Trends in Privacy Litigation and Regulation

December 4, 2008

Rocco Grillo – *Protiviti*

Deborah Thoren-Peden - *Pillsbury*

John Nicholson - *Pillsbury*

Meighan O'Reardon - *Pillsbury*

Pillsbury Winthrop Shaw Pittman LLP and Protiviti, Inc.

Presentation Agenda

- Introduction
- State Regulatory Developments
  - Massachusetts, Nevada, and Connecticut
- Recent Privacy Litigation
- Social Networking
- Cloud Computing
- Managing and Mitigating Legal Risk
- Comments and Questions

protiviti® Independent Risk Consulting pillsbury

State Regulatory Developments

MASSACHUSETTS

- "Standards for the Protection of Personal Information of Residents of the Commonwealth" (*201 Mass. Code Regs. § 17.00)*
  - Purpose: To establish "minimum standards to safeguard personal information in both **paper** and **electronic** records."
- Personal Information Defined
  - A Massachusetts resident's first name and last name or first initial and last name in combination with one or more of the following data elements that relate to the resident:

    (a) Social Security Number;

    (b) Driver's License or State Identification Card Number; or

    (c) Financial Account Number or Credit or Debit Card Number.

State Regulatory Developments (cont'd)

MASSACHUSETTS (cont'd)

- Who Must Comply?
  - "…persons who own, license, store or maintain personal information about a resident of the Commonwealth of Massachusetts."
  - A presence in Massachusetts is not required to be liable under the Regulation.

State Regulatory Developments (cont'd)

MASSACHUSETTS (cont'd)

- Requires organizations to develop, implement, maintain and monitor a comprehensive, written information security program for records containing personal information (“Program”).
- Regulations allow for flexibility to tailor each organization’s Program.

State Regulatory Developments (cont'd)

MASSACHUSETTS (cont'd)

- Each Program must address the twelve activities identified in the Regulation.
  - Identifying and assessing risks to security, confidentiality and/or integrity of personal information;
  - Instituting restrictions on physical access to records with personal information;
  - Verifying third-party service providers with access to personal information have the capacity to protect it and contractually requiring them to maintain personal information safeguards;
  - Identifying paper, electronic and other records, computing systems and storage media (laptops and portable devices) used to store personal information.

State Regulatory Developments (cont'd)

MASSACHUSETTS (cont'd)

- If storing or transmitting personal information, the following must be addressed:
  - (1) user authentication protocols;
  - (2) security access control measures;
  - (3) **encryption of records that travel across public networks**;
  - (4) monitoring systems for unauthorized access;
  - (5) **encryption of personal information stored on portable devices**;
  - (6) updating firewalls and system security;
  - (7) maintaining current virus protections; and
  - (8) training for employees on computer security and protecting personal information.

State Regulatory Developments (cont'd)

MASSACHUSETTS (cont'd)

- Tiered Compliance Deadlines
  - May 1, 2009
    - General compliance with the new standards
    - Compliance with third-party service provider requirements
    - Encryption of laptops
  - January 1, 2010
    - Obtaining written certification of compliance from third-party service providers
    - Encryption of all other portable devices

State Regulatory Developments (cont'd)

MASSACHUSETTS (cont'd)

- Compliance Considerations
  - Review information security policies and procedures
  - Review electronic and physical record retention policies and procedures
  - Encryption measures on all portable devices that contain personal information
  - Non-Massachusetts-based businesses should consider incorporating requirements in their information security programs
  - Review outsourcing agreements to verify that service providers with access to personal information are contractually bound to maintain sufficient safeguards

State Regulatory Developments (cont'd)

NEVADA

- "Restrictions on transfer of personal information through electronic transmission" *(Nev. Rev. Stat. § 597.970*)
  - "A business in this State shall not transfer any personal information of a customer through an electronic transmission other than a facsimile to a person outside of the security system of the business unless the business uses encryption to ensure the security of electronic transmission."
  - Effective Date: October 1, 2008

State Regulatory Developments (cont'd)

NEVADA (cont'd)

- Significant Features:
  - First state law to mandate a specific type of security measure (encryption) for personal information.
  - Applies to any organizations “doing business in Nevada.” This standard can include out of state businesses.
  - Applies to all of a business’s customers, not just Nevada-based customers.
  - Transmissions that remain within a business and faxes are excluded from the requirement.
  - Penalties for non-compliance are not specified in the statute.

