Legal Considerations of Cloud Computing

SC GMIS/PMI Charleston

April 9-11, 2012

COLLINS & BURKETT
LAW FIRM, LLC

Margaret A. Collins
Collins & Burkett Law Firm, LLC
1087 Harbor Drive, Suite B
West Columbia, SC 29169
(803) 708-7442

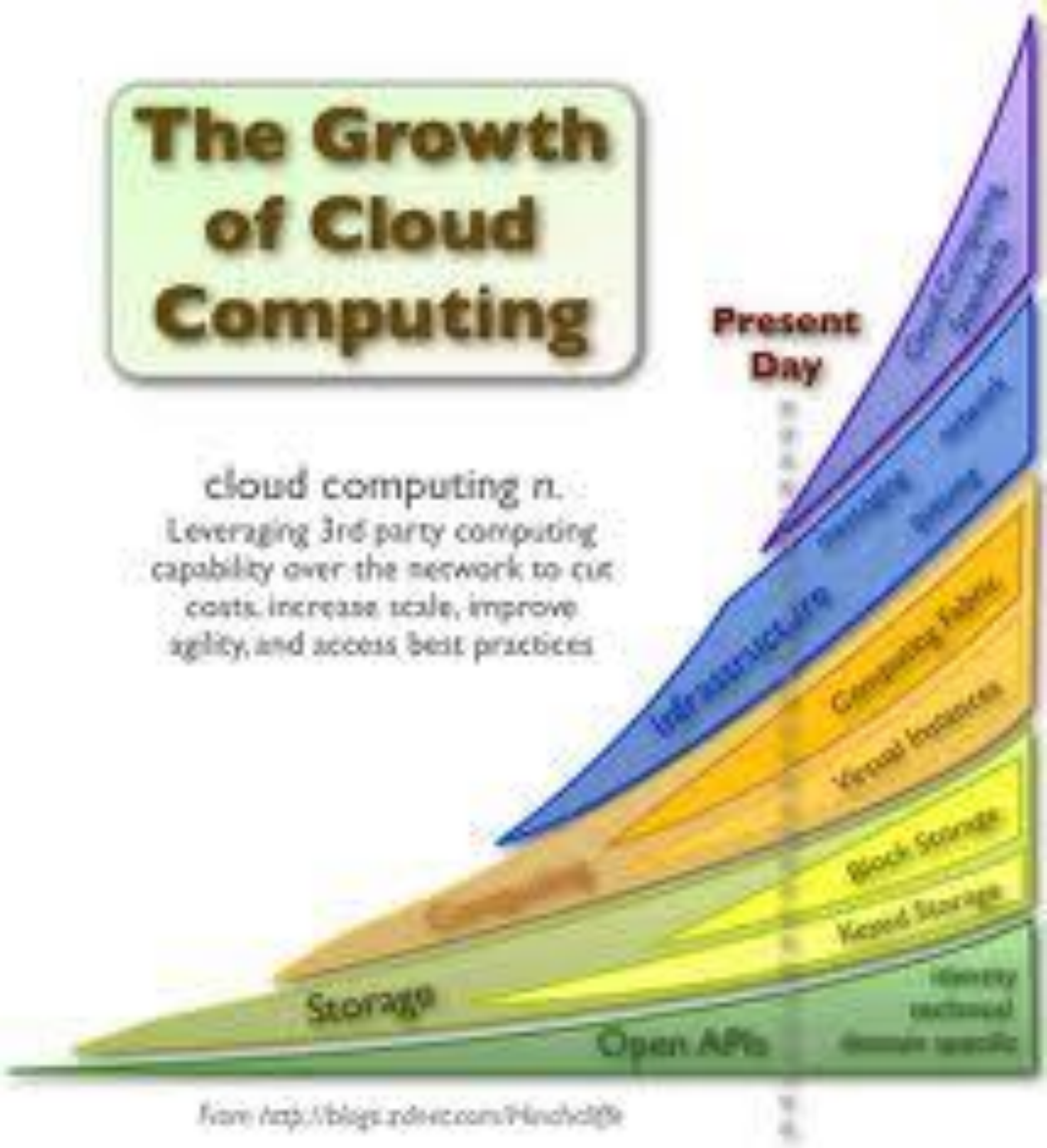
No legal advice provided . . .

THIS PRESENTATION IS TO ASSIST IN A GENERAL UNDERSTANDING OF THE LEGAL ISSUES SURROUNDING CLOUD COMPUTING. IT IS NOT INTENDED, NOR SHOULD IT BE REGARDED, AS LEGAL ADVICE. COMPANIES, ENTITIES OR INDIVIDUALS CONTEMPLATING ENTRY INTO OR USE OF A CLOUD COMPUTING APPLICATION/CONTRACT OR HAVING PARTICULAR QUESTIONS SHOULD SEEK THE ADVICE OF INDIVIDUAL COUNSEL

CLOUD COMPUTING:

Key Points

- Released/migrated with minimal management effort and cost.
- Does not require end-user knowledge of the physical location and configuration
- Not in a specified, known or static place(s)



The Growth of Cloud Computing

cloud computing n.
Leveraging 3rd party computing capability over the network to cut costs, increase scale, improve agility, and access best practices

From http://blogs.zdnet.com/Hinchcliffe

Risk/Benefit Overview:

Benefits:

- Large infrastructure w/o up-front investment; Cost savings; Flexibility & Scalability, etc.

