McDermott Will & Emery

RIMSomnia – What Keeps RIM Managers Awake At Night: The Importance of Privacy

How To Ensure that Valuable Information Remains Private and What To Do if It Doesn't

Brian B. McCauley, CRM
McDermott Will & Emery LLP

January 15, 2014

Privacy and Data Breach Trends – Recent Years

McDermott Will & Emery

Over the past four to five years, mega database breaches of tens of millions of records containing personally identifiable information (PII) were documented, compromising the privacy and finances of millions of individuals.

Privacy Breach Trends 2012-2013

McDermott Will & Emery

- November 2012 - 27.8 million records compromised and 637 breaches reported involving personally identifiable information (PII)

- November 2013 - 10.6 million records compromised and 483 breaches reported involving personally identifiable information (PII) .

-Source: *Privacy Rights Clearing House*

Notable Breaches – 2013

McDermott Will & Emery

- Adobe - **3 million** PII records, more than **150** million username/password combos, and source code from Adobe Acrobat, ColdFusion, ColdFusion Builder
- U.S. Department Of Energy - PII stolen for **53,000** former and current DOE employees - limited to DoE employee PII
- Advocate Medical Group - **4** million patient records stolen off of four stolen computers
- Target – **70 to 110** million credit card numbers compromised in potentially the largest retailer data breach in US history

Progress in The Prevention of Data Breaches

McDermott Will & Emery

The news is not all that bad – but we have a long way to go……

- In 2013 Breach stats declined, but data is still at risk from poorly protected databases, applications, and endpoints

A History of Privacy in the U.S.

McDermott Will & Emery

- Cast your mind back …
- Historical focus: Individuals vs. (1) Government (2) Business
  - 1700's -- 4th Amendment to the U.S. Constitution
  - 1970's -- Privacy Act of 1974 (applies to federal government)
  - 1996 -- HIPAA (protects health information)
  - 1999 -- GLBA (protects financial information)
- Focus shifts: Homeland Security -- September 11, 2001
  - Corresponding explosion of state breach notification laws

A History of Privacy in the U.S.

McDermott Will & Emery

- Fast forward to 2012
  - Administration releases a Consumer Privacy Framework and a "Consumer Privacy Bill of Rights"
  - FTC releases its Final Report on Privacy
  - Bottom line: Most companies doing business anywhere in the U.S. will likely will have to meet some minimum privacy and data security standard

Data Privacy Law: Key Terminology

McDermott Will & Emery

- "**Data subject**" – any natural person identifiable from personal data (whether directly or indirectly).
- "**Personal data**" – any information relating to a "data subject".
- "**Data controller**" – determines the purposes and means of the "processing" of personal data.
- "**Processing**" – any operation or set of operations performed upon personal data, whether or not by automatic means.
- "**Data Processor**" – processes personal data on behalf of the controller.

Data Privacy Law: Key Principles

McDermott Will & Emery

1. Process personal data fairly and lawfully.
2. Collect personal data only for specified, explicit and legitimate purposes.
3. Collect and store personal data only to an extent that is adequate, relevant and not excessive.
4. Ensure that all personal data held is accurate and, where necessary, kept up to date.
5. Do not keep personal data for any longer than is necessary.
6. Process personal data only in accordance with the rights of data subjects.
7. Implement appropriate technical and organizational security measures.
8. *Do not transfer personal data outside the European Economic Area.*

What applies to U.S. business?

McDermott Will & Emery

Assessment depends on type of data and type of business activity:

- Do you collect “personal information” of employees or customers? (focus on myriad state laws)
- Do you extend credit? (FCRA, FACTA, Red Flags)
- Do you perform credit or background checks? (FCRA, state laws)
- Do you accept payment cards? (PCI-DSS, state laws)
- Do you self-insure your employee benefit plans? (HIPAA)
- Do you engage in marketing? (CAN-SPAM, Junk Fax law, TCPA)
- Do you have a website? (OPPA, COPPA)
- Are you publicly traded? (SOX, SEC Guidance)

U.S. State Law Obligations

McDermott Will & Emery

- Data security (11 states)
- Data destruction (25 states)
- Social Security Number protection (27 states)
- Security breach notification (46 states + DC)
- Data collection and use restrictions
- Massachusetts Data Security Regulations, c. 93H
  - Vendor certification deadline was March 1, 2012

So, now what do we do?

