

Nelson Mullins

Legal Information Risk Management

For the ACC Columbia Chapter, May 13, 2011

Jon Neiditz jon.neiditz@nelsonmullins.com 404-322-6139

John Martin john.martin@nelsonmullins.com 803-255-9241

James Epstein James.Epstein@reachsmart.com 803-404-1314

Agenda

1. Pandora's Archive: The Risks of Technology Making Information More Accessible
2. Cloud Computing, E-Signatures, Contractual Protections, Legal Ethics and Creating a Program



"Big Data" and Its Custodian (You)

- In 2010 the digital universe reached 1.2 million petabytes.
- IDC expects this volume to grow 44-fold in the next 10 years, the equivalent of a stack of DVDs reaching halfway to Mars.
- Corporate counsel will get more than its fair share of these 53 million petabytes.
 - In 2009, IDC estimated that although individuals still created more than 70 percent of digital information, enterprises eventually ended up with the responsibility— or liability—for 85 percent of it.

Pandora's Archive

The Risks of Technology Making Information More Accessible

I. Backup Tapes

- Long considered "inaccessible" and burdensome under the Discovery Rules (subject to caveats). *See, e.g., Zubulake v. UBS Warburg LLC*, 220 FRD 212, 217 (S.D.N.Y. 2003) ("As a general rule . . . a party need not preserve all backup tapes even when it reasonably anticipates litigation.").
- Two Exceptions:
 - (1) Where backup tapes are considered "accessible" (i.e., actively used for information retrieval); and
 - (2) Where company can identify particular employee documents stored on backup tapes, the tapes of litigation's "key players" should be preserved.
- So, one less thing to worry about, right?



Pandora's Archive

The Risks of Technology Making Information More Accessible

I. Backup Tapes (continued)

- **One less thing to worry about, right? Maybe not.**
- At least one eDiscovery Vendor now claims that it "unlocks the data contained on backup tapes, making [the data] . . . *easily accessible*."
- The product "automates the process of searching and extracting data from offline tapes" and provides "[f]orensically sound extraction of files and emails from backup tapes."
- *See Goshawk Dedicated Ltd. v. Am. Viatical Servs., LLC*, 2010 U.S. Dist. LEXIS 137550 (N.D. Ga. Oct. 4, 2010) (citing this vendor as the technology used in search and retrieval of responsive ESI from backup tapes).
- Disaster recovery backup tapes may soon be considered accessible and subject to litigation holds.

For more, see http://www.indexengines.com/products_tape.html.



Pandora's Archive

The Risks of Technology Making Information More Accessible

II. PDAs

Different Risks, Just as Scary . . .



Pandora's Archive

The Risks of Technology Making Information More Accessible

II. PDAs


- No doubt they apply to 2006 ESI Amendments. *See, e.g., Southeastern Mech. Servs. v. Brody*, 657 F. Supp. 2d 1293, 1302 (M.D. Fla. 2009) (imposing sanctions against defendants for wiping data off Blackberries).
- May have once been a benefit/burden argument. *See* Rules 26(b)(2)(B) & (C)(iii), FRCP.
- Likely no longer the case with newer technologies. *See, e.g., Humphrey v. Sallie Mae, Inc.*, 2010 U.S. Dist. LEXIS 60176 (D.S.C. June 17, 2010); *Crews v. Domino's Pizza Corp.*, 2009 U.S. Dist. LEXIS 126718 (C.D. Cal. July 31, 2009).



Pandora's Archive

The Risks of Technology Making Information More Accessible

III. Cloud-Based Data Synchronization Tools

- Is *everything* accessible?
- More convenience  more risks



Pandora's Archive

The Risks of Technology Making Information More Accessible

IV. Instant Messaging

- Many companies consider IMs to be transitory and/or ephemeral in nature and therefore not discoverable . *See, e.g., Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey*, 497 F. Supp. 2d 627, 640 (E.D. Pa. 2007) (defendant did not engage in spoliation where computers automatically deleted temporary cache files).
- Growing ability for this data to be stored, indexed and searched for decreasing costs may change this approach.



Pandora's Archive

The Risks of Technology Making Information More Accessible

V. Voice Mail

- Previous difficulties with search and retrieval made burden and "inaccessibility" arguments strong. *See* Rules 26(b)(2)(B) & (C)(iii), FRCP.
- Technology is now allowing voicemails to forward to e-mail inboxes as WAV files, and, in some instances, the voicemails may even be transcribed.
- Creates stronger arguments that voicemail is discoverable.
- *See, e.g., In Re: Seroquel Products Liability Litigation*, 244 F.R.D. 650, 661 (M.D. Fl. 2007) (defendant's failure to produce voicemails, where unified system delivered them to inboxes, was one of several discovery failures leading court to impose sanctions).