Risks:

- Data Loss/Breach
- Location Uncertain=> Duty Uncertain
- Privacy Issues
- Quality and Level of Service Uncertain
- Negotiability of Terms of Service
- Amendment of Terms, Termination & Recovery of Data
- IP Protection/Confidentiality/Compliance Issues
- Limitations of liability, damages and remedies

Partial Legal Checklist

Data Losses and Breaches

Risk Allocation/Liability

Data Retention Issues

Regulatory & Statutory Compliance

Control (e.g. physical location/configuration)

Financial Viability/Liability of Vendor(s)

E-discovery Concerns

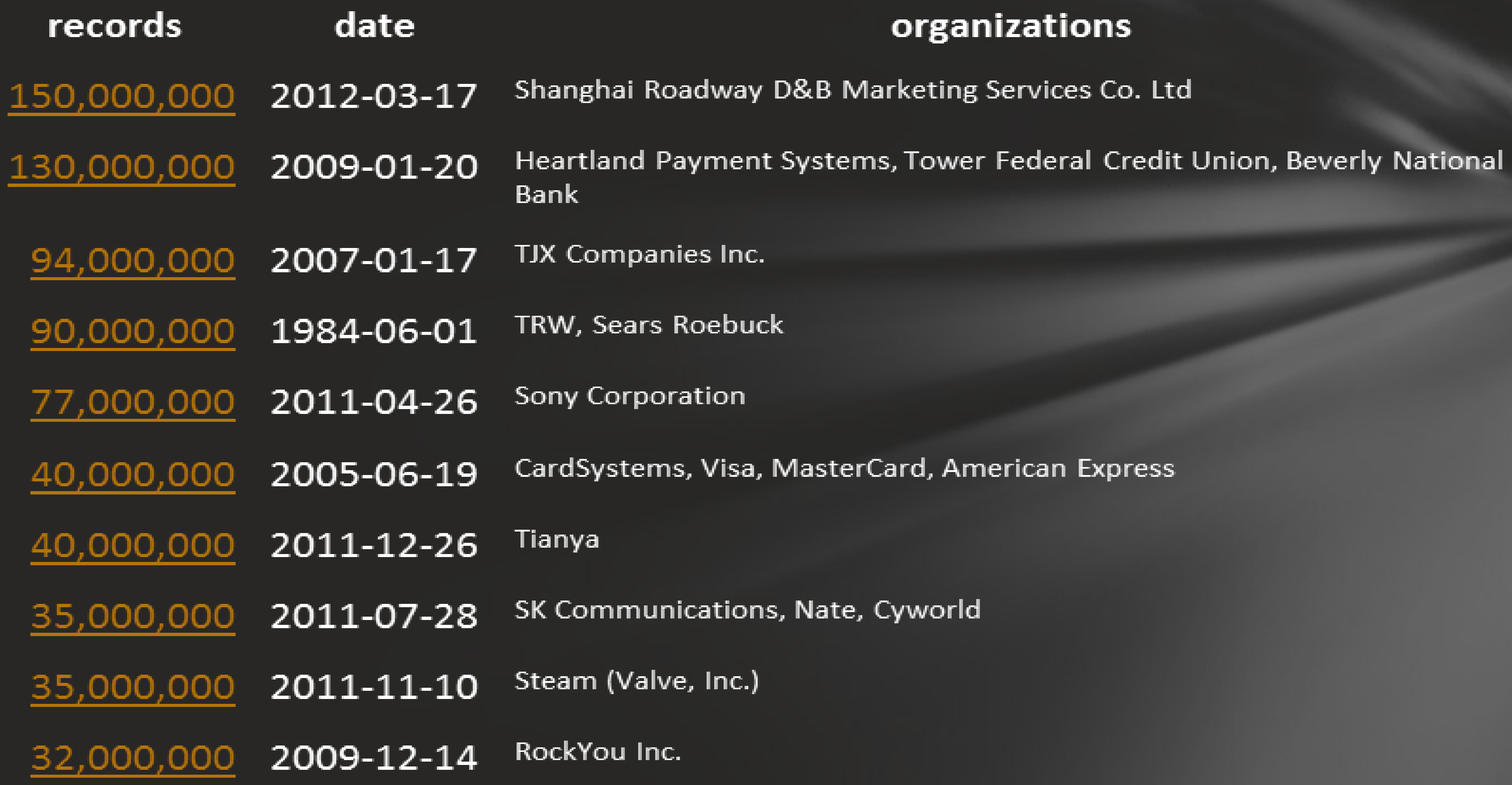
IPR/Trade Secret issues

Recent Data Losses/Breaches

records	date	organizations
12	2012-04-04	Globovision
119	2012-04-04	Viajar10.com
442	2012-04-04	Baylor Law School
24,000	2012-04-04	Utah Department of Health
0	2012-04-03	Unknown Organization, Victoria Fire Dept.
92	2012-04-03	Abundant Organics
33	2012-04-03	Bunkerhosting.de
16	2012-04-03	Provincial Government of Riaud
300	2012-04-02	Glenwood IGA
4,577	2012-04-02	Thai4promotion.com

Source: www.datalossdb.org

Data Loss: Largest



records	date	organizations
150,000,000	2012-03-17	Shanghai Roadway D&B Marketing Services Co. Ltd
130,000,000	2009-01-20	Heartland Payment Systems, Tower Federal Credit Union, Beverly National Bank
94,000,000	2007-01-17	TJX Companies Inc.
90,000,000	1984-06-01	TRW, Sears Roebuck
77,000,000	2011-04-26	Sony Corporation
40,000,000	2005-06-19	CardSystems, Visa, MasterCard, American Express
40,000,000	2011-12-26	Tianya
35,000,000	2011-07-28	SK Communications, Nate, Cyworld
35,000,000	2011-11-10	Steam (Valve, Inc.)
32,000,000	2009-12-14	RockYou Inc.

