laws under which the information was collected;
- Have data in a multi-jurisdictional environment:
  - From one jurisdiction to another;
  - From provider to provider; or
  - From machine to machine, thus creating different legal impacts.





# Contracting with CCPs

---

## Rather than modifying TOS:

- Allow agencies greater ability to comply with and audit the privacy concerns;
- Affirm that the CCP is following IT security requirements and procedures to ensure that information is appropriately secured;
- Review the monitoring/testing/evaluating on a regular basis to ensure that controls continue to work properly, safeguarding the information; and
- Ensure that CCPs do not use subcontractors or transfer information to other third parties without the knowledge and approval of the contracting agency.

## Agency rules of conduct (for the contractor and the contractor's employees):

- Include agency personally identifiable information breach notification policies and incident handling requirements;
- List the anticipated threats and hazards that the contractor must guard against;
- Describe the safeguards that the contractor must specifically provide; and
- Allow government inspection during performance of the contract.





## Other Federal Policy Issues

---

- What an agency publishes on a social network site comprise “federal records”;
- The terms of services agreements may not be legally acceptable to the federal government indemnification;
- The service provided by the Agency to the public may constitute an “information collection” under the Paperwork Reduction Act;
- User generated content is hard to control and can prove a threat to agency reputation if not constantly monitored;
- Not all sites are accessible to those with disabilities; and
- Most providers are for-profit enterprises, and often support their operations by placing advertisements, which can raise endorsement issues.



## Considerations

- Cloud computing and social networking can be an option for federal agencies when rights of individuals are recognized and the potential risks are identified and addressed;
- Include privacy staff early in the development process; and
- Review the Agency policy on Social Networking.