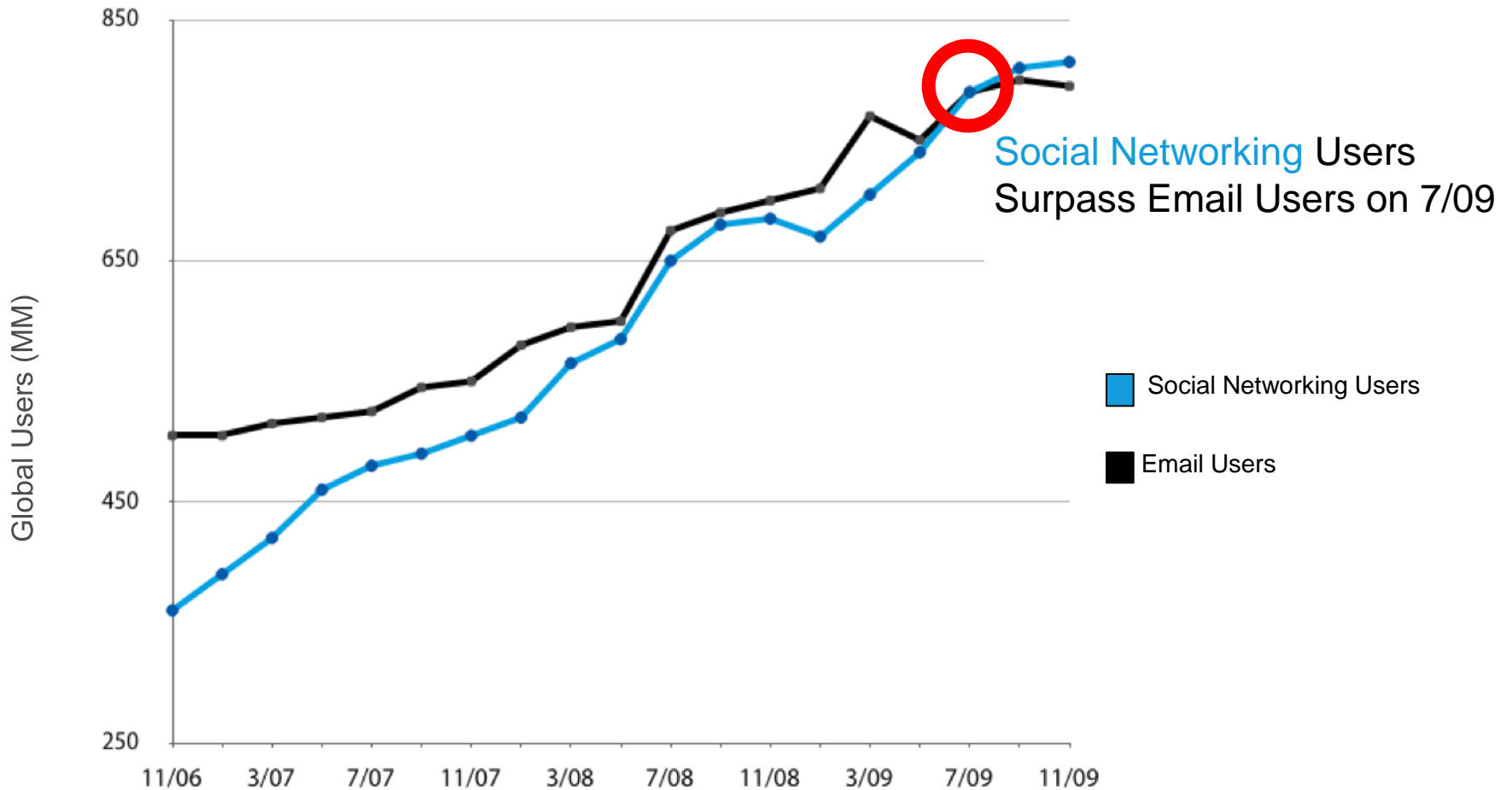
Are You in the Cloud?