Source: www.datalossdb.org

Data Breach Headlines:

Lost Data May Have Exposed 800,000 People in California March 30, 2012 - *NPR*
"A disaster preparedness exercise to ensure California's child support system could be run remotely went smoothly, except for one casualty: the names, Social Security numbers and other private records of about 800,000 adults and children were released."

Report: 25 percent admit to at least one breach in past year. 11/10/11-*CSO*
Forrester Research surveyed over 2,300 IT execs in Canada, France, Germany, the UK, and the US. Twenty-five percent admitted they suffered a security breach in the past year.

MasterCard, Visa Warn of Processor Breach
March 30, 2012 - *Krebs on Security*
"VISA and MasterCard are alerting banks across the country about a recent major breach at a U.S.-based credit card processor. Sources in the financial sector are calling the breach “massive,” and say it may involve more than 10 million compromised card numbers."

Examples of Liabilities for Breaches:

Heartland (Credit Card Processor) $139.4M

- $60M Fine to Visa; $26M Legal Fees; $42.9M for future settlements; Plus investigation costs

Veteran's Administration: Laptop stolen after employee breach of protocol (not direct cloud issue, but what about "cookie access"? Notice governmental liability, too.)

- $20M to settle 5 class actions
- Note: FBI recovered laptop and no theft of information

Sutter Health (based on California's Data Security Statute)

- Class Action seeks $1,000 per person statutory damages=$943M

Sony Computer (PlayStation hack of up to 100 million individuals)

- Class actions alleges 1 week to notify affected parties unreasonable (77M)

Dropbox - Lesson learned: make sure privacy policy matches practice.

Cross Jurisdiction Issues

Inherently "stateless"

- Conflict of laws and jurisdictional confusion.
- Additional obligations potentially triggered based on residency (vendor, data owner or subject of data)

Privacy and Security Compliance

- Who "owns" the data? How can it be used?
- What laws apply?
- Do the cloud provider's practices, policies and systems comply with all applicable laws?
- Who has the obligation to incur the additional expense to comply? For failing to comply?

Legal Standard/Duty:

Federal:

- Financial: GLBA; Medical: HIPAA, etc.
- Other Industries taking online payments: PCI-DSS (Payments Application Data Security Standard) may become statutory duty in the near future.

Federal and State (1) Deceptive/Unfair Trade Practices Acts

(2) Common Law Breach of Fid. Duty/Contract, etc

States:

Most States have independent state privacy laws. (AK, AZ, CA, DE, FL, GA, HA, IL, KY, LA, MA, ME, MO, NC, NE, NV, NY, OK, PA, SC, TN, TX, VA, VI, VT, UT, WA, WI, WY, WV, and expanding fast.)

- Similar, but not the same statutory language.
- Not interpreted similarly. (e.g. CA – ZIP Code is PII)

South Carolina Law:

SC CODE § 39-1-90; Effective Date: July 1, 2009

I. Definition of Personal Information: The first name or first initial and last name plus 1 of the following:

(a) Social security number;
(b) Driver’s license or state identification number;
(c) Financial account number, or credit card or debit card number in combination with any required security code, access code, or password that would permit access to a resident's financial account; or
(d) Other numbers or information which may be used to access a person's financial accounts or numbers or information issued by a governmental or regulatory entity that uniquely will identify an individual.

II. Summary: A person conducting business in this State, and owning or licensing computerized data or other data that includes personal identifying information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of this State whose personal identifying information that was not rendered unusable through encryption, redaction, or other methods was, or is reasonably believed to have been, acquired by an unauthorized person when the illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the resident. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or with measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

South Carolina Penalties:

A resident of this State who is injured by a violation of this section, in addition to and cumulative of all other rights and remedies available at law, may:

(1) institute a civil action to recover damages in case of a willful and knowing violation;

(2) institute a civil action that must be limited to actual damages resulting from a violation in case of a negligent violation of this section;

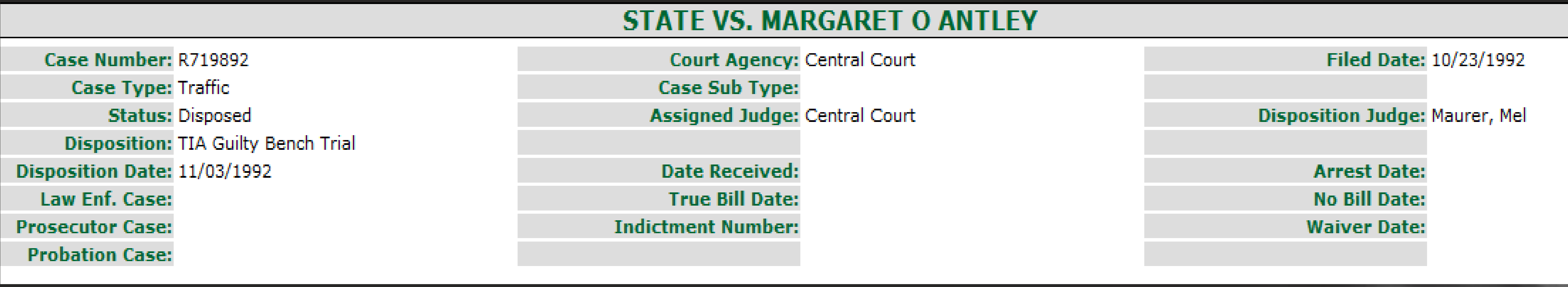
(3) seek an injunction to enforce compliance; and

(4) recover *attorney's fees and court costs*, if successful.