State Regulatory Developments (cont'd)

CONNECTICUT

- "An Act Concerning the Confidentiality of Social Security Numbers" (*Public Act No. 08-167*)
  - "Any person in possession of personal information of another person shall safeguard the data, computer files and documents containing the information from misuse by third parties, and shall destroy, erase or make unreadable such data, computer files and documents prior to disposal."
  - "Any person who collects Social Security numbers in the course of business shall create a privacy protection policy which shall be published or publicly displayed."
  - Effective Date: October 1, 2008
  - Penalties: Provides for fines of $500 per violation not to exceed $500,000.

State Regulatory Developments (cont'd)

Trends

- Expansion of regulations beyond electronic format to paper (Massachusetts)
- Greater specificity in the security measures required by State laws
  - Encryption specifically required in Nevada law not merely “reasonable” security measures
  - Payment Card Industry Data Security Standards (PCI DSS) incorporated in 2007 Minnesota Plastic Card Security Act (*H.F. No. 1758*)
- States imposing their data security laws on “foreign” businesses
  - A physical presence in the state is often not required
  - Standards for being covered under a particular state’s data security include:
    - “Doing Business” in a particular state
    - Holding a resident’s personal information

protiviti® Independent Risk Consulting pillsbury

Recent Privacy Litigation

Deep Packet Inspection of Internet Transmissions to Target Ads – Valentine v. NebuAd, Inc., et al.

- 50-page Class Action Complaint filed in Federal Court in Northern California, Nov. 2008 (N.D. Cal., No. 3:08-cv-05113)
- NebuAd Inc. and 6 Internet service providers allegedly violated customers' privacy via use of deep packet inspection (DPI) technology
- Complaint alleges:
  - Customers unaware their online activity was being monitored for marketing purposes – technology allowed for identification of web sites accessed, plus what they looked at, compared, bought, credit card information, etc.
  - Either no notice or consent provided, or was insufficient or misleading
  - Technology intentionally negated customers' effort to remove the tracking cookies

Recent Privacy Litigation (cont'd)

Deep Packet Inspection of Internet Transmissions to Target Ads – Valentine v. NebuAd, Inc., et al. (cont'd)

- Plaintiff alleges the Deep Packet Inspection involved wiretapping, forgery and browser hijacking
- Complaint alleges violations of:
  - Electronic Communications Privacy Act, 18 U.S.C. § 2510
  - Computer Fraud and Abuse Act, 18 U.S.C. § 1030
  - California's Invasion of Privacy Act, California Penal Code § 630
  - California's Computer Crime Law, California Penal Code § 502
  - Aiding and abetting violations of these Acts
  - Civil conspiracy to engage in such wrongful conduct
  - Unjust enrichment

Recent Privacy Litigation (cont'd)

Deep Packet Inspection of Internet Transmissions to Target Ads – Valentine v. NebuAd, Inc., et al. (cont'd)

- Complaint describes an August 2008 Congressional Privacy Inquiry involving the tailoring of Internet ads based on consumer's Internet search, surfing or other use
- Congress sent an inquiry to 33 Internet-based companies
  - The complaint includes the responses of the 6 Internet Service Providers listed as defendants

Recent Privacy Litigation (cont'd)

Deep Packet Inspection of Internet Transmissions to Target Ads – Valentine v. NebuAd, Inc., et al. (cont'd)

- Congress sent the following 11 questions to the ISPs:
  - Has your company at any time tailored, or facilitated the tailoring of, Internet advertising based on consumers' Internet search, surfing, or other use?
  - Please describe the nature and extent of any such practice and if such practice had any limitations with respect to health, financial, or other sensitive personal data, and how such limitations were developed and implemented.
  - In what communities, if any, has your company engaged in such practice, how were those communities chosen, and during what time periods was such practice used in each?
  - How many consumers have been subject to such practice in each affected community, or nationwide?

