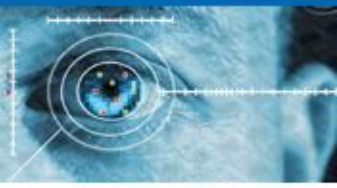


Securing the Cloud: A Legal Perspective

Nick Akerman
Partner
Dorsey & Whitney LLP

Overview

- Security
- Privacy
- Record Retention
- Electronic Discovery
- Potential Liabilities
- Legal Remedies
- Contract Issues
- Compliance/Best Practices

Considerations: Data Security & Data Privacy

- Fall 2009 survey by Mimecast:
  - 46% of all business respondents cited security as a concern in adopting cloud computing as an IT strategy
  - The most reluctant sectors included financial services (76%), energy (75%), and government (67%)
  - 70% of companies that have launched cloud computing initiatives plan to move additional applications and data to the cloud

- Cloud security threats from three fronts:
  - from outside, over the internet
  - from other cloud applications on the network
  - from personnel
  - threats are no different than security fault potentials on any in-house

Considerations: Data Security & Data Privacy (continued)

- Data access governance concerns
  - danger of data falling into the wrong hands – either as a result of people having more privileges than required or by accidental or intentional misuse of the privileges assigned to their job
- Data segregation
  - data is typically in a shared environment alongside data from other customers

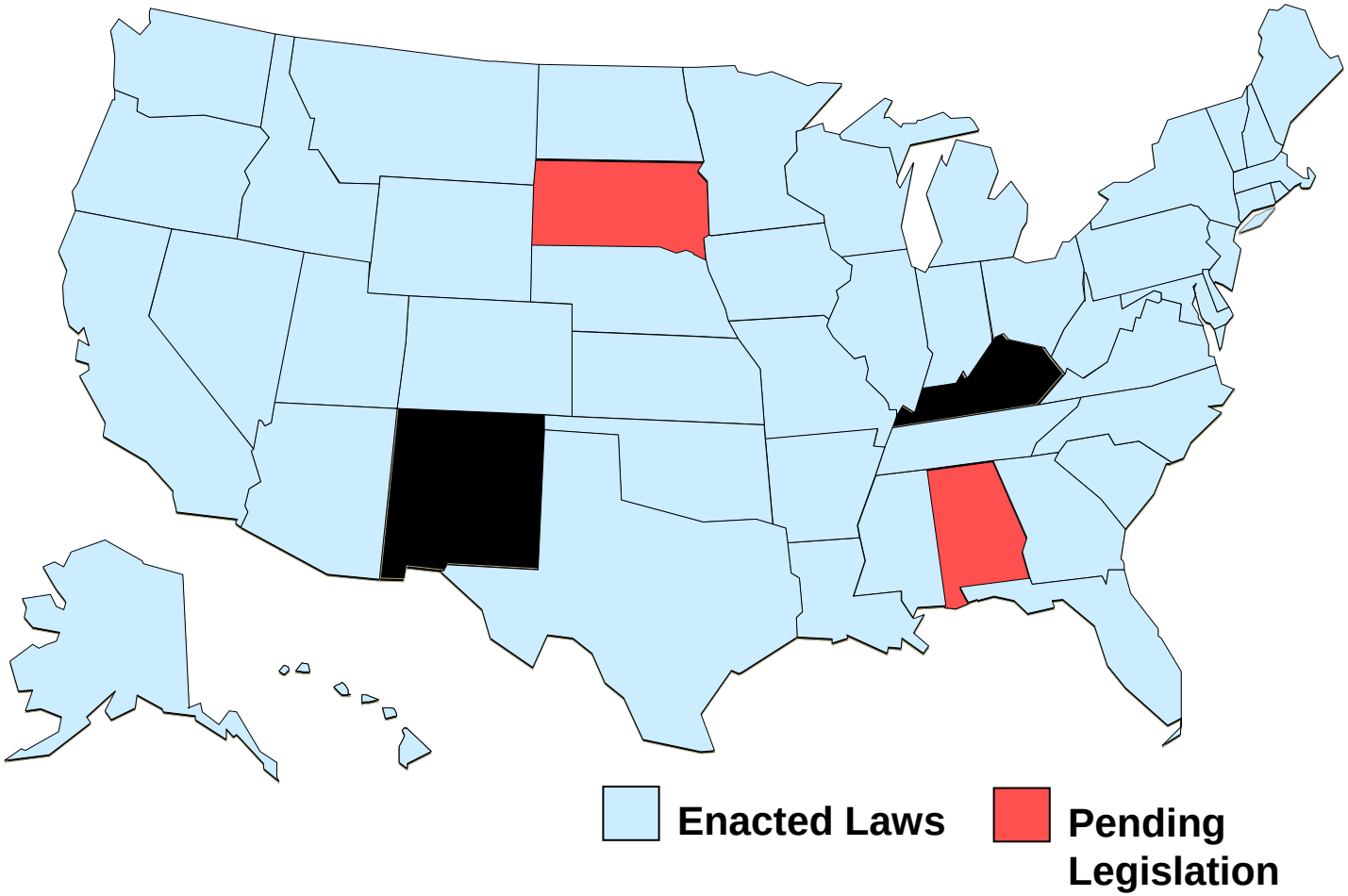
Considerations: Data Security & Data Privacy