Fed’s Definition of PII:

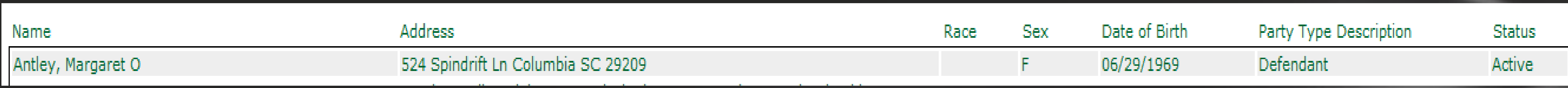
Information which can be used to distinguish or trace an individual's identity, such as their name, address, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.

NIST Special Pub. 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information

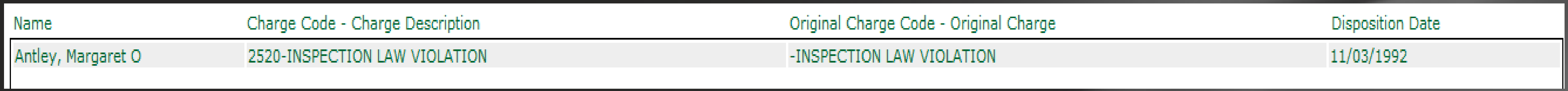


STATE VS. MARGARET O ANTLEY

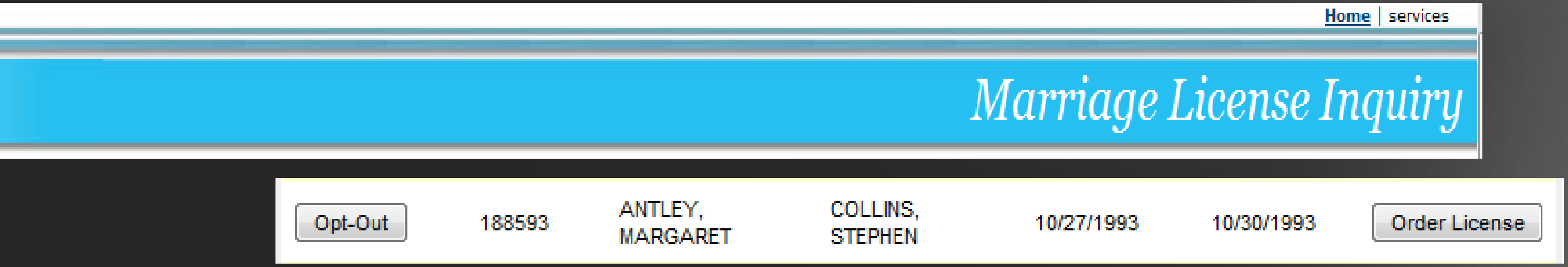
Case Number:	R719892	**Court Agency:**	Central Court	**Filed Date:**	10/23/1992
Case Type:	Traffic	**Case Sub Type:**			
Status:	Disposed	**Assigned Judge:**	Central Court	**Disposition Judge:**	Maurer, Mel
Disposition:	TIA Guilty Bench Trial				
Disposition Date:	11/03/1992	**Date Received:**		**Arrest Date:**	
Law Enf. Case:		**True Bill Date:**		**No Bill Date:**	
Prosecutor Case:		**Indictment Number:**		**Waiver Date:**	
Probation Case:					



Name	Address	Race	Sex	Date of Birth	Party Type Description	Status
Antley, Margaret O	524 Spindrift Ln Columbia SC 29209		F	06/29/1969	Defendant	Active



Name	Charge Code - Charge Description	Original Charge Code - Original Charge	Disposition Date
Antley, Margaret O	2520-INSPECTION LAW VIOLATION	-INSPECTION LAW VIOLATION	11/03/1992



Marriage License Inquiry

Opt-Out	188593	ANTLEY, MARGARET	COLLINS, STEPHEN	10/27/1993	10/30/1993	Order License

New Trend in Litigation

Courts have begun to consider data breach litigation in the same light as some types of tort litigation. Incubation between disclosure and actual damages may be up to 2 years for data breach. No present harm, but future harm may be actionable – similar to asbestos cases. The test is whether or not future damage is “reasonably foreseeable” . . . See Anderson v. Hannaford Bros., No. 10-2384 and 10-2450 (1st Cir., Oct. 20, 2011)

So we may be looking at more liability. But, who may be liable? The Service Agreement is critical.

Issues with Service Agreements

- Standard mass market contracting terms are used
- Non-negotiable (often click through)
- Little or no opportunity to conduct due diligence
- Strong limits on liability (including direct liability)
- Terms often subject to change with little or no notice
- Risk is generally shifted to user through provider friendly agreements
- Unknown Subcontractors/Providers

YOUR terms of service. ..