Recent Privacy Litigation (cont'd)

Deep Packet Inspection of Internet Transmissions to Target Ads – Valentine v. NebuAd, Inc., et al. (cont'd)

- Has your company conducted a legal analysis of the applicability of consumer privacy laws to such practice?
- How did your company notify consumers of such practice?
- Please explain whether your company asked consumers to "opt in" to the use of such practice or allowed consumers who objected to "opt out." If your company allowed consumers who objected to opt out, how did it notify consumers of their opportunity to opt out?

Recent Privacy Litigation (cont'd)

Deep Packet Inspection of Internet Transmissions to Target Ads – Valentine v. NebuAd, Inc., et al. (cont'd)

- How many consumers opted out of being subject to such practice?
- Did your company conduct a legal analysis of the adequacy of any opt-out notice and mechanism employed to allow consumers to effectuate this choice?
- What is the status of consumer data collected as a result of such practice? Has it been destroyed or is it routinely destroyed?
- Is it possible for your company to correlate data regarding consumer Internet use across a variety of services or applications you offer to tailor Internet advertising? Do you do so?

Recent Privacy Litigation (cont'd)

Deep Packet Inspection of Internet Transmissions to Target Ads – Valentine v. NebuAd, Inc., et al. (cont'd)

- Some of the ISP responses seem to indicate they had received assurances the technology relied on anonymous identifiers that could not be used to identify a specific customer
- Most had shut down the pilots and had required NebuAd to destroy to the data
- Same sorts of issues can arise through other data mining efforts

Recent Privacy Litigation (cont'd)

Unsolicited Text Message Ads (Weinstein v. Airit2me, N.D. Ill., No. 1:06-cv-00484)

- Timberland Co. allegedly contracted with Airit2me Inc. and GSI Commerce Inc. to promote a sale
- Allegedly tens of thousands of unsolicited text message ads sent to cell phones
- Charges brought under the Telephone Consumer Protection Act
  - Prohibits marketing calls using an autodialing system unless prior express consent
  - Also prohibits telephone solicitations to individuals on the national "do not call" list
- $7 million settlement given preliminary approval by U.S. District Court

Recent Privacy Litigation (cont'd)

California Deception Claims Preempted by CAN-SPAM Act (*Hoang v. Reunion.com Inc.*, N.D. Cal. No. 08-3518, 10/3/08)

- Deception claims involving "forward-to-a-friend" e-mails brought under California's anti-spam law
- CAN-SPAM Act preempts state statutes, except to the extent that they prohibit "falsity or deception"
- Claims did not allege elements of common law fraud or deceit, including:
  - that the e-mail statements were false,
  - that defendant knew the statements were false when made, and
  - that plaintiffs relied to their detriment on any misrepresentation.

Recent Privacy Litigation (cont'd)

California Deception Claims Preempted by CAN-SPAM Act (*Hoang v. Reunion.com Inc.*, N.D. Cal. No. 08-3518, 10/3/08) (cont'd)

- Court looked at FTC's new Final Rules on CAN-SPAM, which address "forward-to-a-friend" emails and indicates that some can have liability under CAN-SPAM
- If you utilize such advertising advisable to analyze in context of FTC's Rules and possible state laws

Recent Privacy Litigation (cont'd)

Facebook Wins Case Against Spammer

- Spammer accused of sending more than 4 million spam messages from Facebook members' profiles
- $873 million judgment for Facebook
- Facebook senior corporate counsel, "This is not the last lawsuit Facebook will file."

Recent Privacy Litigation (cont'd)

International Developments

- Article 29 Working Party of European Union data protection officials revised FAQs (WP 155) on Binding Corporate Rules ("BCRs") on October 29, 2008
  - Adopting BCRs is a means for global companies to comply with EU data protection laws and export data from an EU country to countries without "adequate" data protection – it is designed to facilitate cross-border data transfers between their centers of operations.
  - FAQs tell companies:
    - the circumstances in which BCRs should be used,
    - who is liable for breaches of the BCRs, and
    - what rights people have when their data is transferred.
  - To facilitate reviews of BCRs by Data Protection authorities FAQs encourage companies drawing up BCRs to include all group obligations and individual rights in a single document.