- Gmail
- Google Docs
- iPad apps like Dropbox
- Windows Live



Trends: 2009 - Social Networking Surpasses Email

Communication has moved to the cloud



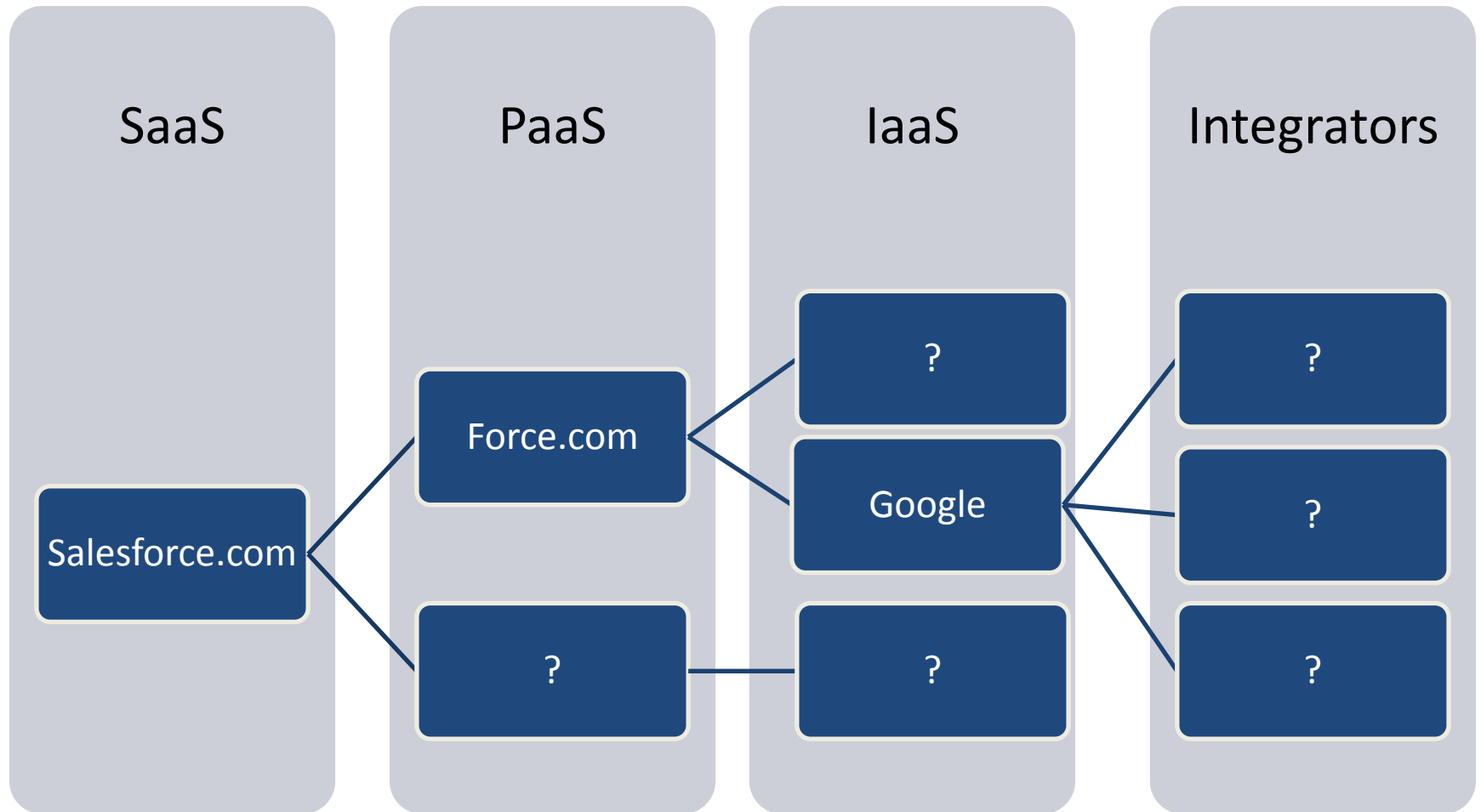
Source: Morgan Stanley Internet Mobile Report, December 2009
Data is for unique, monthly users of social networking and email usage.

Have you entered the cloud without knowing it?

- Many of the public clouds have click-wrap licenses – IT employee may have already started using the cloud
- Clicking "I agree" to cloud vendor's terms can be an effective electronic signature under state (UETA) and federal (ESIGN) law
- Need effective internal controls to manage risks

The Multi-Tenant Server Public Cloud

"If you want a \$1.00 hamburger, you don't get to see how the cow was raised"



The Pros and Cons of Multi-Tenancy

Shared infrastructure (NIST “resource pooling”)

- but pieces of your data are left behind all around the world

Rapid innovation (IDC 2009: 5 times faster development at half the cost*)

- but no audit trail on how they developed

Real-time scalability (NIST “rapid elasticity”)

- but you have no idea WHO has provided it

Automatic upgrades

- are you even aware of them?

Pay-as-you-go subscription model (NIST “metering”)

- but what do you have when you stop paying?

Available through any client platform (NIST “broad network access”)

- transferrable as well?

See NIST Definition of Cloud Computing v15 <http://csrc.nist.gov/groups/SNS/cloud-computing/>

Cloud Security Breach Risks Are On a Different Order of Magnitude Entirely

- Breach risk is mitigated on physical networks through network segmentation
- How much segmentation does a public cloud have?
- What are the collateral damage risks?
- Large public clouds make large targets
- You have no idea what new downstream integrators are coming on board in a large public cloud
- The economic downturn has been an upturn for the global black markets in hacked information
- But will these uncertainties drive cloud providers to adopt or provide levels of security that small companies could not afford?

Biggest Cloud **Security** Legal Issues: Encryption Easier than Destruction

- Payment Card Industry Data Security Standard (PCI-DSS)
Many specific security requirements, including:
 - Immediate, secure destruction of sensitive data
 - Audit requirement
- State and FACTA Secure Destruction Laws
 - Secure destruction, but not immediate
- HIPAA Security
 - Encryption on a par with destruction
- Breach Notification Requirements
 - Who provides the intrusion detection?