- Were they negotiated? Were your contract specialists and legal team involved? Or, was it a click-through by a developer/end-user?
- Do you even know about all of the agreements? Who is authorized to enter into these agreements? Since no software is installed, are there restrictions/obligations on usage?
- What exactly is being purchased? How is this treated under your procurement and software policy procedures?
- Does the cloud provider use third party vendors/subs? Contractual obligations of subs? Performance assurances of subs?

You may need to start with internal procurement, procedures and policy modifications. Then, work your way out to the contract, then the cloud vendor practices.

What isn’t in the Contract: Privacy and Security

Multi-tenant architecture:

- Data from different users are usually stored on a single virtual server.
- Multiple virtual servers run on a single physical server.

Data security depends upon the integrity of the virtualization.

. . . . . . Better or worse than in-house?

Contract Provision Examples:

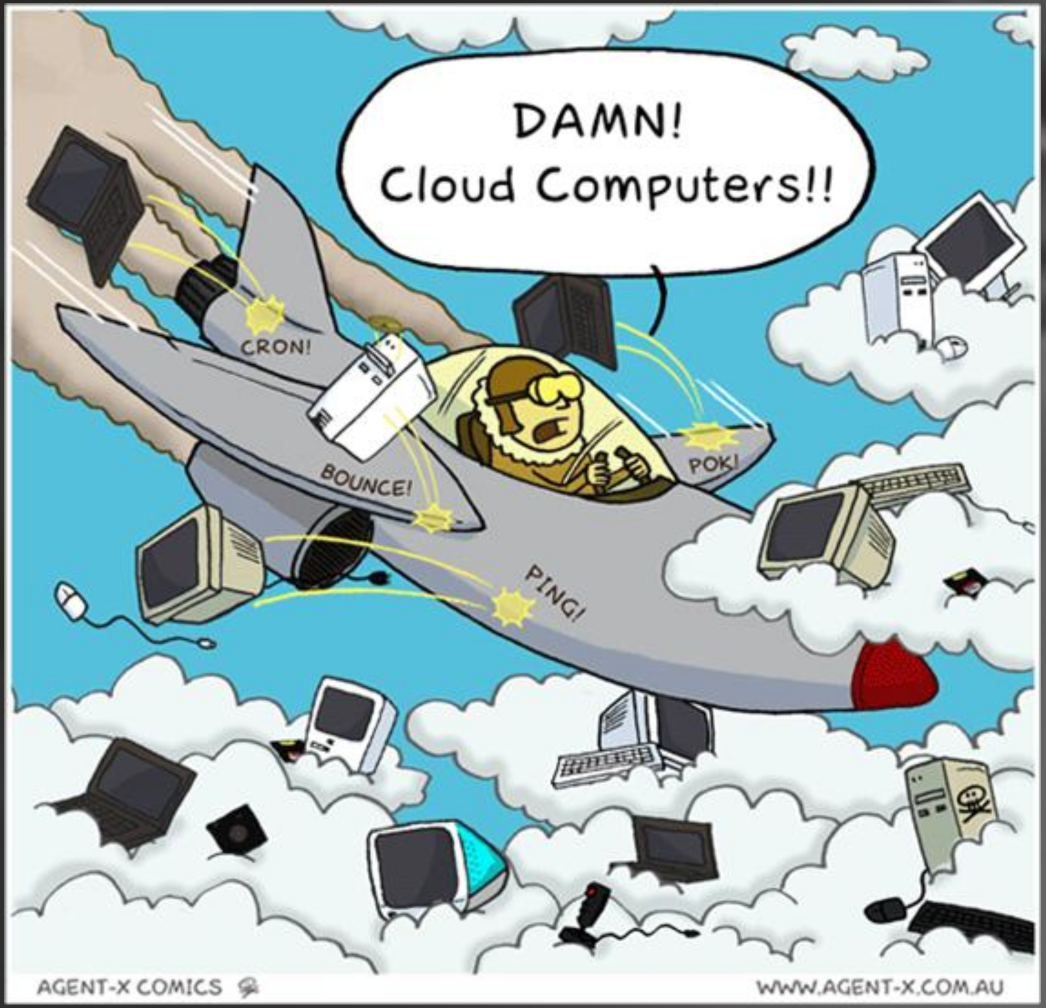
Limitation of Liability:

We and our licensors ***shall not be responsible for any service interruptions****, including, without limitation, power outages, system failures or other interruptions, including those that affect the receipt, processing, acceptance, completion or settlement of any services. (...)*

Contract Provision Examples:

Limitation of Damages:

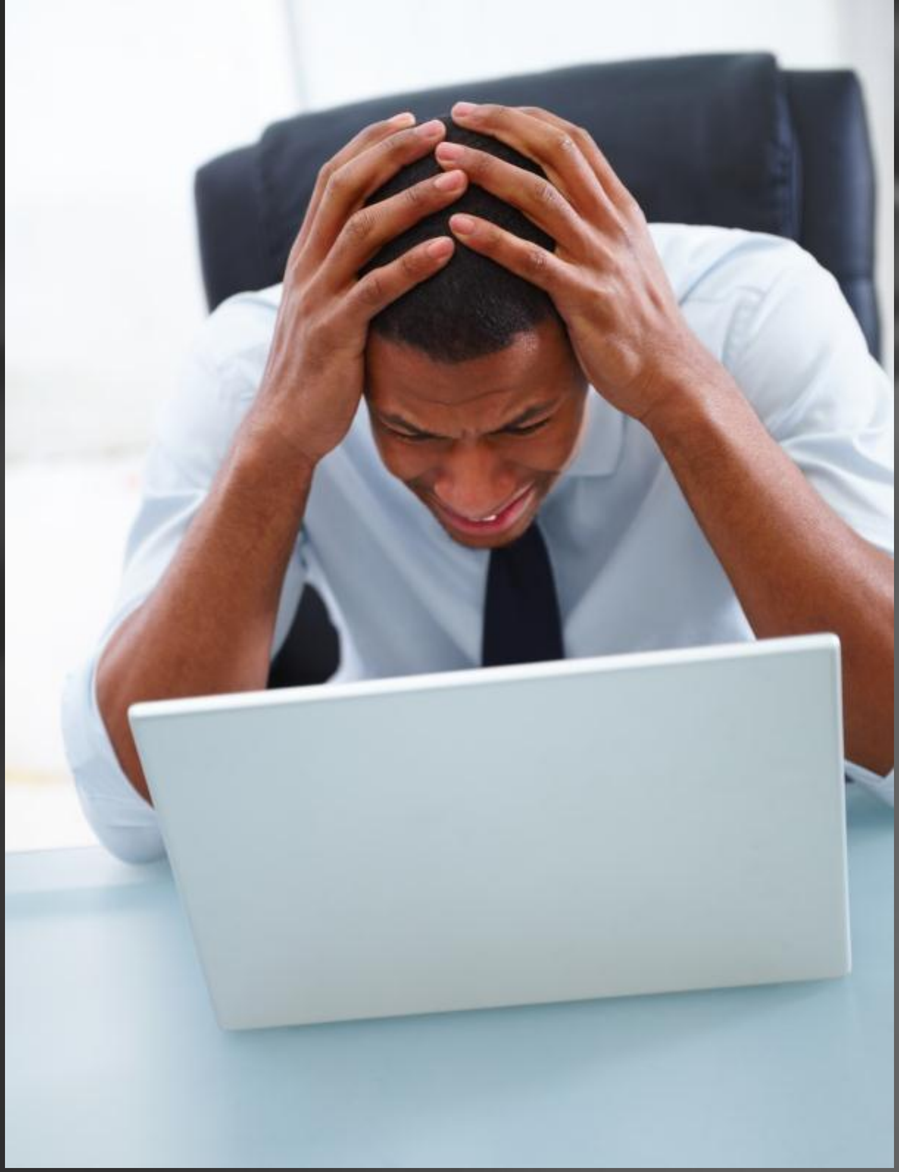
Neither we nor any of our licensors ***shall be liable to you for any direct, indirect, incidental, special, consequential or exemplary damages****, including, but not limited to, damages for loss of profits, goodwill, use, data or other losses (...)*



Contract Provision Examples:

Limitation of Remedies:

…liability is strictly limited to a ***refund of the pro rata portion of the subscription fee*** *for the time in which there was substantial noncompliance of our obligations hereunder. . .*



Cloud vendor liabilities & obligations

- If cloud vendor is hacked, does the data owner have the right to seek its losses from the vendor?
- Consider the same for breaches/failures in regulatory compliance or wrongful disclosures by the vendor.
- What are the vendor’s notification obligations?

Key Contract Terms to Consider:

Preventative Contract Terms to consider:

–Maintain Personally Identifiable Information in strict confidence

–Use PII only for customer's benefit

–Comply with all applicable laws, industry standards and customer's privacy policies

–Develop, implement and maintain reasonable security procedures to protect PII from unauthorized access, destruction, use, modification and disclosure

–"Reasonable security" – Is the security implemented "*legally defensible*"?

–Controls in place to prevent data breach

–-Audit and Enforcement Terms

–Require that customer retain the right to monitor vendor's compliance

–Non-compliance reporting

–Credits/damages

-Incident Response Contract Terms

-Risk of Loss Contract Terms

Electronic Discovery Issues

- “Searchability” and availability of data in the cloud
- Forensic assessment (identifying, collecting and preserving data) in cloud context (Exactly where IS that drive located that needs to be mirrored?)
- Electronic evidence: data integrity issues; authenticating/proving up documents/data for submission of evidence
- Metadata

Audit Trail

Who, What, When Where, Why and How:

Client should have the right to know where and by whom its data is stored, accessed, transferred and altered.

Confirm whether the vendor provides.

Critical for regulated industries and those prone to e-discovery.

NOISE TO SIGNAL
Rob Cottingham - socialsignal.com/n2s

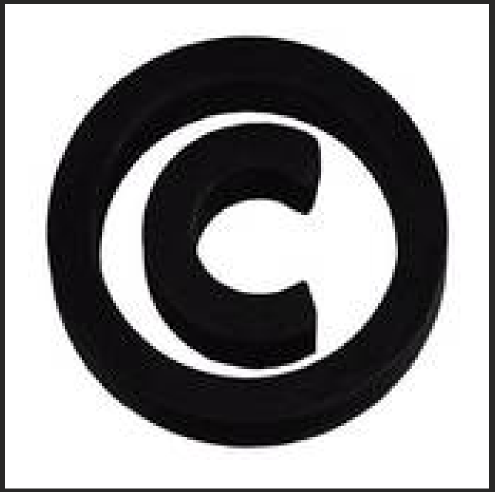
At last, the fossil evidence to prove our theory! The dinosaurs died off – not because of a meteor or climate change – but because their cloud computing platform collapsed!