Recent Privacy Litigation (cont'd)

International Developments (cont'd)

- French data protection authority (CNIL) decision (Nov. 12, 2008)
  - Data sent via Bluetooth devices to mobile phones is private information and thus, protected by French privacy law
  - Ads sent via Bluetooth devices to mobile phones are a form of direct marketing via email and require prior consumer consent
  - Receiving an electronic invitation to receive the ad to the phone is not adequate

Emerging Risk: Social Networking

- **Trends**

Instant Messaging	⇧	*Increasing Risk*	**Classmates**	⇧	*Increasing Risk*
MySpace	⇧	*Increasing Risk*	**LinkedIn**	⇧	*Increasing Risk*
Facebook	⇧	*Increasing Risk*	**Match.com**	⇧	*Increasing Risk*
Blogs	⇧	*Increasing Risk*			

- **Risk Trends**
- Many of the risks are not new, including software attacks, disclosure of information, inaccurate information, and brand damage. Controls also are not necessarily new.
  - Many of the needed policies/standards should already exist within "communications" policies (e.g., defamatory, harassing, obscene, sexually explicit, abusive, or inappropriate content)
  - Some training (warnings about disclosure of information) should already exist
  - Most likely already have some of the technical controls in place to protect web applications
  - May be monitoring external sites for inaccurate information

YAHOO! TECH

Hackers using fake YouTube pages to attack computers

Posted on Thu Oct 9, 2008

SAN FRANCISCO (AFP) - Computer security specialists warn that hackers are using fake YouTube pages to trick people into opening their machines to diabolical software.
A deceptive YouTube attack evolving as it spreads on the Internet is part of a growing trend of hackers to prowl popular online social networking communities in which people trustingly share web links and mini-programs.
"We are seeing tools like this not just for YouTube, but for MySpace, Facebook, America Online instant messaging ...," Trend Micro software threat research manager Jamz Yaneza told AFP on Thursday.

protiviti® Independent Risk Consulting pillsbury

Social Networking: Looking into the Future - Generation Y

- Increased focus on work life balance with Generations Y.
- Increased comfort with technologies - new services & introduce new risks:
  - The risk and liability associated with access to online social networks;
  - Potential introduction of malicious code delivered via MP3 players and other devices;
  - The increased opportunity for data leakage by allowing mobile storage devices and/or access to write to disk media such as CD's or DVD's.
- Currently, use a "Block All" approach but will need more:
  - Acceptable Use and User Network Security policies;
  - Train personnel in the acceptable use of software and technologies;
  - Implement monitoring software that will monitor use, but notify or prevent abuse.