Cloud Security Heat Map

A. Information Security Laws and Standards	Public Cloud Threat Level	Comments/Issues
PCI Compliance		Immediate, secure destruction of all instances of magnetic stripe data, CVV code and PIN; audit requirement
Secure Destruction Laws (15 state laws)		Secure destruction requirement but no immediacy requirement
FACTA Disposal Rule		Secure destruction but no immediacy
FACTA Red Flags Rule		Intrusion detection
HIPAA Security		More specific documentation requirements and breach notification requirements; NIST encryption suffices
State personal information reasonable security laws		Reasonable technical, administrative and physical security
SSN Protection Laws (state)		Specific controls on use and safeguards for social security numbers
State Breach Notification Laws		Breach detection, immediacy of notification (of individual customer or owner/licensee)
SAS 70 Type 2		An audit against organization-specific controls, not a set of standards
ISO		Comprehensive but flexible security
FTC Unfair Trade Practice Case Law		Assure at least "reasonable" security

Security Drafting Considerations

Contract should require cloud vendor to:

- Monitor for breaches
- Provide incident response plan showing how "breach" is defined and its escalation procedures
- Give customer immediate notice of breach
- Preserve data / hardware relating to breach
- Provide access to facilities for forensic analysis following a breach
- Fully reimburse customer for all costs arising from a breach attributable to vendor

Biggest Cloud **Privacy** Legal Issues Arise Mostly from Pre-Internet Law

- EU Data Protection
- Electronic Communications Privacy Act
 - Broad government access, apparently getting broader
- Stored Communications Act
 - Remote Computing Service (RCS) vs. Electronic Communications Service (ECS) vs. both
- Newer Law: FTC Deceptive Trade Practices/APEC
 - Cloud back-end may undermine represented practices
- Purpose restrictions and data-mining

Cloud Privacy Heat Map

B. Privacy Law	Public Cloud Threat Level	Comments/Issues
EU Data Protection		https://www.datenschutzzentrum.de/presse/20100618-cloud-computing.htm Is Safe Harbor sufficient? Must data be limited? Must consents be obtained for all processing and transborder data flows? Must model contract be entered with cloud provider?
HIPAA Privacy		Minimum necessary; rights of access, amendment, accounting of disclosures
Employer Medical Privacy:HIPAA, GINA, ADA, FMLA, ARRA		Preventing inappropriate uses and disclosures
CAN-SPAM Act, Do-Not-Call Laws, Junk Fax Prevention Act		No concern
State Anti-Wiretapping Laws		Remember all-party consent
Electronic Communications Privacy Act		Obama administration just started advocating clear FBI access to transaction records with desk letter, contrary to longstanding initiative by entire tech industry
Stored Communications Act		Is cloud-based outsourced messaging a remote computing service (RCS, that may disclose with consent of "subscriber") or electronic communications service (ECS – that may only disclose with the consent of the addressee) or both? (e.g., Quon, Weaver)
FTC Cases "Deceptive Trade Practices" Case Law		Posted privacy policy issues; cloud "back end" may undermine represented practices
State and Federal Drivers' Privacy Protection Acts		Disclosure issues from intrusions

Biggest Cloud **Records Management & E-Discovery** Issues

- Willingness and ability of cloud provider to resist production per customer wishes
 - Compelled and permitted disclosures under the ECPA
 - Notice and opportunity to defend provision in cloud computing contract
- Willingness and ability of cloud provider to preserve and/or produce Electronically Stored Information (ESI)
 - Mitigation of production but not preservation duties under Rule 26(b)(2)(B) of FRCP
 - Spoliation risks and search costs
 - Adequate control over ESI backed up on indirectly contracted servers ?

Biggest Cloud **Records Management & E-Discovery** Issues

- ESI segmentation issues
 - E.g., ability of cloud provider to limit holds of backup tapes by customer
- E-record and e-document retention/destruction programs supported?
 - Need to assure secure destruction rather than deactivation?
- Data integrity, e-admissibility, and enforceability of e-signatures
 - Reliance on encryption, audit trails, or hash algorithms?



