Cloud Services: Managing Privacy Risks
Structuring Cloud Computing Agreements and Policies Governing Employee Use of Mobile Devices

TUESDAY, OCTOBER 16, 2012
1pm Eastern  |  12pm Central  |  11am Mountain  |  10am Pacific

Today’s faculty features:

Margaret Keane, Shareholder, Littler Mendelson, San Francisco
John Kennedy, Partner, Wiggin and Dana, Stamford, Conn.
Christopher M. Koa, Senior Legal Counsel, Dell, Round Rock, Texas

The audio portion of the conference may be accessed via the telephone or by using your computer’s speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact Customer Service at 1-800-926-7926 ext. 10.
Sound Quality
If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory and you are listening via your computer speakers, you may listen via the phone: dial 1-866-320-7825 and enter your PIN when prompted. Otherwise, please send us a chat or e-mail sound@straffordpub.com immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality
To maximize your screen, press the F11 key on your keyboard. To exit full screen, press the F11 key again.
For CLE purposes, please let us know how many people are listening at your location by completing each of the following steps:

• In the chat box, type (1) your company name and (2) the number of attendees at your location
• Click the word balloon button to send
The Well-Planned Cloud –
Data Privacy and
Security in Commercial Cloud Computing

Christopher M. Koa and John B. Kennedy
October, 2012
Introduction and Overview

**Focus**: Data privacy and security risks in the use of cloud-based services and managing such risks, in part, through service provider contracts

1. Cloud computing defined
2. Advantages and risks of using cloud services
3. Threshold data privacy and security concerns in commercial cloud services; privacy-related due diligence
4. Market trends and provider perspectives on utility models
5. Key contract issues in custom enterprise model contracts
6. Questions
Cloud Computing Defined
Defining “the Cloud”

• National Institute of Standards and Technology:
  – “a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources . . . that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

• More simply, the “cloud’ is “the act of storing, accessing and sharing data, applications and computing power in cyberspace.” (Pew Research Center)

• Almost any kind of information can be stored and processed in the cloud:
  – Customer records, databases, e-mail, health records, financial data, employee records, business applications, consumer applications
What is Cloud Computing?

NIST Definition

• Ubiquitous and broad network access
• Pooled Resources
  - Multi-tenant
• Rapid Provisioning
• Pay as You Go
Deployment & Service/Delivery Models

- Collaborative applications
- ERM, CRM, supply chain apps
- Ops and manufacturing apps
- Patient/student records apps

- Development tools
- Database, middleware
- Infrastructure software

- Server, storage, network components
- OS, virtualization, file system
- Capacity on demand

Private vs. Public

Software as a Service

Platform as a Service

Infrastructure as a Service
Advantages of Cloud Computing

• For customers:
  – Lower initial investment
    • Third party-provided infrastructure, lower IT capital costs, lower overhead
  – Computing costs spread over time
  – Flexibility, agility, scalability (relatively quick access to expanded computing resources)
  – Access to specialized expertise, strong platforms, better security

• For providers:
  – Economies of scale
  – Smoother revenue streams
  – Value-added services opportunities
  – Heightened control of IP and systems
Threshold Data Privacy and Security Concerns in Commercial Cloud Services
Privacy Concerns in Cloud Computing

NIST SP-800-144 ("Guidelines on Security and Privacy in Public Cloud Computing") (December 2011)

FFIEC, “Outsourced Cloud Computing” (July 2012)

- **Loss of direct control** over data processing, related controls and regulatory compliance requirements
- **Loss of transparency**; reduced visibility into systems and operations
- **Data security**; risks of multi-tenanted services environments
- **Multi-jurisdictional data flows**; attendant uncertainty as to applicable laws
- **System complexity**; subcontracting
The EU Take on Privacy in Cloud Computing


• Identifies two central concerns for privacy in cloud computing
  – Lack of control over key aspects of data processing by the data controller
  – Lack of transparency of data processing operations
• Offers detailed guidelines for customer and providers of cloud services
  – Subcontracting safeguards
  – Compliance with data protection principles
  – Detailed contractual safeguards
Threshold Questions for Privacy Counsel

• Will personal data be processed by the cloud provider?

• What are the data flows and what data laws may apply?
  – In what jurisdictions will personal data be collected?
  – In what jurisdictions will personal data be processed?