protiviti® Independent Risk Consulting pillsbury

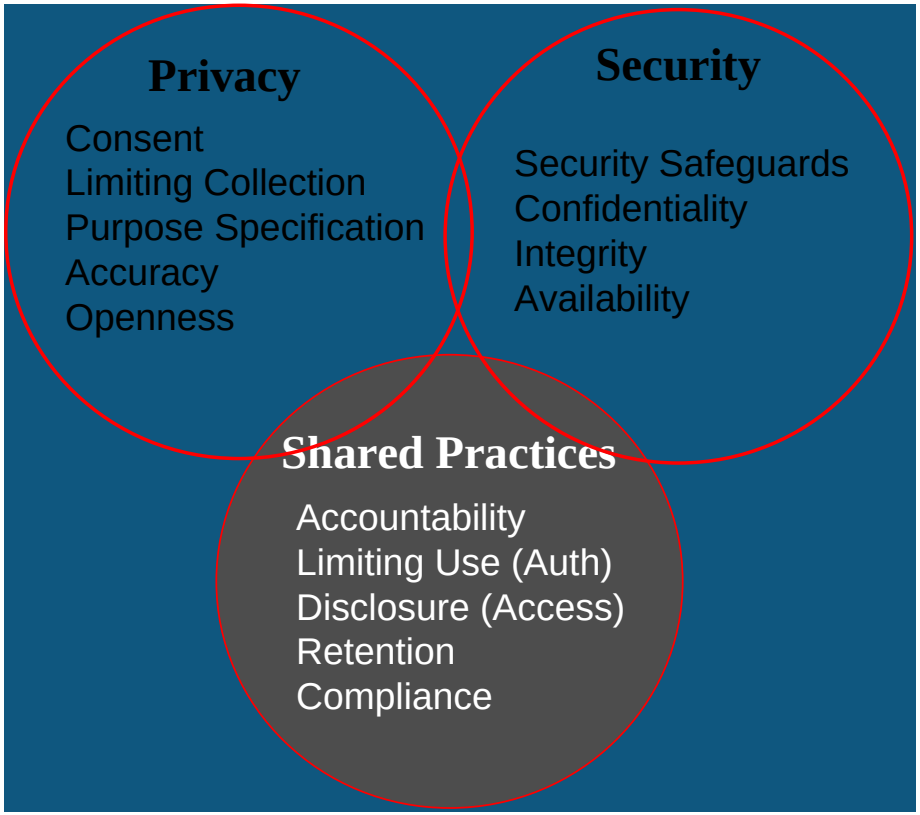
Social Networking: Security & Privacy

Privacy today is not confidentiality, but access - who has access to your personal information.

The development of system enforceable privacy policies, governing not only what personal information can be collected, but how such information can be accessed and used (and audited) once collected — as well as the security of such information while held.

Issues with forensics and investigations especially international incidents with US based resources or management

Issue with Privacy and Surveillance



protiviti® Independent Risk Consulting pillsbury

Cloud Computing - Basics

What is it?

- A general concept that incorporates software as a service (SaaS), Web 2.0 and other recent technology trends, in which the common theme is reliance on the Internet for satisfying the computing needs of the users.
- Services that run in a Web browser and store information in a provider's data center — ranging from adaptations of familiar tools such as email and personal finance to new offerings such as virtual worlds and social networks.

Who is it?

- Google / Microsoft Online
- Facebook / MySpace / Other Social Networking Sites
- Wesabe
  - Allows users to participate in all Wesabe community features and manage bank or credit card accounts

Cloud Computing – New & Changing Issues

What issues are changing in a cloud computing environment?

- Blurring distinction between public and private space
  - Creation of shared spaces into which people inject data
- Becoming less clear what is happening where
  - More federation of services
  - More difficult to track who is doing what with what data

Cloud Computing – New & Changing Issues (cont'd)

What issues are changing in a cloud computing environment? (cont'd)

- Outsourced services are black box
  - Is there a duty to investigate on the part of outsourcer?
  - Who is responsible for cross-border issues?
    - What law governs the service?
    - What do you do if the legal obligations conflict?
  - Who is responsible for backup? Who owns the data?
- Centralization of data creates targets for regulation / enforcement

Cloud Computing - Privacy & Security

Does the cloud computing framework require any different analysis when it comes to privacy and security?

- Privacy
  - Embed fair information practices into the business and service model
    - http://www.ftc.gov/reports/privacy3/fairinfo.shtm
  - Develop ways for rights of use and collection to flow with data

protiviti® Independent Risk Consulting pillsbury

Cloud Computing - Privacy & Security (cont'd)

Does the cloud computing framework require any different analysis when it comes to privacy and security? (cont'd)

- Risk of attack
  - Centralization of data creates targets
    - Curious / Malicious
    - Internal / External
  - When evaluating a service, consider what attracts attack and why
  - Does the platform create infection vectors for malware
    - Does the platform enable users to create new applications
- Risk of subpoena / government action

Managing and Mitigating Legal Risk

Need to Understand What You Have, What You Get and What You Do With Such Information

- Many companies are not fully aware
- Self Assessment, especially high risk areas
  - What do you collect, share, sell, etc.?
  - How do you use it and do you really need it?
  - How do you share it, with whom and who oversees these decisions?
  - How long do you retain and how do you destroy?
  - Answers may vary by department (e.g., HR will be different than Marketing)
  - Laws apply to employees, customers, potential customers, individuals, vendors, and individual employees of vendors
  - Businesses can be covered too, both by law and contract

protiviti® Independent Risk Consulting pillsbury

Managing and Mitigating Legal Risk (cont'd)

Privacy Promises/Standards

- Are your practices/procedures consistent?
- Can you continue to meet such standards?
- Extremely important to look ahead
  - Corporate strategies and opportunities likely to impact

protiviti® Independent Risk Consulting pillsbury

Managing and Mitigating Legal Risk (cont'd)