- Control over and knowledge/information about data
- Data
  - What kind?
  - What will be done with data?
  - Where?
- Data subjects
  - Where?

Notification California Database Security Breach Act

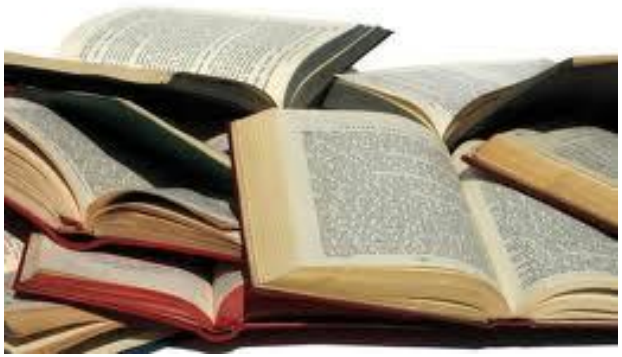
- Effective July 1, 2003
- Companies must notify individuals of security breach that could lead to identity theft
- Security breach is “unauthorized access”
- Does not apply to public information
- Applies to all companies doing business in California regardless of where data is kept
- Authorizes private actions and does not bar class actions
- 46 states have enacted similar laws

States That Have Enacted Breach Notification Laws



Provisions of the Statutes

- Notification requirement to consumers varies among states
- Third party vendors
- Different remedies
- Certain states exempt encrypted and/or redacted data from the notification process
- Timing standard varies
- Law Enforcement Exception
- Key issue is the ambiguous situation
- Investigation requirement



TJX Multi-State Settlement
June 24, 2009

- 2007 data breach to cardholder data and other personal data
- Investigation and action by 41 States
- TJX agreed to implement and maintain a comprehensive data security program
- Must report regularly to the State Attorney Generals on the efficacy of the security program
- $9.75 million paid to the States

Federal Trade Commission Requirements

- Failure to secure personal data is an unfair trade practice – Title 15 U.S.C. Section 45(a)
- Claims about data security should be accurate
- Protect against common technology threats
- Know the identity of third parties with whom sharing customers' sensitive information
- Do not retain unneeded sensitive consumer information
- Dispose of sensitive consumer information properly

HITECH Act – 2009 Stimulus Package

- Amends HIPAA to include notification, September 2009
- Breach of protected information
- Breach as of date discovered or should be known
- Name alone is breach
- Electronic and paper records
- Encryption has to meet certain standards
- Notice to media in certain circumstances

Privacy Concerns Re: Social Network Sites

- *EEOC v. Simply Storage Mgmt, LLC*, (S.D. Ind. May 11, 2010) (observing that "[i]t is reasonable to expect severe emotional or mental injury to manifest itself in some [social networking] content," and therefore allowing discovery of the plaintiffs' Facebook and MySpace accounts where "emotional health" was at issue. The parties disagreed on the scope of discovery, with plaintiffs fearing that the information discovered could embarrass them; however, the Court discounted this concern because the information had already been shared "with at least one other person through private messages or a larger number of people through postings.").