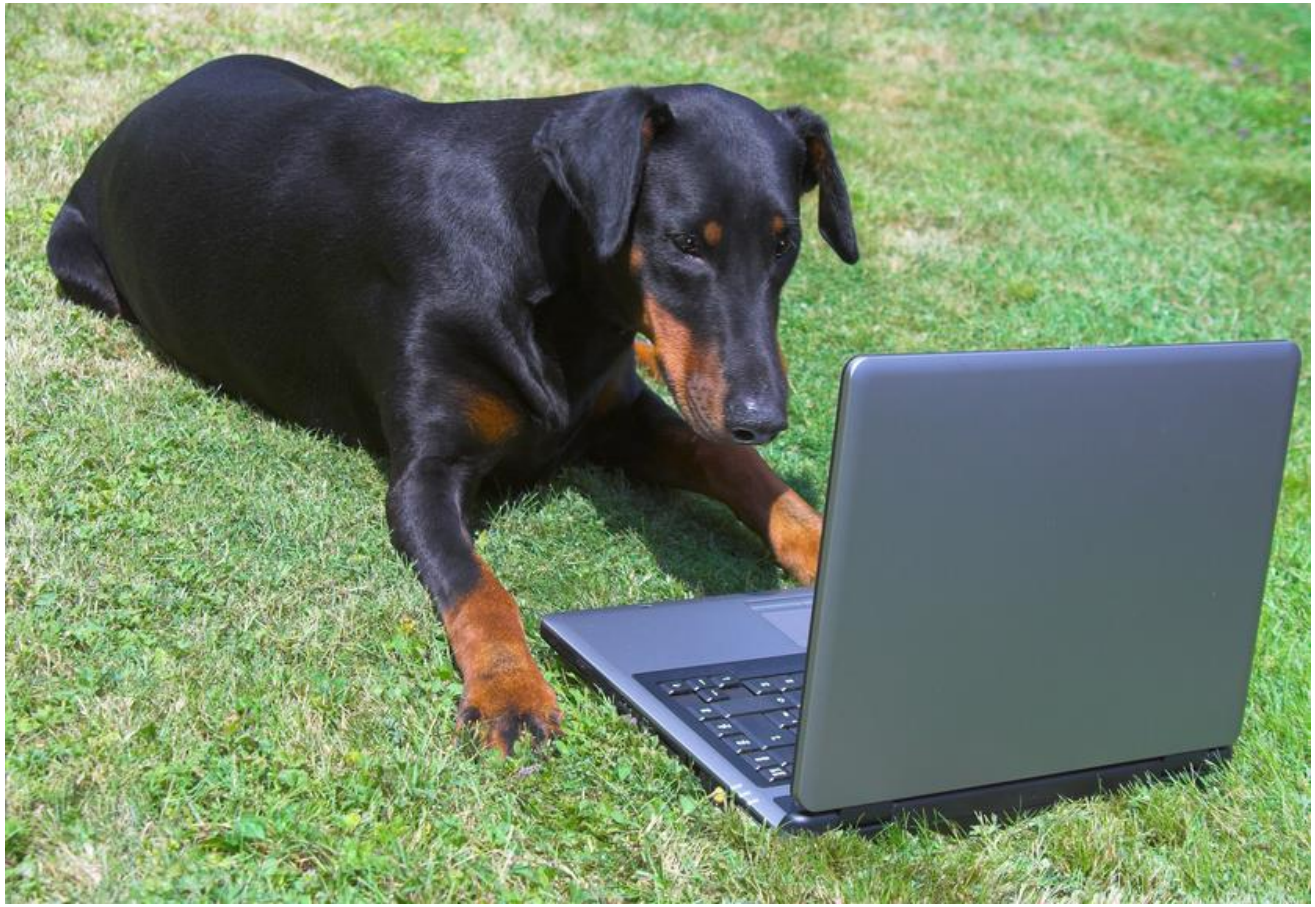
McDermott Will & Emery

Phase I -- Plan

McDermott Will & Emery

Phase II -- Protect

McDermott Will & Emery



Phase III -- Patrol

McDermott Will & Emery

Success Strategies: Planning

McDermott Will & Emery

- Assess current compliance posture under applicable laws
  - State-specific requirements (e.g., for implementing WISPs)
  - Data-specific requirements (e.g., HIPAA, FCRA, PCI-DSS)
  - Business activity-specific requirements (TCPA, CAN-SPAM)
- Design controls to fill gaps
  - Internally and externally facing policies, including incident response
  - Technological controls
  - Vendor risk management

Success Strategies: Protecting

McDermott Will & Emery

- Implement controls identified during the planning phase
- Establish governance structure
- Implement recommended administrative, technical and physical security controls (requires budget dollars and personnel/time investment)
- Roll-out training to complete workforce, give targeted training for key stakeholders
- Line-up key business relationships, including team of crisis responders