C. E-Discovery and Investigations	Public Cloud Threat Level	Comments/Issues
Willingness and/or obligation of cloud vendor to cooperate with customer in responding to discovery, investigations and preservation obligations		Willingness and ability to resist production in accordance with customer wishes; compelled and permitted disclosures under the ECPA
Ability of vendor to comply with preservation (hold) and production requirements imposed on it		Willingness and ability to preserve and/or produce all instances of Electronically Stored Information (ESI); ; mitigation of production but not preservation duties under Rule 26(b)(2)(B) of FRCP
Willingness/ability of vendor to put only backup tapes of particular customer on hold		Are backup tapes segregated by customer?
E-record and e-document retention/destruction programs supported?		Need to assure secure destruction rather than deactivation?
Preservation of replications and other redundancy		Potential major search cost issue, as well as spoliation issue
Data integrity and metadata		As the law of e-evidence develops, will reliance be placed on encryption, audit trails or hash algorithms?
Legal privileges		Issue now being addressed by many bars

Intellectual Property & E-Commerce Heat Map

D. E-Commerce	Public Cloud Threat Level	Comments/Issues
Enforceability of Electronic Signatures and Contracts		Adequate process controls to satisfy UETA, E-SIGN and international laws?
PCI Compliance		Immediate, secure destruction of all instances of magnetic stripe data, CVV code and PIN; audit requirement
E. Intellectual Property		
Risk of Loss/Theft		Large target for theft
Legal Risk of Inadequate Control		Potentially undermining IP rights

Related Data Use and Handling Contractual Provisions

- Confidentiality
 - Is the standard of care sufficient for contractual compliance (NDAs, licenses)?
- Trade secret maintenance
 - What prevents the service provider from learning from a customer's data?
- Secondary uses
 - Can the service provider use data to develop or improve its products and services?
 - Different expectations in consumer / business contexts
- Are the processes of the service provider audited by a third party? Are those audit reports available to the customer?
- Which service provider employees have access to customer data? Do any contractors?

Preparing for Defaults and Termination

- What happens if Provider disappears?
- Cyber-risk and related insurance coverage
- Early warning
- Source code/technology escrow
- Business continuity/exit plans
- Transition, migration
 - Wind-down periods
 - Return of Customer data or destruction, vs. deactivation, and immediately or eventually
 - Post-termination services/migration assistance/transferrable formats

Summary of Big Due Diligence and Contractual Issues

- Location
- Security
- Subcontractors
- How Much Due Diligence/Transparency Possible/Allowed?
- Data Ownership and Limitation of Use
- Response to Legal Process
- Data Retention, Access, Destruction
- Incident Response
- Indemnification/Risk Allocation
- Termination and Transition

May Lawyers Use SaaS?

- North Carolina Bar Proposed 2010 Formal Ethics Opinion 7 *Subscribing to Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property*, issued April 15, 2010 and WISELY withdrawn and sent to subcommittee for further study on October 28, 2010, asked:
 - "Given the duty to safeguard confidential client information, including protecting that information from unauthorized disclosure; the duty to protect client property from destruction, degradation or loss (whether from system failure, natural disaster, or dissolution of a vendor's business); and the continuing need to retrieve client data in a form that is usable outside of the vendor's product³; may a law firm use SaaS?"
- And answered:
 - "Yes, provided steps are taken effectively to minimize the risk of **inadvertent or unauthorized disclosure** of confidential client information and to protect client property, including file information, from **risk of loss.**"
- To deal with inadvertent disclosure in the public cloud, encryption may be necessary.
- To deal with risk of loss in the public cloud, backups have been necessary.

NC FEO 2010-7: Just a Few of the "Best Practices" for "Law Firms" (or for "Lawyers?")

A "lawyer should be able to answer:"

- Would the vendor be willing to include a provision in that agreement stating that the employees at the vendor's data center are **agents of the law firm and have a fiduciary responsibility to protect client information**?
- Has there been an evaluation of the vendor's security measures including the following:
firewalls, encryption techniques, socket security features, and intrusion-detection systems? Has the lawyer requested copies of the SaaS vendor's security audits?
- **Where is data hosted?** Is it in a country with less rigorous protections against unlawful search and seizure?
- If the lawyer terminates use of the SaaS product, or the service otherwise has a break in continuity, how does the lawyer retrieve the data and **what happens** to the data hosted by the service provider?

9/20/10: ABA Ethics Commission Concerns about Cloud and Confidentiality

- unauthorized access to confidential client information by a vendor's employees (or sub-contractors) or by outside parties (e.g., hackers) via the Internet
- the storage of information on servers in countries with fewer legal protections for electronically stored information
- a vendor's failure to back up data adequately
- unclear policies regarding ownership of stored data
- the ability to access the data using easily accessible software in the event that the lawyer terminates the relationship with the cloud computing provider or the provider changes businesses or goes out of business
- the provider's procedures for responding to (or when appropriate, resisting) government requests for access to information
- policies for notifying customers of security breaches
- policies for data destruction when a lawyer no longer wants the relevant data available or transferring the data if a client switches law firms
- insufficient data encryption
- the extent to which lawyers need to obtain client consent before using cloud computing services to store or transmit the client's confidential information

On May 2, the Commission Proposed Changes to:

- Model Rule 1.1 (Competency)
 - Stating that a lawyer's duty of competence includes a duty to remain aware of the benefits and risks associated with technology.
- Model Rule 1.6 (Duty of Confidentiality)
 - New paragraph to the existing rule on confidentiality and require lawyers to make reasonable efforts to prevent the inadvertent disclosure of, or unauthorized access to, confidential information, including information in electronic form:
 - "Factors to be considered in determining the reasonableness of the lawyer's efforts include
 - the sensitivity of the information,
 - the likelihood of disclosure if additional safeguards are not employed, and
 - the cost of employing additional safeguards.
 - "Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. "
- Model Rule 4.4 (Respect for the Rights of Third Persons)
 - Inadvertent transmission of information and clarifies that lawyers have a duty to notify the sender of both physical and electronic information under certain circumstances.