- *Barnes v. CUS Nashville, LLC*, 2010 WL 2265668 (M.D. Tenn. June 3, 2010) (magistrate judge offered to create a Facebook account for himself "[i]f [the parties] will accept the Magistrate Judge as a 'friend' on Facebook for the sole purpose of reviewing photographs and related comments *in camera*" in a case where plaintiff raised privacy concerns about the public dissemination of photographs posted to her Facebook account).

City of Ontario v. Quon

- Whether an employee has a reasonable expectation of privacy in electronic communications is fact-based and will likely depend on the employer's policy.

- The City's general technology usage policy stated that e-mail and Internet usage would be monitored; however, there was an informal policy that supervisors would not audit employees' text messages as long as the employees paid any overage fees.

- Quon brought suit after a supervisor requested transcripts of his messages after noting Quon regularly had overages, even though Quon paid the overage fees. Quon claimed the City violated the Stored Communications Act and Fourth Amendment, among other claims, and the district court agreed.

- The Ninth Circuit reversed and held that users of text messages have a reasonable expectation of privacy in the content of their text messages and that the "operational realities" of the employer created a reasonable expectation of privacy for the employee. *Quon v. Arch Wireless Operating Co.,* 529 F.3d 892, 907 (9th Cir. 2008).

City of Ontario v. Quon

- The Supreme Court reversed on narrow grounds, holding that the City's search of the text messages on the facts of this case was reasonable.

- The Court, however, declined to address employee privacy expectations with respect to employer-provided communications devices, cautioning the judiciary against "elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."

- As the Court explained, "[r]apid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior . . . . At present, it is uncertain how workplace norms, and the law's treatment of them, will evolve."

- While *Quon* does not offer guidance on best practices for technology use and related records management, it does highlight the importance of the employer's policies around technology use.

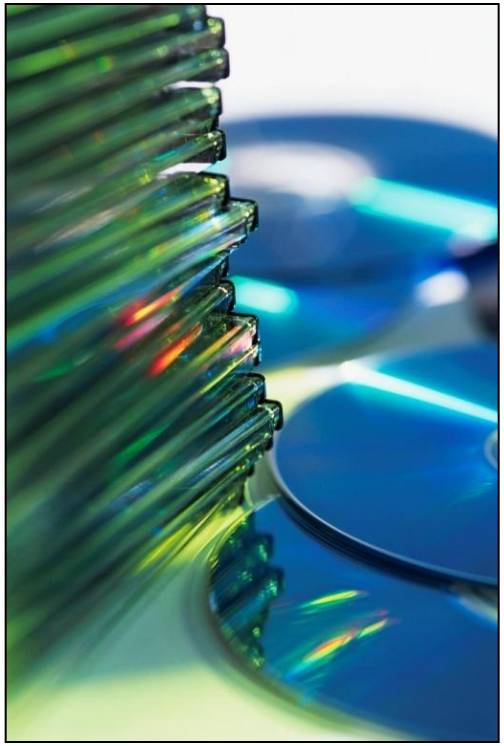
Application of Domestic and International Laws

- Cross-border data transfer compliance (e.g., EU Data Protection Directive)
- Geography / jurisdictions / export law compliance
- Regulated industries (e.g., financial, health, etc.)
- Regulatory / legal compliance by provider

Records Retention

Records retention refers to the length of time a record must be retained to satisfy the purpose for which it was created and to fulfill applicable legal requirements.

While there is no general law governing document retention, there are statutory and regulatory requirements that govern the retention of certain documents in certain industries. There is also a common law duty to preserve records that arises with respect to litigation.