Understand the Scope of Your Risks

- High, moderate, low
  - Many factors go into such evaluation
- Track and measure such risks on an ongoing basis
- Prioritize your privacy resources based on risk

protiviti® Independent Risk Consulting pillsbury

Managing and Mitigating Legal Risk (cont'd)

Need to Know the Laws/Regulations and Track Changes

- Hundreds of laws and regulations in the US alone
- Internationally--there are even more
- Need capable people
- Make sure relevant information is provided to appropriate people in the company

Managing and Mitigating Legal Risk (cont'd)

Similar to Managing any Compliance/Legal Risk

- Need to be able and willing to adjust practices and policies
- Watch for trends in regulatory actions and litigation
- Ensure legal is involved in material changes and contracts
  - New products or services
  - Expansion or contraction of company, products, services
  - Sales or purchases of assets, companies
  - Offshore operation
  - Special marketing arrangements

Managing and Mitigating Legal Risk (cont'd)

Significant Legal Risk Areas Today

- Security breaches
- Data sharing and mining, especially for marketing purposes
- Employee data, especially where used to discipline or terminate
- Identity theft causing consumer fraud or loss
- Protection of IP in age of increased sharing

Managing and Mitigating Legal Risk

Significant Legal Risk Areas Today (cont'd)

- Failure to keep Privacy Promises
- Failure to Protect Customer Database - arguably the company's most important asset
  - More than just breaches; what is the company committing to do in terms of sharing, etc.?
  - Oversight of how third parties handle your data and abide by contractual commitments
- Collection of information or monitoring/recording information in an illegal manner (albeit it, unintentionally)

Managing and Mitigating Legal Risk (cont'd)

Traditional Legal Risk Mitigation Strategies

- Appropriate polices, procedures and practices
  - Update as needed and review frequently to make sure they work
  - Audit or independent reviews
- Clear identification of responsible employees/officers
- Training of employees and, if needed, third parties
- Audit or oversight of third parties handling or having access to your data
- Stay current on information and trends; involvement in appropriate associations

Managing and Mitigating Legal Risk (cont'd)

Some Questions to Ask Yourself

- Questions posed during Congressional Privacy Inquiry regarding tailoring of Internet Ads--can you answer them without concern?
- Are your employee practices acceptable?
  - If sued, are there any gaps/actions you would have taken or handled differently?
  - Are you responsive to privacy issues raised by employees or third parties?
  - Is your employee handbook up to date in terms of privacy practices (e.g., social networking, etc.)?

Managing and Mitigating Legal Risk (cont'd)

Some Questions to Ask Yourself (cont'd)

- Is Marketing using or sharing Information in any way that could pose a reputational risk (e.g., could it show up in the press)?
- For any lawsuit filed against you, have there been privacy related issues, and if so, have you addressed them?
- Are your privacy policies consistent across operations; if not, can you manage easily across the divisions?

Managing and Mitigating Legal Risk (cont'd)

Some Questions to Ask Yourself (cont'd)

- Who in Legal is responsible for tracking privacy trends and changes in the law?
  - How do they communicate such changes to others in the company in a timely fashion?
- As you may not be able to do everything perfectly, are your resources deployed consistent with your risks?

Comments and Questions

Rocco Grillo
Managing Director, Protiviti, Inc.
1290 Avenue of Americas
New York, NY 10104
212-603-8381
rocco.grillo@protiviti.com

Debbie Thoren-Peden
Partner, Pillsbury Winthrop Shaw Pittman LLP
725 South Figueroa Street, Suite 2800
Los Angeles, CA 90017-5406
213-488-7320
deborah.thoren-peden@pillsburylaw.com

Meighan O'Reardon
Associate, Pillsbury Winthrop Shaw Pittman LLP
2300 N Street, NW
Washington, DC 20037-1122
202-663-8377
meighan.oreardon@pillsburylaw.com

John Nicholson
Senior Associate, Pillsbury Winthrop Shaw Pittman LLP
2300 N Street, NW
Washington, DC 20037-1122
202-663-8269
john.nicholson@pillsburylaw.com