Walking the Line Between Cloud Privacy Policies and the GLBA

Cynthia N. Sarno
Chief Privacy Counsel
Farmers Insurance Group of Companies®
October 11, 2012
Outline of Presentation

A. Purposes and Applicable Provisions of the GLBA

- Scope
- Restrictions
- Exceptions
- Objectives

B. Laws Implementing Safeguarding Requirements

- FTC Safeguards Rule
- FACTA Disposal Rule
- Breach of Security Notification Statutes
C. Cloud Provider Privacy Policies

- Rights over data
- Qualification as GLBA Service Provider
- Conflict with your privacy policy
- Hosting Agreements
- Sample cloud provider policies

D. Takeaways
YOU’RE NOT GOING NAKED INTO THE CLOUD!
The Gramm-Leach-Bliley Act (GLBA) restricts “financial institutions” from disclosing “nonpublic personal information” to non-affiliated third parties, other than under applicable exceptions.

Disclosure to a “service provider” is an exception.
A financial institution may provide nonpublic personal information to a third party to perform services, if the financial institution discloses the providing of such information in its Privacy Policy and enters into a contractual agreement that requires the third party to maintain the confidentiality of the information.
“Nonpublic personal information” is an extremely broad category of data, which includes:

- Information a consumer provides to us on an application;
- Account balance and payment information;
- The fact that a person is or has been our customer;
- Any information about the consumer if disclosed in a manner that indicates the person is or was our customer;
- Information from a consumer report.
Financial institutions must issue initial and annual Privacy Notices, which set forth their policies and practices with respect to:

- Disclosing nonpublic personal information to affiliates and nonaffiliated third parties
- Protecting the confidentiality and security of nonpublic personal information
Nonpublic personal information cannot be disclosed other than as described in your Privacy Notice.
GLBA Safeguarding Objectives

Regulators of financial institutions must establish appropriate standards relating to administrative, technical, and physical safeguards—

(1) to insure the security and confidentiality of customer records and information;

(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and

(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.
Implements GLBA safeguarding objectives. Applies to the handling of customer information by all financial institutions over which the FTC has jurisdiction.

Requires:

- Information security program to satisfy GLBA objectives
- Risk assessment
- Implementation of safeguards and monitoring
- Oversight of service providers
- Evaluate and adjust the program
- Applies to users of consumer reports.

- Any person that maintains or otherwise possesses consumer information must “take reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.”
• 46 states and DC have enacted laws that require notification of security breaches involving “personal information”.

• Business that owns or licenses data must notify if resident’s unencrypted personal information was or is reasonably believed to be have been [accessed, accessed and acquired, acquired] by an unauthorized person.

• Person or business that maintains the data must notify the data owner or licensee.

• Narrower category of data than NPPI.
Cloud Provider Privacy Policies

• Common for cloud providers to offer services through shrink wrap contracts, subject to a non-negotiable Privacy Policy.

• Their Privacy Policy may give them rights over your data, e.g., copying, use, change, publishing, displaying, distributing, sharing, marketing.

• Cloud providers can change the terms of their Privacy Policy at any time.
Two Questions Before you go to the Cloud

1. Is the Cloud Provider actually a GLBA “Service Provider” or does its Privacy Policy grant it rights over your data?

2. Will use of this Cloud Provider allow you to comply with your safeguarding obligations?
• Business must carefully consider both the privacy laws and the cloud provider’s Privacy Policy when deciding whether to use a cloud provider to store or process nonpublic personal information and in choosing a particular cloud provider

• The terms under which the information is disclosed to and the rights acquired by the cloud provider will determine the legality of the disclosure, as well as to subsequent use of your data.
Sample Cloud Provider Privacy Policy Provisions
Vendor will host and operate the Software at Amazon Web Services™ (the “Hosting Facility”). Terms and Conditions governing the use of the Amazon Web Services can be found at http://aws/amazon.com/agreement/.
“Customer consents to AWS’s collection, use and disclosure of information associated with Service Offerings in accordance with the Privacy Policy.

‘Privacy Policy’ means the privacy policy currently referenced at http://aws.amazon.com/privacy, as it may be updated by AWS from time to time.”
As a subsidiary of Amazon.com, AWS follows the same information practices as Amazon.com, and information we collect is subject to the Amazon.com Privacy Notice. By visiting the AWS site, you are accepting the Practices described in the Amazon.com Privacy Notice.
• “We receive and store any information you enter on our Web site or give us in any other way.”

• “We use the information you give us for such purposes as...customizing future shopping for you, improving our stores...”

• “We share customer information only as described below and with subsidiaries Amazon.com controls...”
• “We work closely with affiliated businesses. In some cases, we sell product lines jointly with these businesses....You can tell when a third party is involved in your transactions, and we share customer information with that third party.”
“We release account and other personal information when we believe release is appropriate to comply with law; enforce or apply our Conditions of Use and other agreements; or protect the rights, property, and safety of Amazon.com…or others.”
“This Policy governs how we collect, protect, store, process, transfer and use the personally identifiable information we collect from and about you. This policy applies to RightScale’s online and Offline activities.” (2006 - 2011 RightScale, Inc.)
“…The following privacy policies are tailored for the different ways your personal information is collected by different Oracle lines of business and offerings.

The Oracle privacy policy addresses information we collect at our web sites and in off-line sales and marketing activities.

The services privacy policy addresses customer data to which we may be provided access in order to perform consulting, product support, outsourcing and other services.
The Oracle Recruiting privacy policy addresses information we collect we may collect in connection with Oracle's employment recruiting efforts.

The exchange.oracle.com privacy policy addresses Information shared in an online commercial trading community.”
• Can you get a Master Services Agreement?

• How does it relate to the cloud provider’s Privacy Policy?
• Does the transaction involve nonpublic personal information?

• Does the cloud provider have a Privacy Policy?

• Does its Privacy Policy apply to your transaction?

• Can you comply with the cloud provider’s Privacy Policy while complying with your own Privacy Policy and other data security and privacy obligations?

• If not, is the cloud provider willing to negotiate the terms of its Privacy Policy?