SIDLEY AUSTIN LLP

SIDLEY

BEIJING BRUSSELS CHICAGO DALLAS FRANKFURT GENEVA HONG KONG LONDON LOS ANGELES NEW YORK SAN FRANCISCO SHANGHAI SINGAPORE TOKYO WASHINGTON, D.C.

Privacy: The Importance of Getting It Right

2006 CSO Perspectives Conference

Ed McNicholas

Recent Reported HR Data Breaches

Employer	Number affected	How
Bank of America	1.2 million	Theft of tapes
SAIC	45,000	Stolen equipment
Honeywell	19,000	Data posted on web
Time Warner	600,000	Lost back-up tapes
MCI	16,500	Stolen laptop
Purdue	11,360	Unauthorized access
US DOJ	80,000	Stolen laptop
Motorola	30,000	Stolen computers
FDIC	6,000	Unauthorized access
Eastman Kodak	5,800	Stolen laptop
San Diego County	32,000	Hacking
US Air Force	33,000	Stolen log-in
Boeing	161,000	Stolen lap-top
Ford Motor Co.	70,000	Stolen computer

Other Data Breaches

Employer	Number affected	How
ChoicePoint	163,000	Bogus accounts established by ID thieves
PayMaxx	25,000	Exposed online
DSW	1.4 million	Hacking
LexisNexis	310,000	Passwords compromised
University of California, Berkeley	98,400	Stolen laptop
Boston College	120,000	Hacking
Nevada Department of Motor Vehicles	8,900	Stolen computer
Northwestern University	21,000	Hacking
Polo Ralph Lauren/HSBC	180,000	Hacking
Ameritrade	200,000	Lost backup tape
Wachovia, Bank of America, PNC; Commerce Bancorp	676,000	Dishonest insiders

What Happened to ChoicePoint?

- ChoicePoint accumulated and disclosed information including many unique personal identifiers, such as SSNs.
- Subscribers could purchase the information contained in ChoicePoint's databases
- Ultimately notified 163,000 consumers of possible misuse of personal information.
- ChoicePoint's security breach allegedly resulted in at least 800 reported cases of identity theft.

Consequences ChoicePoint?

- FTC obtained record $10 million fine and $ 5 million restitution
- ChoicePoint now must establish, implement and maintain a “comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers.”
- ChoicePoint must submit to biennial assessments from an independent third party of its security program, with reports submitted to the FTC, through the year 2026.

Lessons from ChoicePoint

CHOICEPOINT

- Discontinue controversial products after media firestorm
- Disclaim responsibility and focus on the hacker
- Deem General Counsel to be Chief Privacy Officer after breach
- Dribble conflicting stories over several days then later issue 8-K with more facts

RECOMMENDED

- Assess risks in advance through privacy reviews and data mapping
- Investigate failure of security fully
- Create CPO and build privacy compliance infrastructure in advance
- Conduct a serious internal investigation and release accurate information in one news cycle

Data Breach Consequences

20% of individuals who receive a data breach notification end their relationship with the company that provides it

40% consider ending the relationship

5% hire lawyers

-- Survey data rough, but point taken

Data Breach Legislation

- Currently at least 24 different state laws
- California started it …
  - Requires notice to consumers of breach in the security, confidentiality, or integrity of unencrypted computerized personal information held by a business or government agency (Cal. Civ. Code 1798.80-1798.82)
- Federal legislation in committee

State Affirmative Security Obligations

- California AB 1950
  - requires specified businesses to use safeguards to ensure the security of Californians' personal information (defined as name plus SSN, driver's license/state ID, or financial account number) and to contractually require third parties to do the same
  - does not apply to businesses that are subject to other information security laws, such as the federal financial and medical information security rules

California Privacy Laws

- California Constitution, Article 1, section 1
- Office of Privacy Protection - California Business and Professions Code sections 350-352
- Automobile "Black Boxes" Vehicle Code section 9951
- Birth and Death Certificate Access - Health and Safety Code sections 103525, 103525.5, 103526, 103526.5, 103527, and 103528.
- Birth and Death Record Indices - Health and Safety Code sections102230, 102231 and 102232.
- Cellular Telephone Number Directory – Public Utilities Code section 2891.1
- Computer Spyware – Business and Professions Code section 22947 et seq.
- Consolidation of Identity Theft Cases - Penal Code section 786.
- Consumer Credit Reporting Agencies Act Civil Code section 1785.1-1785.36
- Court Records: Protection of Victim and Witness Information – Penal Code section 964
- Credit Card Address Change - Civil Code section 1747.06
- Credit Card/Telephone Service Address Change, Civil Code section 1799.1b.
- Credit Card or Check Payment- Civil Code sections 1725 and 1747.8.
- Credit Card Full Disclosure Act, Civil Code sections 1748.10 - 1748.12
- Credit Card Number Truncation - California Civil Code section 1747.9
- Credit Card "Skimmers" - Penal Code section 502.6.
- Credit Cards, Substitutes - Civil Code section 1747.05.
- Debt Collection: Identity Theft Victim Rights - Civil Code section 1788.18.
- Destruction of Customer Records - California Civil Code sections 1798.80 and 1798.84
- Driver's License Information Confidentiality - Vehicle Code sections 1808-1821.
- Driver's License Information, Scanning or "Swiping" - Civil Code section 1798.90.1.
- Electronic Eavesdropping - Penal Code sections 630-637.9
- Electronic Surveillance in Rental Cars – Civil Code section 1936
- Employment of Offenders - Penal Code sections 4017.1 and 5071 and Welfare and Institutions Code section 219.5.
- Fair Debt Collection Practices Act, Civil Code sections 1788-1788.33
- Financial Information Privacy Act, California- Financial Code sections 4050 - 4060.
- Identity Theft: Victim Access to Records on Fraudulent Transactions or Accounts - California Civil Code section 1748.95, California Financial Code sections 4002 and 22470. .
- Identity Theft - California Penal Code sections 530.5-530.8