Required Terms and Conditions Being Considered by the ABA Ethics Commission:

The Commission previously asked for input on whether lawyers have an ethical obligation to incorporate certain terms into their cloud contracts:

- the ownership and physical location of stored data
- the provider's backup policies
- the accessibility of stored data by the provider's employees or sub-contractors
- the provider's compliance with particular state and federal laws governing data privacy (including notifications regarding security breaches)
- the format of the stored data (and whether it is compatible with software available through other providers)
- the type of data encryption
- policies regarding the retrieval of data upon the termination of services

9/10/10: NY Bar, Much More Assertively than NC, Defines Reasonable Care to Include:

- ensuring that the cloud provider has an enforceable obligation to preserve confidentiality and security, and that the provider will notify the lawyer if served with process requiring the production of client information;
- investigating the provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate;
- employing "available" technology to guard against reasonably foreseeable attempts to infiltrate the data; and/or
- investigating the provider's ability to purge and wipe any copies of the data and to move the data to a different host if the lawyer becomes dissatisfied or otherwise wants to change providers.

Even More Specific Obligations from the NY Bar

- The lawyer must periodically reconfirm that the provider's security measures remain effective as technology changes.
- If the lawyer has information to suggest that the provider's security measures are not longer adequate, or if the lawyer learns of a breach of confidentiality at the provider, the lawyer must
 - investigate whether there has been a breach of confidentiality of its client information,
 - **notify clients**, and
 - **discontinue use of the service** unless the lawyer receives assurances that the problems have been sufficiently remediated.

Out on the Public Cloud: What Shall We Do With the Drunken Pirate?

The screenshot shows a Windows Internet Explorer browser window displaying the Facebook page for the group "Support The Drunken Pirate (Stacy Snyder)". The browser's address bar shows the URL <http://www.facebook.com/group.php?gid=2323938795>. The Facebook page header includes the "facebook" logo and a login section with fields for "Email" and "Password", a "Login" button, and options for "Keep me logged in" and "Forgot your password?".

Below the header, a "Sign Up" button is followed by the text: "Support The Drunken Pirate (Stacy Snyder) is on Facebook. Sign up for Facebook to connect with Support The Drunken Pirate (Stacy Snyder)."

The main content area features a profile picture of a woman wearing a red pirate hat and drinking from a yellow cup. To the right of the picture, the group name "Support The Drunken Pirate (Stacy Snyder)" is displayed with a "AA" icon. Below the name are tabs for "Wall", "Info", "Photos", and "Discussions".

The "Info" tab is selected, showing the following details:

- Basic Info**
 - Name: Support The Drunken Pirate (Stacy Snyder)
 - Category: Common Interest - Politics
 - Description: Millersville University is violating Pennsylvania state law by revoking the right for Stacy Snyder to receive her education degree.
 - The Pennsylvania Crimes Code (Section 9124, states, neither summary offenses nor expungements can be used in consideration of acceptance or denial of a state license or certificate.
 - Millersville University revoked Stacy Snyder's right to her education degree because of an alleged drunken photo on Myspace.
 - Privacy Type: Open: All content is public.
- Contact Info**
 - Website: <http://www.foxnews.com/story/0,2933,2690...>
 - Office: West Chester
- Recent News**
 - News: <http://www.msnbc.msn.com/id/18372103/>

The Windows taskbar at the bottom shows the "start" button, several open applications (including "15 Micro...", "Heraeus - 5...", "Adobe A...", "C:\My Docu...", "Support The...", "Magazine > ...", and "Microsoft Po..."), and the system tray with the time "5:20 PM".

