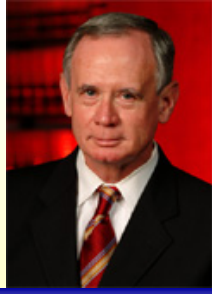
Internet Law Update: 2008

Wildman Harrold
Attorneys and Counselors

William J. Cook
June 27, 2008

First 2008

Bill Cook



- Partner, Wildman Harrold, Chicago
- Intellectual Property, Internet and Web law (Business Continuity and Security)
- Chambers 2008
- 90 trials
- Expert presentations on Internet liability before U.S. House Judiciary Comm., GAO, FCC
- Extensive experience representing retailers on PCI matters
- Chicago IMNA Board Member, Immediate Past President
- Former Head of US DOJ Computer Crime Task Force; Counter-Espionage Coordinator and Counter-Terrorist Coordinator; DOJ FEMA Coordinator (Chicago)
- NRC Committee on Critical Infrastructure Protection and the Law

First 2008

2008 Internet Law Update Summary

- Privacy drives security and corporate liability, but fails to provide relief to victims under case law
- Organization liability for loss of databases: Michigan case and state law
- Civil computer fraud must include damage and loss
- PCI standards are being used successfully by banks, regulators and legislative groups to punish retailers – whether or not they are responsible
- Insider threats continue to be the biggest danger-creating loss, regulatory exposure and proof issues
- E-discovery is the greatest legal threat facing IT staff
- EU compliance enforcement 5 to 6 years behind US courts

First 2008

Nature of the Threat 2008

- Credit card losses in 2007=$5.49 billion
  - Continued growth in Russian & Ukrainian organized crime activity for next 5 to 6 years (USSS)
  - Legitimate security technology companies failing in Russia due to employment by hostile technologies
  - $100,000 per day profit maximum due to handling issues
  - 4/08: Belgium company PCI compliant, but hacked for 4.2 million cards the same day
- Advanced Persistent Threat
  - DOD talk for alleged dedicated Chinese state sponsored hacking
  - Initial focus on DOD facilities and contractors
  - Now focus said to be private corporations
  - Regulatory backlash

First 2008

Scope of PCI

- Enforcement of PCI DS Standards across all related retail areas
  - Healthcare
  - Higher education
  - Utilities
  - State and Local Government
  - Insurance
  - Banking

First 2008

Duty to Provide InfoSec

- Major trend driven by expansion of privacy law
  - Expanding across all industries
    - Not just financial and healthcare sectors
    - Impact on range of corporate deals
  - Applies to most corporate data
    - Not just personal data
    - Also financial, transactional, tax, confidential, etc.
- It is all about protecting the stakeholders
  - Shareholders / investors, employees, customers and prospects, interests of regulatory agencies, unrelated third parties, national interests

Duty to Provide InfoSec

- Many sources, no single law or regulation
- U.S. Federal laws and regulations
  - Electronic records generally – E-SIGN
  - Financial records – Sarbanes-Oxley
  - Tax records – IRS
  - Other records – SEC, FDA, HHS, etc.
  - Personal information
    - GLBA (financial industry)
    - HIPAA (healthcare records)
    - COPPA (children)
    - Safe Harbor (EU source data)
    - FTC Section 5 (all industries)

Duty to Provide InfoSec

- State laws and regulations
  - Electronic records generally – UETA
  - General security laws
    - Obligations to implement security
    - Data destruction laws
  - Other specific laws, e.g., EFT, insurance, etc.
- Evidentiary requirements
  - e.g., *AmEx* case
- Contractual commitments

Duty to Provide InfoSec

- Tort law
  - *Bell v. Michigan Council* – failure to provide security for employee data
  - *In re Verizon* – failure to apply patches
  - Negligent enablement
- FTC and State AG enforcement actions
  - False representations and promises
  - Unfair business practices
- International Laws
  - EU Data Protection Directive
  - EU country implementing laws and regulations
  - Argentina, Australia, Canada, Japan, and others

First 2008

Duty to Provide InfoSec

- Because security is a legal obligation, what do you have to do?
  - Do you have to encrypt this data?
  - Are passwords sufficient or do you need a token?
  - Is it OK to allow Wi-Fi access?
- A “legal” standard for “reasonable security” is developing in the U.S.
- It is focused on a “process” rather than specific technical requirements