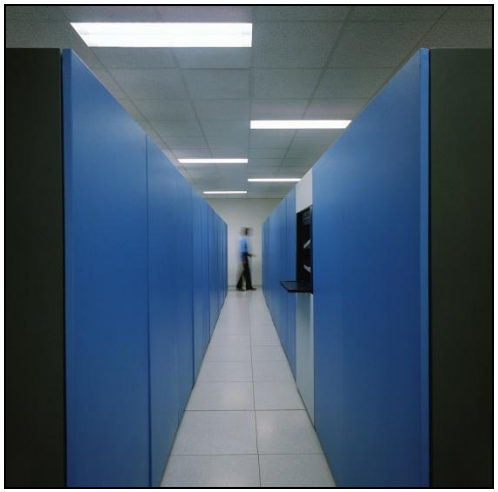
Records Management

- A records retention policy is typically comprised of a schedule setting forth the length of time documents must be retained, a framework for implementing that schedule, and a statement of the company's policy on retention.
- To begin developing a document retention policy it is necessary to understand:
  - what types of records the corporation has;
  - who controls those records;
  - where the records are located;
  - the types of litigation or enforcement action the company can expect; and
  - when the records become obsolete so they can be destroyed.

Records Retention

While it may seem obvious, the first thing that must be done to develop a sound policy is identify the records that are regularly created and/or received by the company. A complete records inventory – which identifies the records, their location, and the format in which they are maintained – is the basis from which the records retention schedule is created.

The failure to account for changing technology in records retention policies represents a significant risk.



Records Management

- 2009 Electronic Records Management Survey, Cohasset Associates & ARMA
  - 78% of respondents reported they do not have retention practices in place for emerging sources of records (voice mail, IM, blogs, Web pages)
- Cloud solutions must consider records management requirements, for example:
  - Can the solution implement records disposition schedules, including the ability to transfer and permanently delete records?
  - Cloud providers or managers may not be able to ensure complete deletion of records
- If particular cloud deployments present insurmountable obstacles to records management, there will be a negative impact on the company's records program.

E-Discovery

- Gartner study: Data increasingly lives in the cloud.
  - Companies are increasingly using cloud-based services for e-mail, word processing, and spreadsheets.
  - These are the three most important targets of discovery and regulatory investigations
- Spoliation occurs where evidence is destroyed or significantly altered when litigation or investigation is pending or reasonably foreseeable.
  - consequences of spoliation can be severe and may include criminal charges, monetary sanctions, dismissal, suppression or exclusion of evidence, or an adverse inference jury instruction.
- Consider:
  - How are document holds enforced and how is data preserved?
  - How is metadata protected?
  - How is Information searched for and retrieved pursuant to e-discovery requirements?
  - How is attorney/client privilege maintained?
- Subpoenas:
  - You may not even know about them if the cloud vendor gets the subpoena
- Cooperation:
  - With the other party…and with your cloud provider

E-Discovery

- F.R.C.P. 34(a)(1):
  - "…produce and permit the requesting party or its representative to inspect, copy, test, or sample the following items in the responding party's possession, custody, or control."
  - Typically, cloud customer is the party in control and cloud service is the party in possession
  - Requesting cloud provider to perform discovery on behalf of customer could present issues regarding attorney/client privilege
  - Without customer consent, potential to impinge upon Stored Communications Act (18 U.S.C. §§ 2701 to 2712)

Flagg v. City of Detroit 2008 WL 787061 (E.D. Mich. 2008)

- Most significant test for cloud-based deployments is control
- Party in control over the data is the one that determines discoverability of data in the cloud
- The third party in possession of data is not required to produce ESI

Crispin v. Audigier (C.D. Cal.) (May 26, 2010)

- Involved postings on Facebook and MySpace
- Judge went to great lengths to explain why the provider is NOT required to produce documents based on the protections offered by the SCA

The Stored Communications Act (SCA)

- Law enacted in 1986.
- It is not a stand-alone law but forms part of the Electronic Communications Privacy Act;
- It is codified as 18 U.S.C. §§ 2701 to 2712.
- The SCA addresses voluntary and compelled disclosure of "stored wire and electronic communications and transactional records" held by third-party internet service providers (ISPs)
- Crime committed by a person who “intentionally accesses without authorization a facility through which an electronic communication service is provided or intentionally exceeds an authorization to access that facility.”
- § 2707 provides for civil action for a person who is aggrieved by violation of the statute