Success Strategies: Patrolling

McDermott Will & Emery

- Conduct regular assessments to ensure that program is operating as intended, and addressing changes in business operations or otherwise that impact the program
- Internal audit conducts privacy and security assessments
- Automated processes for ongoing IT systems monitoring
- Dedicated governance personnel reviewing program at periodic intervals and points of process or business-change
- Incident response program

Data Protection Law, U.S. Model:
Focus on Data Security

McDermott Will & Emery

- Laws in 46 states, plus DC
- In general, companies are required to **notify** affected consumers of a "**security breach**" (unauthorized access that comprises the security or confidentiality of **protected data**).
- What is protected data?
  - Typically, the kind that can lead to identity theft. E.g., name **plus** (1) government issued IDs; (2) financial account information; and (3) credit card information.
- In some states, must also notify government authorities, the media, and potentially post notices on website
- 11 states affirmatively require written data security programs

Security Breaches: Prevention

McDermott Will & Emery

- Have a Proper Background Screening Program for new hires and vendors
- Review contracts with IT Vendors
- Pre-Arrange a Breach Service Provider, Outside Counsel and Reputational Risk Advisor
- Provide e-Learning to workforce on safeguarding data
- Keep General Counsel's office current to state disclosure laws, federal regulations, foreign requirements and updates
- Develop an Incident Response Plan
- Conduct annual Risk Assessments
- Hold an internal "Privacy" workshop to identify vulnerabilities.
- Consider Privacy and Network Security (Cyber Risk) Insurance as a financial protection

Just Had A Breach, Now What Do We Do?

McDermott Will & Emery

- To whom do we report what happened?
- How do we investigate the incident?
- What was on the laptop?
- How do we really know?

- What jurisdictions are involved?
- What are our notification obligations?
- What are the lessons learned?
- How do we make sure this does not happen again?

Security Breach: 5 Step Response

McDermott Will & Emery

1. Discovery
2. Gather Incident Response Team
3. Investigation
4. Remediation
5. Notification (e.g., business partners, consumers, agencies)
6. Post-incident review: Learning from mistakes, applying best practices

Incident Response Team

McDermott Will & Emery

Investigation and Remediation

McDermott Will & Emery

- Notify Team immediately
- Designate point person for:
  - Technical investigation
  - External communications
  - Regulators (including Card Associations)
  - Law enforcement
  - Insurance claims
  - Restoration of system
- Engage Forensic consultant to preserve evidence of event
- Keep fingers off the crime scene
- Communications issues

Consumer Notification

McDermott Will & Emery

Seven Key Questions:

1. What information was involved?
2. Was data improperly accessed, acquired or disclosed?
3. Likelihood of misuse (may not be relevant to notification)?
4. Was data protected? (Passwords, Encryption, Redaction)
5. Where do the individuals reside? (look to that state's law)
6. Are credit cards involved?
7. Do we have mailing address for all involved?

Managing and Mitigating Legal Risk

McDermott Will & Emery

- 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
- Evaluate your privacy promises/standards
- 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

Managing and Mitigating Legal Risk

McDermott Will & Emery

- 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

Questions to Ask When Working with Personal Data

McDermott Will & Emery

- What data do you need?
- What is the level of sensitivity of this data?
- How did you get this data?
- For what purpose did you receive it?
- For what purpose(s) do you want to use it?
- Who will be able to see it?
- Have you been / can you be transparent about this use / access?
- What are the risks of using this data in this way?
- Can you mitigate those risks through better security or through using less data?
- How long do you need the data for?
- What do you do with the data when you are done?

Quick Hit – Privacy – Loyalty Cards

McDermott Will & Emery

- Loyalty Cards: Purchases are recorded and the data sold for marketing purposes.
- These purchasing records are being sold to Life and Health Insurance Companies who then evaluate your rates based on your food and non-prescription spending habits.

-Source: Bottom Line Winter 2014

LFIGS – HIPAA Task Force

McDermott Will & Emery

- HIPAA (1996)
- Hi-Tech (Compliance Requirement February 2010)
- Provisions of the Final Omnibus Rule – January 2013
- LFIGS III – Report – Target Publish: Summer 2014

The Evolving Information Governance Professional

McDermott Will & Emery

- Expansion and re-branding of Core Services
- Legal Holds Management
- Internal Discovery
- Controlled Intake and Release of Information
- DMS Governance
- Retention and Disposition
- Imaging
- The Information Governance Professional

THANK YOU!

McDermott Will & Emery

- Appreciation to Heather Egan Sussman, Esq. and Ann Killilea, Esq. of McDermott
- The ARMA-GWDC Chapter
- Archive Systems for Sponsoring today's presentation
- Questions?