IPR and Ownership Issues

Trade Secret Protection. Third parties access may affect trade secrets and IP rights of a company.

- Should have confidentiality & NDA with the vendor
  - includes subcontractors, all licensors, contractors, employees, agents and everyone having access or right to access the data.

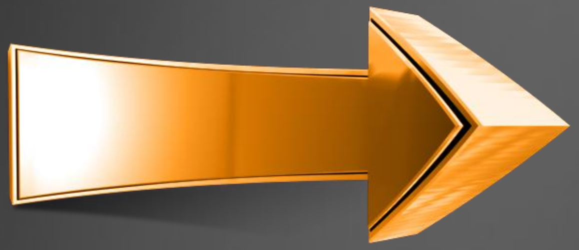
Ensure that no rights (even a license) in IP are transferred to the vendor. . . Even better: (1) the data owner is granted all actual and potential IP's; and (2) vendor, et al. agree to provide any and all necessary assignments to perfect such IPR's.



Exit Issues:

Upon exit, consider:

- portability and interoperability.
- can the records be successfully accessed?
- Can the data be used in another platform?
- Can data be extracted from the cloud? Does it include all data (e.g. metadata)? E-discovery anticipation is critical for exit strategy.
- Obligations of each party in case of exit. (Is the sensitive data wiped?)
- Data retention policies carried out?
- Upholding confidentiality obligations you have to others?
- How quickly can you get a replacement up and running?



War Stories

The “Christmas” rush and property tax bills

- Auditor’s tax bills late due to “Black Friday”

The “Subletting of the Cloud” – who is your vendor?

- Effect: small company’s storage (email archive) ***and backup*** were gone. Who, if anyone, is liable?

Shared Server Hacked – Server shut down

- Effects? Boston University was unable to grant students access to financial aid, registration, email, etc. for weeks.

The out-of-state customer

- CA Supreme Ct. held that Zips considered Personally Identifiable Information

The “accidental delete” (loss of data)

War Stories II

“Dropbox” lack of notification for cloud breaches.

Los Angeles’ completion of a rollout to Google Apps is a year late.

- Google: LA contracted with Google Apps to meet certain public safety requirements that were incorporated by reference . . . Late performance.
  - Google’s Response “Those requirements weren't . . . in the original contract and led to delays. . .Many security standards for government systems were designed before cloud computing," Google said. "It's not to say in trying to meet these standards that Google Apps is not secure, but it takes more work to make it compliant."

Recommendations/Takeaways

Internal:

1. Consider all stakeholder’s authority and procurement practices.

2. Carry over all policies for access/password/records retention/security/policies and procedures to cloud vendors and subs.

3. Consider IP and sensitive data (PII) protections – prohibit/limit/regulate use of cloud for sensitive matters?

Recommendations/Takeaways

External:

1. Understand vendor’s contractual responsibilities and limitations.

2. Plan for both expected and unexpected termination and for an orderly return or secure disposal of assets. Consider all possibilities: mergers; patent trolls; bankruptcy, etc.

3. Pre-contract due diligence: contract term negotiation, notification and audit rights, post-contract monitoring, contract termination, and the transition of data custodianship.

4. Keep informed of the applicable legal environments. Keep apprised of ever-changing standards and norms – is your practice “legally defendable?”

Recommendations/Takeaways

- Know location and subject/content of data, as well as all regs.
- Address ownership of its data in its original, authenticable and portable format.
- NDA’s & confidentiality *prior to upload* to protect IP.
- Address and consider all security issues - data breaches, notification requirements, liability, interruption in access, etc.
- Address monitoring and audit procedures, as well as regular testing for vulnerabilities.
- Perform complete portability and disaster recovery analysis.
- Involve Business, Legal and Technical Teams.

Summary of Recommendations:

DUE DILIGENCE

DUE DILIGENCE

DUE DILIGENCE

DUE DILIGENCE

Case Study:

Google App Engine:

Terms of Service

Google App Engine : Terms of Service

1.2. In order to use the Service, you must first agree to the Terms. You can agree to the Terms by actually using the Service. You understand and agree that Google will treat your use of the Service as acceptance of the Terms from that point onwards.

. . . . .

Google App Engine Terms of Service

3. Service Policies and Privacy

3.1. You agree to comply with the Google App Engine Program Policies included available at http://code.google.com/appengine/program_policies.html (or such URL as Google may provide) (the "Program Policies") which is incorporated herein by this reference and which may be updated from time to time.

Google App Engine Terms of Service

3.2. The Service shall be subject to the privacy policy for the Service available at http://www.google.com/intl/en/privacypolicy.html (or such URL as Google may provide), which references and incorporates Google's privacy policy available at http://www.google.com/intl/en/privacypolicy.html. You agree to the use of your data in accordance with Google's privacy policies

Google App Engine Terms of Service

3.3. You agree that you will protect the privacy and legal rights of the users of your application. You must provide legally adequate privacy notice and protection for those users. To do so, at a minimum, you must incorporate the privacy terms available at http://code.google.com/appengine/privacy.html into the privacy policy for your application. If the users provide you with user names, passwords, or other login information or personal information, you must make the users aware that the information will be available to your application and to Google. . . .