Computer Fraud and Abuse Act Provides Proactive Tool to Protect Data

- Title 18 U.S.C. § 1030 – Enacted in 1984
- Criminal statute
- Civil remedy in 1994 amendment
- Computers used in interstate commerce
- Amended in 2001 and 2008
- Computers in foreign countries
- Provides for damages and injunction

Various Causes of Action

- Stealing valuable computer data
- Schemes to defraud
- Trafficking in a computer password or similar information with intent to defraud
- Damaging computer data
- Hacking
- Extortion
- Sending computer viruses

Legal Requirements

- Protected computer
- Lack of authorization or exceeding authorization to access computer
- Theft of information or anything of value
- Damage to data permanent
- $5,000 loss
- Limited to economic damages
- Compensatory damages
- Two-year statute of limitations

Key Issue: Unauthorized Access

- Section 1030(a)(4) - Whoever knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value…

Authorization Established by Company

- First Circuit: the CFAA "is primarily a statute imposing limits on access and enhancing control by information providers."
- Companies can set predicate for CFAA violation
- Rules on authorized access
- Agreements can set limits
- Similar to criminal trespass

International Airport Centers LLC v. Citrin

- Employee destroyed data on company computer
- Authorization based on law of agency
- Authorization terminates with disloyal act
- Judge Posner found that authorization terminated when employee “resolved to destroy files that incriminated himself and other files that were also the property of his employer.”

LVRC Holdings LLC v. Brekka (9th Cir.)

- Employee emailed to himself competitively sensitive data
- Refused to adopt *Citrin*
- Employee cannot access company computers without authorization because employer gave him permission
- Does not address rules or agreements limiting access

Ways to Establish Lack of Authorization

- Hacking by outsider who breaks into computer
- Exceeds expected norms of intended use
- Terminates agency relationship with employer by disloyal conduct
- Violates company policies and rules
- Breaches contractual obligation

Tort of Conversion

- Tangible v. Intangible property
- *Thyroff v. Nationwide Mutual Insurance Company*, 8 N.Y.3d 283 (2007)
- Computer data included in conversion based on changing societal values
- Similar remedies to the CFAA
- May have advantages over the CFAA

Companies can mitigate their “risk” by re-evaluating 7 areas of their business

1. Hiring Practices
2. Company Rules
3. Appropriate Agreements
4. Use of Technology
5. Termination Practices
6. Protocols for Response
7. Company Compliance Program

Company Rules

- Employee Handbook
- Compliance Code of Conduct
- Terms of Use on company Web site
- Training
- International rules

Terms of Use

- Require users to provide accurate registration information
- Limit use of account to registered user at one computer at a time
- Prohibit use of web crawlers, robots and similar devices
- Post acceptable use guidelines that prohibit abuse, harassment and similar conduct
- Specify limitations on use of materials obtained (e.g., no commercial use)

Agreements

- Officers/Employees/Third Parties
- Among related companies
- Confidentiality/Non-Disclosure
- Post employment restrictive covenants
- Anti-Raiding Covenants
- Agreement to search personal computers
- Permissions re use of the computers
- Customer agreements
- Data vendor agreements

Use of Technology

- Password protection is simplest
- Access based on need to know
- Risks re transportable media
- Encryption
- Audit trail
- Coordinating with document retention and e-discovery

The Termination Process

- Employees must return all company property
- Standard Exit Interview Form
- Explain post employment obligations
- Retain evidence

Protocols for Response

- Speed is of the essence
- Designate a coordinator
- Be investigative ready
- Be prepared to memorialize actions
- Notify law enforcement
- Prepare standard court papers with company policies and agreements

Cloud Contracts: Approach

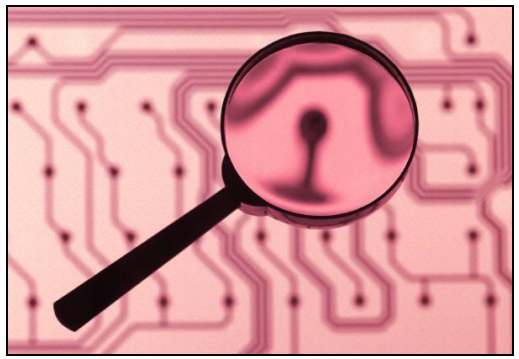
- IT, legal/compliance, privacy and business/management and other functional areas should work together
- Determine position on issues and develop contract language for this