Satisfying the Legal Standard Depends on the Company's Process

- Identify the assets to be protected
  - Both (i) under company control and (ii) outsourced
- Conduct risk assessment
  - Identify and evaluate threats, vulnerabilities, and damages
  - Consider available options
- Develop and implement a security program
  - That is responsive to the risk assessment
  - That addresses the required categories of controls
- Address third parties
- Continually monitor, reassess, and adjust
  - To ensure it is effective
  - To address new threats, vulnerabilities, and options

Executives & InfoSec

- Who?
  - Not just CIO and risk management functions
  - CEO, CFO, GC, Senior Management
  - Board of Directors
- What?
  - Approve the security program
  - Oversee development, implementation, and maintenance of the security program
  - Require regular reporting

First 2008

Duty to Disclose Security Breaches

- Duty to disclose security breaches to:
  - Those who may be affected/injured
  - Regulators, enforcement agencies, etc.
- Obligation akin to “duty to warn”
- Started in California in 2003, now 34 states impose some obligation
- Laws differ, but all based on California model
- Having a major PR impact

First 2008

Breach Notification Legal Requirements

- Covered information – “name” plus one of:
  - SSN
  - Drivers license number
  - Financial account or credit card number
  - Other
- Triggering event
  - Any breach of security, *or*
  - Breach with reasonable likelihood of harm
- Obligation on breach
  - Notify persons whose information compromised
  - Notify state enforcement agencies – (some states)
  - Notify credit agencies – (some states)

First 2008

Breach Notification Legal Requirements

- Timing of the notice
  - In the "most expedient time possible and without unreasonable delay"
  - Delay OK for law enforcement investigation or to take necessary measures to determine the scope of the breach and restore system integrity
- Form of notice
  - In writing
  - Electronic form (but must comply with E-SIGN)
  - Substitute notice
  - Alt – follow company incident response plan
- Penalties
  - State enforcement (e.g., A.G. office)
  - Some private right of action

First 2008

Data Security Cases

- Former or Current Employees
- Company officers
- Vendors
- Agents
- Competitors

First 2008

Employee Theft

- 49% of US companies had a data theft in 2007 (CM)
- US companies lost 5%($625B) of annual revenues to employee fraud (ACFE)
- 70% of employee theft is committed by employees with less than 30 days (Unicru Inc.)
- Only 8% of internal fraud committed by someone with “a prior”
- Average insider job takes place for 18 months before it’s identified (Bankers Ideanet)

First 2008

Liability Created by Vendors

- Theft from global telecommunications client's healthcare vendor included computers with personal data on the hard drives
- Client's employee database of health information, personal credit cards and other personal information missing
- Actions taken:
  - HIPAA exposure identified
  - Potential employee legal action(s) identified
  - Vendor forced to meet ISO 17799 and corporate standards
    - Prepared and oversaw E&Y ISO 17799 security audit and evaluated compensating controls
  - Negotiated vendor contract changes and remediation
  - Rewrote security provisions for vendor contracts

Trade Secret Theft by Defecting CEO

- CEO and 5 key employees left ecommerce client with trade secret information to start up competing company
- Actions taken:
  - Immediately walled off data at new employer
  - Checked client's records for data transfers
  - Forced forensic analysis of departed hard drives to locate stolen information
  - Evaluated Economic Espionage Act referral
  - Opponents clearly understood liability and embarrassment if they did not cooperate
  - Used threat of litigation to achieve client's business strategy without actually having to go to court
  - Negotiated return of all data and essentially shut down potential competitor

First 2008

Justifying Competitive Intelligence Gathering

- Client's President accessed competitor's FTP site and obtained customer lists, vendor price lists, source code
- Criminal and civil actions filed against Client at the same time as FBI search of corporate offices
- Actions taken:
  - Successfully countered civil action by analysis of competitor's security practices, FTP site permissions and actual practices
  - Assisted in PR response

First 2008

Identity Theft

- Now possible for consumers to strike back on banks and credit card companies
- Wolfe case
- Reality is different

First 2008

Organizations Required to Protect Employee Information

- Michigan union found negligent in failing to protect membership information from identity theft
- Stolen laptop with PCI Audit results on Limewire
- Going in to get the stolen laptop and information

First 2008

CFAA: Damages Plus Loss Required

First 2008

E-discovery

- Safe Harbor is very shallow
- Rule 37 allows parties to delete data lost as a result of routine, good faith operations
  - Judge's discretion
- Most companies don't qualify due to lack of internal controls
- Lack of written retention policies and actual pas practices
- Spoliation sanctions

First 2008

- William J. Cook
- Wildman Harrold Allen & Dixon
- 225 W. Wacker Dr.
- Chicago, Il. 60606
- cook@wildman.com
- 312-201-2399