Things to Do With the New Authenticity That Get You Fired

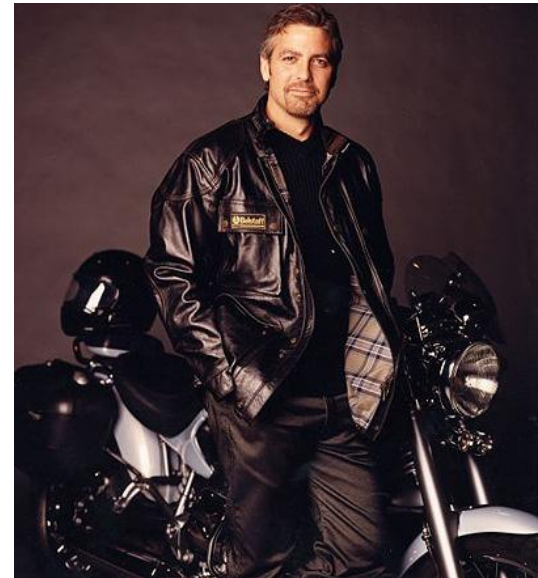
- Feb. 26, 2009: A U.K. teenager was fired for calling her job "boring." According to The Daily Mail, Kimberley Swann posted comments such as, **"First day at work. Omg !! So dull!!"**
- March 9, 2009: Dan Leone, a stadium operations employee for the Philadelphia Eagles, was fired after posting **"Dan is [expletive] devastated about Dawkins signing with Denver ... Dam Eagles R Retarded!!"** [sic].
- April 27, 2009: A Swiss woman was fired after calling in sick and then logging into Facebook on her "sick day." Apparently the woman had a migraine and called out of work because she thought the light from a computer would bother her and she needed to lie in a dark room.

Facebook Got Me Fired (cont.), or did it?

- August 27, 2009: Ashley Payne, a Georgia high school teacher, was forced to resign after the local school board came across pictures of her sipping beer and wine. The pictures, which appeared on Payne's Facebook page, were from a vacation she had taken that summer, which included a trip to the Guinness Brewery in Ireland.
- March 3, 2010: Gloria Gadsden, a professor at East Stroudsburg University in Pennsylvania, was fired after updating her Facebook status with things such as, "**Does anyone know where I can find a very discrete hitman? Yes, it's been that kind of day.**" [sic]
- November 8, 2010: NLRB files an administrative complaint against an employer who fired an employee for criticizing the employer, which it said was protected activity either in a union shop or a non-union shop (right to organize). Settled in February, and the NLRB has since given other signals of protecting non-defamatory criticism.

The Prevalence of Peeping and Leaking

- Temptation by databases
- Hospital staff snoop celebrity medical records:
 - Reportedly 40 doctors and other employees at the Palisades Medical Center in North Bergen, N.J., got suspensions for allegedly leaking confidential medical information about George Clooney and his girlfriend when they had their motorcycle accident
 - Last week there were firings reported of hospital employees who gained inappropriate access to information on the victims of the tragedy in Arizona
- Political peeping from Joe the Plummer and Candidate McCain to Candidates Obama and Clinton



Many Organizational Leaks and Breaches Are Eventually Monetized...

- Lawanda Jackson indicted for criminal HIPAA violations, for allegedly receiving \$4600 from the National Enquirer for 33 disclosures in 2006-07; checks were written to her husband

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

2008-APR -9 PM 2:31
CLERK U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
LOS ANGELES

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

February 2008 Grand Jury

UNITED STATES OF AMERICA,)
Plaintiff,)
v.)
LAWANDA JACKSON,)
Defendant.)

CR 08- **08-00430**

I N D I C T M E N T

[42 U.S.C. § 1320d-6(a)(2),
b(3): Wrongful Obtaining of
Individually Identifiable
Health Information for
Commercial Advantage; 18 U.S.C.
§ 2(b): Causing an Act to be
Done]

[FILED UNDER SEAL]

The Grand Jury charges:

At all times relevant to this Indictment:

INTRODUCTORY ALLEGATIONS

1. UCLA Health System was comprised of the following
medical facilities: UCLA Medical Center, Santa Monica-UCLA
Medical Center and Orthopaedic Hospital, Resnick
Neuropsychiatric Hospital at UCLA, Mattel Children's Hospital
UCLA, and the UCLA Medical Group. The individuals working at
these various medical facilities were employed by UCLA
Healthcare. Both UCLA Healthcare and UCLA Health System were