• Are there potential regulatory show-stoppers?
  – E.g., data transfer restrictions, data residency requirements, regulatory approvals, mandated foreign government access to provider systems

• Have privacy and security risk assessments been conducted?

• Will the use of cloud services violate existing contractual and privacy commitments to customers?

• Is the vendor solution compatible with the customer’s corporate polices for privacy, data security, record retention, e-discovery, audit and risk management?
Privacy Diligence of Cloud Service Providers

What to look for in privacy and security policies and practices
• Provider service agreement terms and privacy policies
• Inspections of data centers (when feasible)
• Written security policies consistent with or exceeding customer policies
  – Technical, administrative, logical measures; encryption policy
  – Compliance with applicable standards (ISAE 3402, ISO 270001, PCI DSS, etc.)
• Industry certifications, third party assessments, audit reports
• Disaster recovery and business continuity capabilities
• Shared environment security: account segregation and controls
• Breach prevention and response plans; security track record
• Logging, monitoring and auditing capabilities
• Reliance upon subcontractors for data-related processes
• Data transfer/transition policies (i.e., “portability”)
• Data recoverability and data destruction practices
Contracting for Cloud Services:

Market Trends for Standard Utility Model Deals
Current Commercial Trends in Cloud Contracting

• Standard Utility Model
• Customized Enterprise model (more expensive)
• Public statements of cloud computing principles, best practices
• Service offerings intended to address customer data privacy concerns
Utility Model: Market Trends

• Market Trends re Utility Cloud Based on NIST Draft Cloud Computing Synopsis and Recommendations (May 2012)
  – SLAs
  – Remedies
  – Data Backup
  – Data Preservation on Termination
  – Liability
  – Security & Data Breaches

• Provider Rationale for Standard Utility Model Contract Terms
Contracting for Cloud Services:
Privacy and Security Issues to Consider in Custom Enterprise Service Model Deals
Customized Contract Issues –
1. Data Ownership, Collection and Use

- Specify **customer ownership** of customer-provided data
  - Address rights in any transactional or relationship data, derivative data and ‘meta-data’
- Specify the **provider’s use rights** in customer data
  - Limit to uses required to provide the services, comply with law and meet archival requirements
  - Clearly define any permitted first or third party marketing uses or other secondary uses of customer data
  - If anonymized or de-identified data may be created, specify standards and allocate related risks
  - Provider reps or covenants to comply with customer privacy policies (to the extent these have been disclosed)
- In contracts subject to EU data protection requirements, **clarify data controller (customer) and data processor (provider) roles**
  - Consider whether the provider (processor) may become a controller
Customized Contract Issues –
2. Data Availability, Retention, Destruction

• Include defined **service levels for data access and availability**
  – E.g., uptime, system response time, mean time to restore or fix, support response time
  – Are there defined metrics and service credits for failures?
  – Where appropriate, specify rights of access to and correction of data (e.g., in contracts subject to EU data protection law)

• Are company **data retention requirements** specified, including for litigation holds and audit trails?

• Are the parties’ **disaster recovery and business continuity** obligations and performance goals clearly allocated and stated?

• Address **secure data destruction** or de-identification of personal data
  – Specifications for destruction or return
  – Problem of residual data with sub-processors, multi-tenants
Customized Contract Issues –
3. Data Security

- **Identify customer’s data security requirements** in the contract
  - Or do a gap analysis of provider’s infosec plan and address gaps
- Include in the contract:
  - Comprehensive security undertakings appropriate to sensitivity of the data (e.g., access controls, encryption, network security, personnel clearance, etc.)
  - A detailed information security requirements schedule
  - Service levels, response times (where applicable)
  - Reference applicable data security standards (e.g., ISO, PCI DSS)
- If shared environments are used, address **data segregation requirements**
- Clarify **provider-controlled security** vs. **customer-controlled security**
  - Responsibilities matrix
- Include a **right to monitor** provider’s continuing compliance with security controls
- Include **remedies for data loss**, unavailability and/or corruption
  - E.g., credits, costs to restore or re-create
Customized Contract Issues –
4. Security Incidents, Data Breaches

• Defined triggers: “security breach”, “security incident”, other?

• Perimeters: how are the parties’ responsibilities for securing hard and virtual assets allocated across the entire service model?

