# Data Privacy & Security in the Cloud: Legal Basics and New Developments

Lawrence R. Freedman
Partner, Edwards Wildman Palmer LLP
lfreedman@edwardswildman.com
(202) 939-7923

# Data Privacy & Security in the Cloud: Legal Basics and New Developments

## The Basics

- Two basic data security obligations
  - Duty to protect data
    - Provide "reasonable security" for corporate data in their possession
    - Ensure that service providers (e.g., cloud providers) do the same
  - Duty to disclose data breaches
    - Disclose breaches (to affected parties and regulators)
    - Disclose "material risks" (public companies)

# Data Privacy & Security in the Cloud: Legal Basics and New Developments

## The Basics

- Multiple sources for data security obligations
  - Statutes and regulations -
    - Privacy laws
    - Security laws and regulations (mostly state level)
    - Unfair business practice laws and enforcement thereof (e.g., FTC)
    - Corporate governance legislation and regulations (e.g. SOX)
    - Sector-specific regulations (e.g., HIPAA, GLB, SEC, COPPA)
  - Common Law Obligations
  - Rules of Evidence
  - Contractual Obligations
  - Industry Self-Regulation (e.g., credit card industry PCI rules)
  - Self-Imposed Obligations (e.g., what you say on your website)

# Data Privacy & Security in the Cloud: Legal Basics and New Developments

## The Basics

- What is reasonable data security?
  - Defined by law/regulation for selected sectors
    - GLB security regulations (financial sector)
    - FISMA (gov't agencies)
    - HIPAA security regulations (healthcare sector)
    - Massachusetts regulations (all sectors)
  - Largely defined by the FTC for all other sectors
    - Primarily by FTC enforcement actions (all sectors)
    - State AGs following suit (when interpreting state security laws)
  - Embodied in the concept of a "Comprehensive Written Information Security Program" (WISP)

# Data Privacy & Security in the Cloud: Legal Basics and New Developments

## The Basics

- What, generally, does reasonable data security require?
  - Assigning responsibility
  - Identifying what needs to be protected
    - Both (i) under company control and (ii) outsourced / cloud
  - Conducting risk assessment
    - Identify and evaluate threats, vulnerabilities, and damages
  - Selecting, developing and implementing security controls --
    - That are responsive to the risk assessment
    - That address the required "categories" of controls
  - Addressing third party security (e.g., cloud providers)
  - Monitoring the effectiveness of the program
  - Regularly reviewing, reassessing, and adjusting the program

# Data Privacy & Security in the Cloud: Legal Basics and New Developments

## The Basics

- The three core cloud security requirements
  - Due diligence in selection of cloud provider
    - Select and retain service providers that are capable of maintaining appropriate safeguards for the information at issue
  - Imposition of contractual security requirements
    - Contractually require cloud providers to implement and maintain such safeguards
  - Monitoring of compliance

# Data Privacy & Security in the Cloud: Legal Basics and New Developments

## The Basics

- Possible sources of assurance of appropriate data security
  - US-EU Safe Harbor Program
    - Self asserted claims of reasonable security, etc.
  - Cloud Security Alliance – Security, Trust & Assurance Registry (STAR)
    - Self assessment and self asserted claims re security
  - FedRamp certification
  - Third party audits / certification of compliance with standards, etc.
    - E.g., ISO 27001 certification

# Data Privacy & Security in the Cloud: Legal Basics and New Developments

## The Basics

- The duty to disclosure data breaches (state law obligations)
  - Now 47 states; covers cloud storage/processing
  - Triggered by breach of covered personal data
    - Must notify subjects of breached data (and often State AG)
    - Basic approach - cloud provider has duty to notify customer; customer has duty to notify data subjects and state AGs
  - Increasing pressure on cloud users (new Florida law. eff. July 1, 2014) -
    - Adds express duty to provide "reasonable" security for covered data
    - Requires cloud providers to notify customer within 10 days of breach
    - Requires customer to notify data subjects within 30 days total
    - Adds requirement for AG notice and duty to provide AG with forensic reports, breach policies, and other security docs upon request
      - May facilitate government investigation of security practices

# Data Privacy & Security in the Cloud: Legal Basics and New Developments

## The Basics

- The duty to disclosure data breaches (SEC obligations)
  - SEC Disclosure Guidance (October 13, 2011)
    - Division of Corporate Finance
    - Public companies must disclose material events which a reasonable investor would consider important to an investment decision
    - Guidance: Registrants should disclose material cybersecurity risks and incidents
  - SEC Roundtable re cybersecurity issues and SEC response (March 26, 2014)
  - SEC National Exam Program Risk Alert (April 15, 2014)
    - Office of Compliance Inspections and Examinations (OCIE)
    - Explains its initiative to "assess cybersecurity preparedness in the securities industry"
    - Includes specific focus on risks associated with third party service providers (and compliance with diligence, contract, and monitoring requirements noted above)

# Data Privacy & Security in the Cloud: Legal Basics and New Developments

## New Developments: The Courts

- *Aereo*
  - Not really a cloud case!
    - Core issues under copyright
  - But raises lots of cloud concerns
    - Impact on remote storage; triggered
    - *Amicus* intervention by cloud/ tech industry
  - "Threading the needle" by the USSC
    - Seeking to limit holding
  - But, did they?