ARM:arm

FILED

...But Others May Just Do it Because They Believe It's the Right Thing to Do

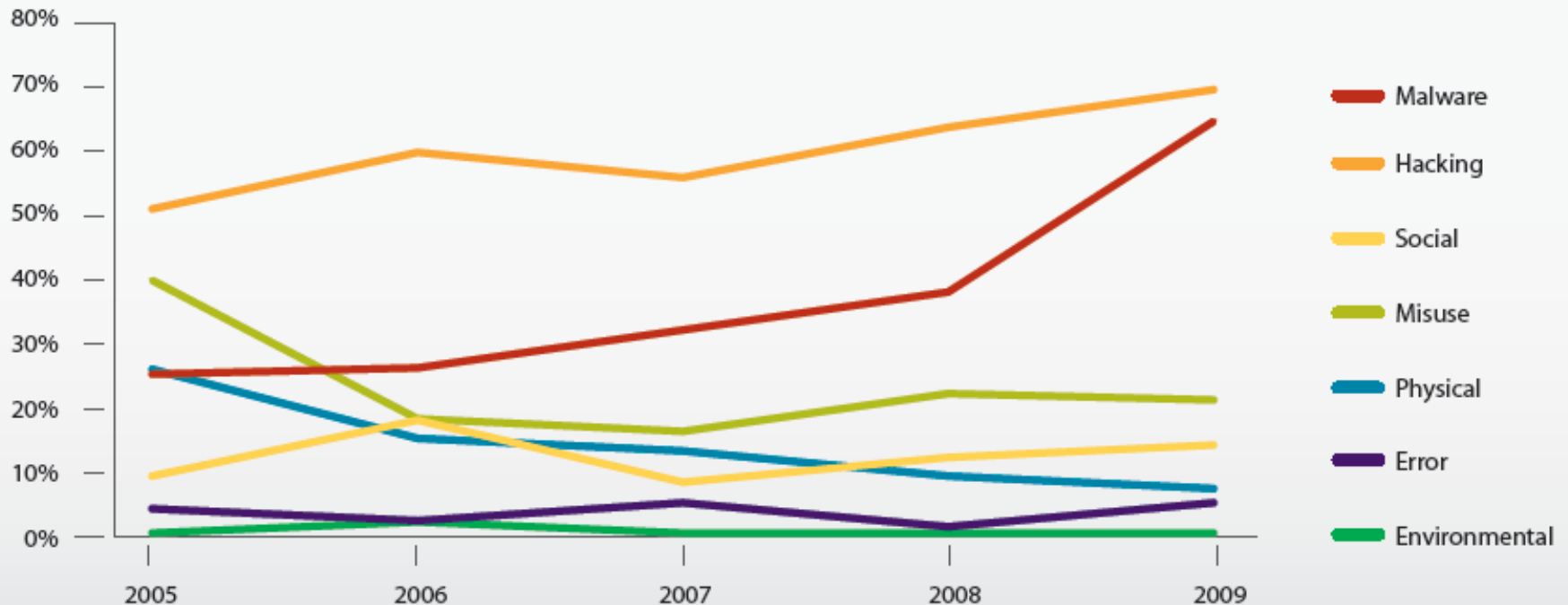
- "OpenLeaks is a project that aims at making whistleblowing safer and more widespread. This will be done by providing dedicated and generally free services to whistleblowers and organizations interested in transparency. We will also create a Knowledge Base aiming to provide a comprehensive reference to all areas surrounding whistleblowing."
 - (Just a thought: How do we know that a downstream "integrator" in the multi-tenant server public cloud doesn't believe in or practice that "transparency?")

Motivation for Leaks, Breaches and Data Dumps

- The black market trading in personal and company information has been growing steadily
 - Verizon and other data show malware and hacking to have become dominant as breach sources
- But a new ethos of transparency and whistleblowing has been growing as well
- Organizational information governance and management strategies need to address both
- "Listening to employees" in this context is entirely different from the listening for which, e.g., Toyota became famous

Breach Data—Verizon—Threat Categories

Threat Categories over Time by Percentage of Breaches



Verizon 2009 DBIR

The Implication for Organizations that Some Leaks are Made in Good Faith

- Tendency for both political figures and traditional media to characterize whistleblowers as traitors/criminals
- Employers may want to take a different approach: Dialogue with employees, including
 - Training in importance of information governance and privacy, information security and trade secret protections
 - Strong, credible commitments by employees to protect information (promises may matter)
 - Listening through whistleblower and other programs

Current Information Management Legal Challenges of Social Media

- Regulatory -
 - employees may post inappropriate comments or material on social media sites
 - advertising restrictions and transparency of representation
 - social media sites may not keep, protect and produce information as required
- Litigation/Reputational -
 - hostile third parties can have a major impact on brand and reputation, and companies must play defense well, not ignoring social media
 - inappropriate employee conduct on a social media site may subject the company to a lawsuit or tarnish a company's brand
 - difficulties in cooperation with social media sites in litigation and e-discovery
 - Gartner: by the end of 2013, half of all companies will have been asked to produce material from social media websites for e-discovery
- Information Security -
 - Collateral damage risks in connection with malicious attacks and viruses
 - Large targets
 - May lack capability to destroy all instances of information securely
- Privacy -
 - EU Data Protection
 - Electronic Communications Privacy Act/Stored Communications Act

Key Steps in Establishing an Effective Strategy

1. Create awareness at the board and senior management level; get senior management to understand the importance of information governance to the future of its business as well as the potential dangers of, e.g., social media, big data, cloud computing and leaks;
2. Create an information governance committee (made up of business unit reps as well as Legal and HR) who will be responsible for conducting studies and risk assessments regarding how media and interactions with employees about information can advance and hurt your business objectives
3. Determine what employees may speak on behalf of the company on authorized social media site.
4. Develop appropriate policies and procedures for addressing social media for marketing and employee behavior.
5. Audit and monitor authorized social media sites
6. Improve employee communications, training and whistleblower programs in the area of information governance

Questions? (LOL)

Jon.Neiditz@nelsonmullins.com

John.Martin@nelsonmullins.com

James.Epstein@reachsmart.com