• Detailed incident response plan:
  – Incident verification and notice to customer; chain of command
  – Containment and mitigation
  – Investigation, forensics and information sharing
  – Data preservation and audit capability
  – Remediation, service restoration and prevention
  – Cooperation with customer in meeting legal requirements
  – Customer retains control over notice obligations and communications with regulators and the public

• Allocate financial responsibility for breach-related costs
Customized Contract Issues –
5. Data Location, Transfer, Third Party Access

• The cloud computing model for provisioning services is inherently cross-border
  – Data can be located simultaneously in different countries and be subject to different national privacy and data security laws

• Customer (data controller) contractual right to control cross-border data transfers
  – Will the provider offer geographically bounded services?

• Will anticipated cross-border flows of personal data be subject to ‘adequacy’ requirements (e.g., transfers outside of the EU)?
  – Are compliant data transfer mechanisms in place (e.g., model contracts, Safe Harbor certification, BCRs, other)?
  – Are flow-down terms required for approved sub-processors?

• Potential for compelled disclosure to government authorities
  – E.g., Patriot Act concerns of non-U.S. cloud customers

• What are the provider’s standard practices for responding to subpoenas or other government process? Litigation holds?
Customized Contract Issues –
6. Subcontracting and Sub-processors

- Cloud providers may engage multiple subcontractors for provisioning storage and processing services around the world
  - Some cloud providers are themselves cloud customers (e.g., ‘cloud bursting’ services)
- Seek rights of prior notice and approval of provider’s subcontracting of data-sensitive services
  - Pre-approval of all existing subcontractors
  - Mechanics of the notice, approval and removal process
  - Possible pre-conditions to subcontractor appointments:
    - Due diligence right
    - Flow-down provisions from prime contract into subcontracts
    - Third party beneficiary status for the customer
    - Provider assumption of primary liability for subcontractor acts and omissions; joint and several liability
- Revised EU model controller-to-processor clauses
Customized Contract Issues – 7. Audits, Monitoring and Inspections

• The right and ability to monitor and/or audit service providers is a requirement for many regulated businesses that outsource
  – Scope and type of audit, oversight standards/protocols should be specified
    • E.g., ISAE 3402 Type 2, ISO 27001, FISMA
    • E.g., SOX, SEC, FINRA, HIPAA, GLBA
    • Special terms for audits by governmental authorities
  – Audit obligations should flow through to subcontractors in “layered” services arrangements
  – Terms should include access to audit reports, certifications, taking corrective measures and remedies for failure to correct
  – Requirement to maintain applicable certifications during the term
  – Timing of audits; audit frequency and costs; follow-up audits

• Include periodic inspection rights
  – Scope of inspection: compliance with agreed contract specifications for infrastructure and data security and/or specified potential vulnerabilities
8. Compliance with Privacy-Related Laws

- Have customer’s data-related legal compliance requirements been included or referenced in the contract?
  - E.g., HIPAA, GLBA, PCI DSS, data breach notification statutes, data security statutes
  - Are local country privacy law schedules or annexes required?
  - Forms of data transfer agreements

- “Customer laws” vs. “Provider laws”
  - What level of responsibility for customer compliance with data privacy laws should be placed on the provider?

- Allocation of responsibility for complying with changes in law
  - Parties obligations to monitor changes in law
  - Allocating financial responsibility for related changes in the services
  - Governance and change control
Customized Contract Issues –
9. Termination, Exit Services and Data Portability

• Termination events
  – **Customer**: e.g., convenience, for cause, insolvency, change of control, regulatory orders
  – **Provider**: e.g., non-payment; material violation of provider IP rights
    • AUP violations?

• Consequences of termination
  – Exit and transition period?
    • Duration and pricing
  – No liens on customer data or other provider right to withhold data
  – Specifications for return of data and format/transfer requirements
  – Provider obligation to destroy/delete data securely, at customer’s option
    • Certification of compliance
    • Specifications for destruction
  – Provider cooperation with successor
Customized Contract Issues –
10. Indemnification, Liability Limits and Insurance

• Typically a sensitive issue with respect to privacy and security
• Indemnification
  – In data-sensitive arrangements, consider seeking indemnification for provider breaches of confidentiality, data privacy and security obligations (including compliance with laws)
• Liability Caps
  – Typically limited to some period of fees (e.g., 1 year)
  – Exceptions: willfulness, indemnity obligations, violations of law?
• Exclusion of consequential damages
  – Consider ‘carving in’ data loss, corruption or unavailability due to provider breach
  – Also carve in for data breach costs (including fines)
• Provider insurance coverage
A Few Cloud Computing Resources

