DICKINSON WRIGHT PLLC presents

Privacy Rights and Data Security Compliance

Legal and Business Best Practices

SecureWorld Expo - Detroit 2011
October 6, 2011

Brian Balow
Partner
BBalow@dickinsonwright com

Tatiana Melnik
Associate
TMelnik@dickinsonwright.com

Outline

I. Privacy
   A. History
   B. Foundation
   C. Why It Matters Today
II. Data Security
   A. A Few Examples
   B. Best Practices

Outline

I. Privacy
   A. History
   B. Foundation
   C. Why It Matters Today
II. Data Security
   A. A Few Examples
   B. Best Practices

Privacy: A Bit of History

The Foundation of Privacy

What is "Privacy"?

The foundation of Privacy

- **Federal Laws**
  - US Constitution
  - Statutes
    - Federal Trade Commission Act (1914) - Section 5
    - Electronic Communications Privacy Act (1986)
    - Computer Security Act (1987)
    - Gramm-Leach-Bliley Act (1999)
    - Health Insurance Portability and Accountability Act (1996) and the more recent Health Information Technology for Economic and Clinical Health (2009)
    - *Many* more…

The Foundation of Privacy

- U.S. Constitution
  - Griswold v. Connecticut (emanations from penumbras)
  - Roe v. Wade – the right of women to choose
  - Whalen v. Roe - privacy v. the public interest

The Foundation of Privacy

- U.S. Constitution: Context Matters
  - **"The Constitution does not explicitly mention any right of privacy"** - Roe v. Wade
  - "Zones of privacy" - Griswold v. Connecticut
    - First Amendement: Right of association
    - Third Amendment: Right not to have to quarter soldiers
    - Fourth Amendment: Right against unreasonable search and seizure ("expectation of privacy")
    - Fifth Amendment: Right against self-incrimination
    - Ninth Amendment: Preservation of unenumerated rights

The Foundation of Privacy

- U.S. Constitution: Context Matters
  - Analogy = Potter Stewart's famous quote, holding that the Constitution protected all obscenity except "hard-core pornography." Stewart wrote, "I shall not today attempt further to define the kinds of material I understand to be embraced within that shorthand description; and perhaps I could never succeed in intelligibly doing so. But *I know it when I see it*, and the motion picture involved in this case is not that."
  - So it goes with "privacy" under the Constitution.

The Foundation of Privacy

- Federal Legislation: Context Still Matters
  - Targeted Information: Financial (GLBA), medical (HIPAA)
  - Targeted Constituency: Consumers (FTC Section 5), children (COPPA)
  - Specific identification of information deemed to be "private"
  - Specific identification of obligations regarding the use of particular information

The foundation of Privacy

- **State Laws**
  - Various state statutes addressing
    - Social Security Numbers
    - Drivers licenses
    - Protection of health care information
    - Recordkeeping and data destruction
    - **Breach disclosure**
- **Industry Standards**
  - PCI DSS

The foundation of Privacy

- **International Laws**
  - E.U. Privacy Directive 95/46/EC
    - Addresses the collection, use, processing, and movement of personal data
  - EU Internet Privacy Law of 2002 (Directive 2002/58/EC)
    - Protects data in electronic transactions
  - Individuals countries have their own laws

The Foundation of Privacy

- **Laws Govern**
  - What information can be collected
  - How it must be stored and secured
  - Under what circumstances it can be shared
  - Under what circumstances it can be disclosed
  - Requirements for responding to data breaches and data losses
  - Penalties for data breaches and data losses

Outline

I. Privacy
   A. History
   B. Foundation
   C. Why It Matters Today

II. Data Security

A. A Few Examples
B. Best Practices

A Few Examples

- **Citigroup** (May/June 2011)
  - More than 360,000 accounts impacted
  - Breach occurred on May 10, notified those impacted on June 3
  - Stole names, account numbers and email addresses
    - By logging into the Citi Account Online website and guessing account numbers (address bar)
    - *PCI Compliance?*
  - In June, Citi confirmed that had incurred about $2.7 million in losses due to fraudulent charges