And . . .

SIDLEY AUSTIN LLP
SIDLEY

California Privacy Laws

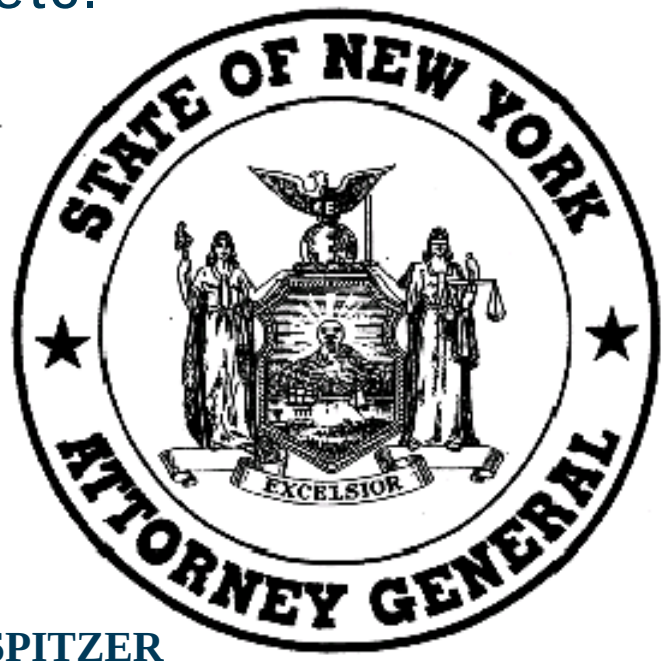
OFFICE OF
Privacy
Protection

- Identity Theft Victim's Rights Against Claimants - Civil Code section 1798.92-1798.9
- Information Practices Act of 1977- California Civil Code section 1798 et seq.
- Information-Sharing Disclosure, “Shine the Light” – Civil Code sections 1798.82-1798.84
- Insurance Information and Privacy Protection Act, Insurance Code section 791 et seq.
- Investigative Consumer Reporting Agencies Act, California Civil Code sections 1786-1786.60
- Legal and Civil Rights of Persons Involuntarily Detained - Welfare & Institutions Code section 5328
- Library Records, Confidentiality - Government Code sections 6254, 6267 and 6276.28
- Mandated Blood Testing and Confidentiality to Protect Public Health - California Health & Safety Code sections 120975-121020
- Medical Information, Collection for Direct Marketing Purposes – Civil Code section 1798.91
- Medical Information Confidentiality - California Civil Code sections 56-56.37
- Online Privacy Protection Act of 2003 - Business & Professions Code section 22575-22579
- Patient Access to Health Records - California Health & Safety Code section 123110 et seq.
- Personal Information Collected on Internet - California Government Code section 11015.5
- Public Records Act - California Government Code sections 6250-6268.
- Search Warrant, Penal Code section 1524.
- Security Breach Notice - Civil Code sections 1798.29 and 1798.82 - 1798.84
- Security of Personal Information – Civil Code section 1798.81.5
- Social Security Number Confidentiality - California Civil Code sections 1798.85-1798.86, 1785.11.1, 1785.11.6 and 1786.60
- Social Security Number Confidentiality in Family Court Records - California Family Code section 2024.5.
- Social Security Number Truncation on Pay Stubs – Labor Code section 226
- Spam Laws - Business and Professions Code sections 17529 and following and 17538.45.
- State Agency Privacy Policies, Government Code section 11019.9.
- Statute of Limitations, Penal Code section 803.
- Supermarket Club Card Act - Civil Code section 1749.60 and following.
- Telecommunications Customer Privacy - Public Utilities Code sections 2891-2894.10.
- Telemarketing: State do-not-call list - Business and Professions Code sections 17590-17594.
- Unsolicited Cell Phone/Pager Text Ads - Business and Professions Code section 17538.41.
- Veterans' Discharge Papers, Notice of Public Record Status - California Government Code section 27377.
- Warranty cards - Civil Code section 1793.1.