“Cloud Computing Synopsis and Recommendations”, NIST Special Publication 800-146 (L. Badger, T. Grance, R. Patt-Corner, J. Voas)


“Outsourced Cloud Computing”, Federal Financial Institutions Examination Council (July 10, 2012)


“Reaching for the Cloud(s): Privacy Issues Related to Cloud Computing”, Office of the Privacy Commissioner of Canada


New Haven
One Century Tower
P.O. Box 1832
New Haven, CT 06508

New York
450 Lexington Avenue
Suite 3800
New York, NY 10017

Philadelphia
Two Liberty Place
50 S. 16th Street, Suite 2925
Philadelphia, PA 19102

Stamford
Two Stamford Plaza
281 Tresser Boulevard
Stamford, CT 06901

Hartford
One CityPlace
185 Asylum Street
Hartford, CT 06103

Greenwich
30 Milbank Avenue
Greenwich, CT 06830
Questions?

Christopher M. Koa
chris_koa@dell.com
512.728.5039

John B. Kennedy
jkennedy@wiggin.com
203.363.7640
The Accidental Cloud

• Wireless and Smartphone = Gateway to Cloud
• Think of Mobile Devices as “Cloud Access Tools”
• Your Employees are sending data to the Cloud 24/7
Running Water, Electricity and Wi-Fi

• By 2015, the global mobile worker population will reach 1.3 million, representing 37.2% of the global workforce

• IPASS Global Workforce Report for Q2 describes wireless access as a necessity of life

• Do you consider wireless access (3G, 4G and wi-fi) as important to your life as running water and electricity?
  – Yes, it is that important to the way I live – 59%
  – No, but it is pretty close – 29%

  IPASS Global Mobile Workforce Report, Q2 2012, p. 5
What Lives in the Accidental Cloud

• Mobile devices send information to data storage, video, photography and social networking sites, and web-based email providers
• Cloud services can replace thumb drives for storage
• Cloud services also provide collaboration capabilities – may be used to circumvent IT restriction on sharing information outside the enterprise
• Third party storage: Where is your data?
  – iCloud
  – Google Docs
  – Dropbox.com
  – Box.net
• Generally, there is no reasonable expectation of privacy in data held by third parties
• An employer rarely has any control over data stored by third party providers
Lingo: Dual Use Mobile Devices and BYOD

• Dual Use Mobile Device: Mobile device used to create, store and transmit both personal and work-related data

• BYOD: Bring Your Own Device
  – A BYOD program includes:
    • Policies that govern use of personal devices to access corporate services
    • Policies attempt to manage risk associated with storage and transmittal of data using devices that may be outside of the employer's control
    • Policies address impact of mobile devices on existing workplace behavior

• Some Other Considerations:
  – Regulatory issues, esp. FINRA – financial services, insurance, HIPPA
  – Federal Trade Commission
  – E-discovery implications
What is MDM – Mobile Device Management?

Mobile Device Management:

• Software that allows corporate IT to manage use of mobile devices. Component of BYOD programs. Features may allow an employee to:
  – Require users to register device as condition of network access
  – Lock down end user’s ability to use specific device features or apps, such as cameras, Siri or iCloud
  – Enable remote locking or wipe of device
  – Enforce use of strong passwords
  – Implement anti-spam solutions – Siri, iCloud file sharing, blacklists
  – Prevent users from disabling or altering security settings on devices
Policies Affected by BYOD

- Data Privacy & Security
- Harassment, Discrimination & EEO
- Workplace Safety
- Time Recording and Overtime
- Acceptable Use of Technology
- Compliance and Ethics
- Records Management
- Litigation Holds
- Confidentiality & Trade Secret Protection
The Perils of Mobile Devices

• Lost or stolen devices
• Malware
• Friends & Family
• Implications of a security breach
1. Remote wipes of lost devices – can be viewed as either pro-privacy or an intrusion. Participation in BYOD program may be conditioned upon consent to remote wipes.