Google App Engine Terms of Service

4. **Fees for Use of the Service . . .**

4.2. A bill will be issued …., effecting payment to Google and servicing your account. Google may also provide information in response to valid legal process, such as subpoenas, search warrants and court orders, or to establish or exercise its legal rights or defend against legal claims. Google shall not be liable for any use or disclosure of such information by such third parties. Google reserves the right to discontinue the provision of the Service to you for any late payments. . . .

Google App Engine Terms of Service

5.2. Google reserves the right (but shall have no obligation) to pre-screen, review, flag, filter, modify, refuse or remove any or all Content from the Service. You agree to immediately take down any Content …. In the event that you elect not to comply with a request from Google to take down certain Content, Google reserves the right to directly take down such Content or to disable the Application. . . . .

Google App Engine Terms of Service

5.4. You agree that you are solely responsible for (and that Google has no responsibility to you or to any third party for) the Application or any Content that you create, transmit or display while using the Service and for the consequences of your actions (including any loss or damage which Google may suffer) by doing so.

5.5. You agree that ***Google has no responsibility or liability*** for the deletion or failure to store any Content and other communications maintained or transmitted through use of the Service. You further acknowledge that you are solely responsible for securing and backing up your Application and any Content.

Google App Engine Terms of Service

6. Proprietary Rights

. . . 6.3. Except as provided in Section 8, Google acknowledges and agrees that it obtains no right, title or interest from you (or your licensors) under these Terms in or to any Content or the Application that you create, submit, post, transmit or display on, or through, the Service, including any intellectual property rights which subsist in that Content and the Application (whether those rights happen to be registered or not, and wherever in the world those rights may exist). Unless you have agreed otherwise in writing with Google, you agree that you are responsible for protecting and enforcing those rights and that Google has no obligation to do so on your behalf. . . .

.

Google App Engine Terms of Service

8. License from You

8.1. Google claims no ownership or control over any Content or Application. You retain copyright and any other rights you already hold in the Content and/or Application, and you are responsible for protecting those rights, as appropriate. By submitting, posting or displaying the Content on or through the Service you give Google a worldwide, royalty-free, and non-exclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute such Content for the sole purpose of enabling Google to provide you with the Service in accordance with its privacy policy. Furthermore, by creating an Application through use of the Service, you give Google a worldwide, royalty-free, and non-exclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute such Application for the sole purpose of enabling Google to provide you with the Service in accordance with its privacy policy.

8. License from You

8.2. You agree that Google, in its sole discretion, may use your trade names, trademarks, service marks, logos, domain names and other distinctive brand features in presentations, marketing materials, customer lists, financial reports and Web site listings (including links to your website) for the purpose of advertising or publicizing your use of the Service.

. . . . .

Google Apps Engine - Excerpts from Privacy Policy:

Information sharing

Google only shares personal information with other companies or individuals outside of Google in the following limited circumstances:

. . . .

We have a good faith belief that access, use, preservation or disclosure of such information is reasonably necessary to (a) satisfy any applicable law, regulation, legal process or enforceable governmental request, (b) enforce applicable Terms of Service, including investigation of potential violations thereof, (c) detect, prevent, or otherwise address fraud, security or technical issues, or (d) protect against harm to the rights, property or safety of Google, its users or the public as required or permitted by law. . . .

Changes to this Privacy Policy

Please note that this Privacy Policy may change from time to time.

Helpful Resources

Bradshaw, Millard & Walden, *The Terms They are a-Changin' . . . Watching Cloud Contracts Take Shape*, 7 Issues in Technology Innovation, 1 (March 2011)

ID Experts Corp: Top 11 Trends for 2012 in Healthcare Data, According to Industry Experts**,** **http://www.prnewswire.com/news-releases/top-11-trends-for-2012-in-healthcare-data-according-to-industry-experts-136731208.html**

On privacy concerns in cloud computing, see Robert Gellman, Privacy in the clouds: Risks to privacy and confidentiality from cloud computing (World Privacy Forum, 23 February 2009), and Centre for Commercial Law Studies focuses on certain key aspects of the 1995 EU Data Protection Directive ('DPD'). The DPD is relevant even to non-EU entities because of its potentially-broad reach.

Mann, Milne and Morain, *Visible Ops, Private Cloud: From Virtualization to Private Cloud in 4 Practical Steps*, IT Process Institute, 2011. (See also *Visible Ops Security* and *Visible Ops Handbook*)

Mimosa, Michael, *Cloud Computing Legal Issues*, http://searchsecurity.techtarget.com/magazineContent/Cloud-computing-legal-issues

For a recent analysis of class action suits for virtual privacy cases: Ballon and Mantell. *Cloud Litigation: Suing over Data Privacy and Behavioral Advertising, http://centurycitybar.com/newslettertemplate/Sept11/article2.htm, September 2011.*

Cloud Computing Legal Issues Seminar, The Info Law Group, video: http://www.youtube.com/watch?v=YzVLatUEILY; Deck: https://www.issa.org/images/upload/files/2011%20Conf%20Deck%20Cloud%20Computing%20Legal%20Risk%20and%20Liability.pdf

Legal Considerations of Cloud Computing

Please contact me for more information or questions . . .

Meg@cb-lawsc.com

COLLINS & BURKETT
LAW FIRM, LLC

Margaret A. Collins, Attorney
Collins & Burkett Law Firm, LLC
1087 Harbor Drive, Suite B
West Columbia, SC 29169
(803) 708-7442

SC GMIS