A Few Examples

- **Lockheed Martin** (May 2011) as a result of the breach of **RSA Security** (March 2011)
  - RSA is the maker of SecurID
  - Breach occurred in March but did not disclose until June
    - Disclosure appears to have been prompted by an attack on Lockheed in May
  - RSA breach from a Phishing attach - Excel file called "2011 Recruitment Plans.xls"

A Few Examples

- **Sony** (April/May 2011)
  - Gaming network infiltrated
    - Problems began after it sued George Hotz
    - Appears that "Anonymous" was not pleased and began a DoS
    - Hacker(s) took advantage; entered system and stole data (Anonymous has denied responsibility for breach)
  - More than 100 million users affected
    - Stolen names, passwords birth dates, and maybe credit cards
  - Cost of repair? As of May, up to $171 million *(ZDNet)*

A Few Examples

- The number of and size of data breaches continues to rise
  - HITECH - mandatory breach reporting for those in the healthcare industry
    - If over 500 individuals impacted - public shaming
    - As of Oct. 4, 2011 - 330 reports, **with 21 organizations submitting more than once**, affecting more than 11 million records
  - State reporting obligations
  - Federal laws on the horizon?

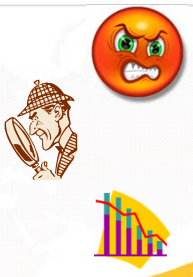
For more examples of data breaches please see http://datalossdb.org

Enforcers

- **Federal Trade Commission**
  - Section 5
  - Actions against - Microsoft, Eli Lilly, Pet Co, etc.
- **State Attorneys' General**
  - State Laws
  - Actions against - HP, Lifetime Fitness, Facebook, etc.
- **Office of the Civil Rights (HHS)**
  - HIPAA/HITECH
  - Actions against - U of Cali, Gen. Hospital Corp., Cignet Health
- **Private Plaintiffs**
  - Please see Michigan Bar article included in packet

Impact of Data Breaches

- Angry Customers
- Negative Publicity
- Tarnished Reputation
- Embarrassment
- Investigations - State AGs
- Lawsuits, Fines and Penalties
- Financial Losses

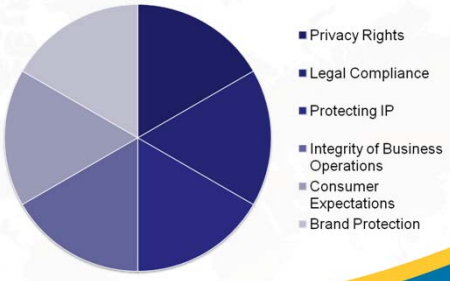


Impact of Data Breaches

- Expensive to handle
  - $268 per record - cost to rapidly respond to average data breach *(Ponemon nstitute, 2010)*

Breach Type	Cost 2010	Cost 2009
First timer YES	$326	$228
Malicious or criminal attack YES	$318	$215
Third party mistake YES	$302	$217
Quick response YES	$268	$219
Lost or stolen device YES	$258	$225
Security effectiveness NO	$255	$207
CISO leadership NO	$232	$236
External consulting support NO	$229	$231
Negligence NO	$227	$237
System failure NO	$216	$225
System failure YES	$210	$166

Reasons for Data Security



Best Practices

- Take on only the liability that is necessary
- Live up to advertised promises
  - FTC - Section 5
    - Enforces privacy policies as promises made to consumers
    - Google Buzz action - enrolling users without their explicit consent in violation of Google's own privacy policy

Best Practices

- Look to standards organizations
  - NIST Standards
    - Data at rest
    - Data in motion
- Plan ahead
  - Costs an average of $326 per record to respond if it is an organizations first time
    - Costs can be defrayed by planning ahead
    - Risk assessment
    - Thoughtful policies and procedures

Best Practices

- Training and Awareness
  - Breaches happen, this is a part of living with IT
  - Training staff will minimize risks of internal breaches
  - Rogue employee defense
    - Can shield employers from liability to the extent the conduct occurred in spite of and contrary to reasonable safeguards, including documented *training*
- Enforce Policies and Procedures
- Audit for Compliance and Review Policies and Procedures

This slide presentation is informational only and was prepared to summarize relevant legal consideration when formulating a social media policy. It does not constitute legal or professional advice.

You are encouraged to consult with an attorney if you have specific questions relating to any of the topics covered in this presentation, and Dickinson Wright would be pleased to assist you on these matters.