# Data Privacy & Security in the Cloud: Legal Basics and New Developments

## New Developments: The Courts

- *Microsoft*
  - Just when you thought it was "Safe Harbor" to go out into the water…
    - Practice of deploying foreign data centers as work-around to disparate data compliance requirements
    - Particularly to satisfy Europeans concerned about reach of U.S. authorities
  - Subpoena vs. warrant – big difference!
  - "Hybrid" approach – authorized under applicable statutes (Stored Communications Act + Electronic Communications Privacy Act)
  - Ruling: "control" "controls," and information must be turned over

# Data Privacy & Security in the Cloud: Legal Basics and New Developments

## New Developments: Federal Legislation & Regulation

- White House "big data" working group
  - Policy recommendations released May 1, 2014
  - Favoring a national breach notification law
  - Amendments to ECPA
    - The 180-day issue

# Data Privacy & Security in the Cloud: Legal Basics and New Developments

## New Developments: Federal Legislation & Regulation

- Congress on Cybersecurity
  - Sharing of information – key to removing impediments to solving security threats
  - Cyber Intelligence Sharing and Protection Act ("CISPA")
    - Passed by House in April 2013 over threat of veto by President Obama
    - No vote by Senate
  - Cybersecurity Information Sharing Act ("CISA")
    - Passed by Senate Intelligence Committee on July 8, 2014
    - Concern: NSA access to private reports
    - Impact on cloud: information sharing obligations (+ long term greater confidence (?))

# Data Privacy & Security in the Cloud: Legal Basics and New Developments

## New Developments: Federal Legislation & Regulation

- Congress – on Data Breach Notification
  - Multiple bills, seeking to harmonize patchwork of state laws
    - S.1193 Data Security and Breach Notification Act of 2013
    - S.1897 Data Security and Breach Notification Act of 2014
    - S.1927 Data Security Act of 2014
    - S.1976 Data Security and Breach Notification Act of 2014
    - S.1995 Personal Data Protection and Breach Accountability Act of 2014
    - S.2690 Protecting Student Privacy Act of 2014
  - Issues:
    - How long to notify
    - Whether states are preempted

# Data Privacy & Security in the Cloud: Legal Basics and New Developments

## New Developments: Federal Legislation & Regulation

- ECPA reform
  - S.607 Leahy-Lee Electronic Communications Privacy Act Amendments Act of 2014; H.R.1852 Email Privacy Act of 2014
  - DCIA interested!
  - White House wants reform
  - Issues include:
    - Warrant requirement
    - Notification
    - SEC

# Data Privacy & Security in the Cloud: Legal Basics and New Developments

## New Developments: Federal Legislation & Regulation

- Telecommunications regulation
  - "Net neutrality"
    - Hottest issue in the history of the FCC
    - Virtually all major tech companies have weighed in
  - Where do you stand?... Depends upon: where you stand!
  - Basics of net neutrality
  - Fast lanes vs. slow lanes vs. compensated access
  - Impact on cloud providers

# Data Privacy & Security in the Cloud: Legal Basics and New Developments

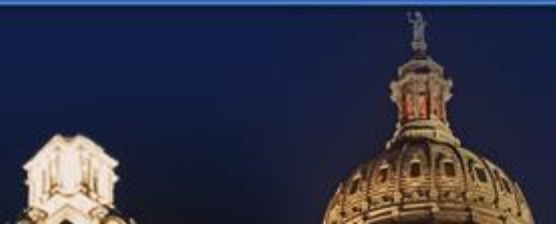
## New Developments: Beyond Washington

- EU data protection regulation
  - Proposed restrictions on U.S. involvement/transfers
  - Concerns about public authority access requests in third countries to personal data stored and processed in EU
  - Scheduled for vote by end of year
  - Recent survey: 1% of cloud providers currently in compliance with proposed regulation

# Data Privacy & Security in the Cloud: Legal Basics and New Developments

## New Developments: Beyond Washington

- EU Cloud Service Level Agreement Standardisation Guidelines (June 2014)
- EU ruling (and Google negotiations) – "Right to be Forgotten" According to EU Justice Commissioner:
  - Right to ask companies operating search engines to remove links with personal information about them – under certain conditions
  - Applies when information is inaccurate, for example, or inadequate, irrelevant, outdated or excessive for the purposes of data processing
  - Balanced against other fundamental rights, such as the freedom of expression and the freedom of the media





# Thank you!