Cloud Contracts: Provisions

- Protection of data
- Control by customer over data
- Provider control over data
- Responsibilities of provider and customer
- Indemnification, limitation of liability/exceptions and consequential damage disclaimers
- Pricing, business continuity, termination, service level, compliance, litigation/e-discovery and auditing/security
- Relationships
  - Incident response/contingency plans
  - Data breach
  - Controls to prevent data breach, security and controls
- Data preservation and electronic discovery
  - Service level agreements
  - Handling of failures

Cloud Contracts: Due Diligence

- Consider more than one provider
  - Financial strength of provider
  - Insurance coverage of provider
  - What happens if merger or acquisition or bankruptcy involving provider?
  - Has provider had a security breach?
  - Who is data processor? Subcontractor?
  - Provider's privacy and related policies, procedures and requirements
  - Customer's privacy and related policies, procedures and requirements



Snap-On Business Solutions, Inc. v. O'Neil & Associates

- Snap-On and Mitsubishi entered into a license agreement whereby both contributed to electronic auto database
- Mitsubishi approached O'Neil two years into contract to replace Snap-On
- O'Neil used robot to copy database
- Issue: Was O'Neil authorized to access the database?

State Data Compliance Statutes for Personal Data

- **Nevada** – personal information must be encrypted when it is transferred – effective October 1, 2008
- **Connecticut** – businesses must "safeguard the data, computer files and documents containing the information from misuse by third parties." – effective October 1, 2008
- **Massachusetts** Data Compliance rules effective March 1, 2010
  - Applies to a business located anywhere that stores or maintains personal information about a Massachusetts resident
  - Mandates a compliance program consistent with the Federal Sentencing Guidelines
- **Washington State** – personal information encrypted effective July 1, 2010

Massachusetts – Administrative, Technical and Physical Safeguards

- Develop Security Policies that are enforced through encryption
- Appoint Security Coordinator
- Minimize risks from third parties terminated access to former employees and ensuring compliance by vendors
- Train the workforce on importance of personal information security
- Conduct regular audits at least annually
- Enforce the policies through disciplinary measures and document responsive actions
- Respond to incidents encouraging employees to report violations

Best Practices & E-Discovery

- Data can be stored in any country
  - Know where the data center is located, as the physical question raises the question of legal governance over the data
  - Address which country's court system will settle a dispute in event of a conflict between the cloud vendor and customer
  - Be aware of the prevailing law in that particular nation.
    - For example, German law will not allow documents to leave Germany if your client is the government. How would you adhere to these requirements in a cloud scenario?
    - The European Network and Information Security Agency - November 2009 report on cloud computing - warns companies remain responsible under UK law for safeguarding their customers' information even if that data is stored by a service provider in the cloud.
    - Intellectual property protection

Best Practices & E-Discovery

- Ensure process regarding third-party access to stored data
- The agreement with the provider must contemplate everything involved with e-discovery: Notices upon service of process, procedures for receiving discovery requests, protocols for communication and data transfer between litigating attorneys and service provider personnel, pricing, etc.

Best Practices: Records Management

- Define a Cloud Governance Program and train your staff regarding its contents
- Have Records Management staff review the cloud provider contract around a security model for preservation of data that includes communication, collaboration, infrastructure, and the application platform
  - Ensure your cloud provider agreement guarantees data recovery and assured destruction of data
  - State explicitly in the contract information ownership and control amongst parties
- Solid records management policies and data governance practices set instructions to capture, manage, and retain records; address how data will migrate to new formats and operating systems; address how to transfer permanent records in the cloud to the records authority; and create a framework for portability and accessibility issues.
- Determine which copies of records will be declared as the record copy and manage these in accordance with judicial records management content. Remember, the value of records in the cloud may be greater than the value of the other set because of indexing or other reasons.

Thank You!

Questions?

Nick Akerman
Partner, Dorsey & Whitney LLP