2. Litigation issues:
   – Identification of BYOD devices/information
   – Practical challenges of data collection
   – Does the employee “control” data on the devices?
   – Will employees be required to produce mobile devices to employer for inspection, preservation and production?
   – Will employees be required to allow access to other home devices such as storage devices, or Cloud-based storage accounts?
3. Accessing data stored with online services – What is a reasonable expectation of privacy? Be careful.

- *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC*, 587 F. Supp. 2d 548 (S.D.N.Y. 2008) (employee had reasonable expectation of privacy in password protected emails stored on hotmail and gmail servers, regardless of fact that she accessed them on a work computer)

- *Steingart v. Loving Care Agency, Inc.*, 201 N.J. 300 (NJ 2010) (employee had reasonable expectation of privacy in personal password protected web-based email sent through employer’s computer)

- *Pietrylo v. Hillstone Restaurant Group*, No. 06-5754, 2008 U.S. Dist. LEXIS 108834, at *20 (D.N.J. July 24, 2008) (question of whether employee had a reasonable expectation of privacy in My Space page is a question of fact)

- *Ehling v. Monmouth-Ocean Hospital Service Corp.*, Civ. No. 2:11-CV 033305 (WJM) (D.N.J. May 30, 2012)(plaintiff may have reasonable expectation of privacy in Facebook posting where she restricted access to her Facebook page)

Setting Up a BYOD Program

- Need to address challenges of dual use devices, REGARDLESS of whether you adopt a BYOD program

- If you implement BYOD, your policy should be part of an integrated Information Governance Plan

- Determine goals and objectives
  - Economics – Not necessarily saving money
  - Security
  - E-Discovery compliance
  - Risk Management concerns
  - Privacy Considerations
    - Remote wipes
    - Containers
    - Backups
  - Pushing back the tide
Setting Up a BYOD Program

• Who participates in program?
  – Limit to exempt employees.
  – If non-exempt employees are included, need to address overtime wage exposure.
  – Exclude contractors and contingent workers who may be working for other customers.
  – Consider excluding individuals in sensitive positions or involved in litigation or regulatory proceedings.
Setting Up a BYOD Program

• Who will pay and what devices are included?
  – Who pays for/owns device?
  – Who pays for service plan – employer selected options or reimbursement?
  – Options include technology allowances, reimbursement, standard devices issued by employer.
Setting Up a BYOD Program

• What conditions will be imposed on participants in the program?

• Address tradeoff of privacy for convenience
  – Participation in program is a privilege, not a right
  – Privacy tradeoff for convenience of remote access and device
Setting Up a BYOD Program

Privacy Parameters

• Distinguish between data and device

• Device
  – May require return upon demand or inspection as part of investigation
  – May require return, with data intact, upon separation from employment

• Data
  – Determine whether employer will retain right to review all contents of device or will exclude categories such as music and photos
  – Require employee to provide access to cloud backups or home server?
  – Monitor/limit employee’s use of web-based applications? Example: Siri, Dropbox, iCloud, etc.
  – Set parameters for timing, terms and extent of remote wipes
• 60 percent of corporations plan to implement formal programs for monitoring external social media security breaches and incidents by 2015
• Less than 10% of these organizations now use these techniques for security monitoring
• Tread carefully before engaging in collection and sharing of information, especially account passwords, from employee’s mobile devices
• Understand risks of monitoring personal activities
• Password issues. Require strong passwords
• If device is sending location-based information, disclose the practice. Tread carefully.
• Determine need for access to other personal computer devices, home storage and Cloud-based storage accounts
Can Data in the Cloud Undermine Your Trade Secret Protection?

Trade Secrets Must Be:
1. Maintained in confidence
2. Have commercial value from not being generally known
3. Must not be readily ascertainable by proper means

Risk Areas:
1. LinkedIn – Customer lists in the public domain?
   - Customer information not a trade secret where publicly available information “exceeded the amount and level of detail contained in the Sasqua database.”
   - Sasqua did not have password protected computers; did not require employee to sign confidentiality or non-solicitation agreement
Protection of Trade Secret Information in the Cloud

- Take Reasonable Measures to Protect Trade Secrets in a BYOD Environment
- Use Confidentiality Agreements/Proprietary Information Assignment Agreements ("PIAA")
Questions?
The Accidental Cloud

November 16, 2012

Margaret A. Keane, Esq.
Littler Mendelson, P.C.
San Francisco Office
(415) 288-6303
mkeane@littler.com