SIDLEY AUSTIN LLP
SIDLEY

Growing State Enforcement

- "Private Attorney General" activity
- State Attorneys General responding to public fears after ChoicePoint, etc.
- After ChoicePoint, a large group of state attorneys general demanded that ChoicePoint provide their citizens with the same notices required under California law
- Multiple security bills pending in various state capitols



ELIOT SPITZER
Attorney General

Common Law Tort Security Obligations

- Negligence
- Invasion of Privacy Tort Claims
  - Intrusion upon seclusion – intentional intrusion upon the seclusion of another or private affairs or concerns that would be highly offensive to a reasonable person
  - Public disclosure of private facts – Giving publicity to a matter concerning the private life of another when highly offensive to a reasonable person and not of legitimate concern to the public
- Beware the *T.J. Hooper* -- reasonable, not common

Federal Regulatory Frameworks

- Financial institution regulation under Gramm-Leach-Bliley Act
- Regulation of personally identifiable health information under HIPAA
- Duty to assess internal controls under Sarbanes-Oxley §404
- FTC's "unfair" and "deceptive" standards.

The trend is clearly toward more regulation of information. There is increasing public pressure to keep data secure, and the plaintiffs' bar is no doubt looking for class-action opportunities in this area.

FTC Attention

FTC has taken an aggressive stance toward privacy enforcement in recent years

- 12 Data Security Cases
  - Moving from deception to unfairness
  - Deception is based on not doing what you say you will do in a privacy policy or contract
  - Unfairness is based on evolving, objective standards
- 6 Spyware / Adware Cases
- 12+ Financial Pretexting Cases
- 80+ SPAM cases

FTC Attention -- *BJ's Wholesale*

The *BJ's Wholesale decision* "should provide clear notice to the business community that failure to maintain reasonable and appropriate security measures in light of the sensitivity of the information can cause substantial consumer injury and violate the FTC Act."

– Chairman Majoras, testifying before Senate Committee on Commerce, Science, & Transportation (6/16/05)

- Comply with your privacy promises
- Security programs must adapt to changing threats
- Security programs appropriate to circumstances

FTC Attention

What might the FTC ask for in the event of a security breach? – EVERYTHING!

- All policies adopted or statements made regarding the collection, disclosure, use and protection of personal information
- All documents sufficient to identify and describe in detail all systems and/or databases that collect, maintain, store, transmit or otherwise handle personal information
- Any risk assessments conducted to identify risks to the security and confidentiality of personal information
- All documents that set forth, assess, evaluate, question, challenge, contest or recommend changes to the security procedures, practices, policies, and defenses with respect to personal information
- All service providers that receive, maintain, process or otherwise are permitted to access personal information
- All documents that reflect, concern or relate to incidents of possible unauthorized access to personal information
- EU Privacy safe harbor compliance documentation

Global Privacy Challenges

- Emerging State Privacy Regimes -- California, New York . . . .
- U.S. Federal sector-specific privacy/security regimes: financial (GLB), medical and healthcare (HIPAA), communications, marketing, U.S. PATRIOT Act
- The European Union Directive and International Data Transfer Regimes: Safe Harbor, Contracts, etc.
- New International Privacy regimes – Canada, Japan, APEC, and . . . the Rest of the World
- Employee monitoring and workplace privacy
- New norms from Litigation

European Union Data Protection Directive (95/46/EC)

- 1995 – i.e., Pre-www
- Provides principles for privacy, security, access, onward transfer of personally identifiable information in the EU
- Limits collection, processing, and retention of personal data
- Allows onward transfer of personal information only to countries that provide “adequate” protection

- U.S. DOES NOT HAVE ADEQUATE PRIVACY PROTECTIONS ACCORDING TO THE EU
- ANY CORPORATION OPERATING IN EU IS AUTOMATICALLY SUBJECT TO THE EU DATA PROTECTION DIRECTIVE

EU Data Directive - Compliance Options

- Safe Harbor
  - negotiate agreement between U.S. Department of Commerce and European Commission
- Model Contracts
  - model language as proposed by EU Commission
- Binding Corporate Rules
  - internal rules regarding privacy and security adopted by the company and approved by each EU DPA
- Consents and Other Ad Hoc Methods
  - obtain consents for every transborder data transfer
- Ostrich mode

Where Are We On Privacy?

- Privacy 1.0 –

  Fine-print notices
  Conflicting international regimes
  Little to no real EU or other enforcement
  US absent; sporadic cases

- Privacy 2.0 –

  “Layered” notices
  Emerging global standards
  Scattered US and EU enforcement
  Occasional regulator focus

- Privacy 3.0 -

  Useful consumer choice
  Global trade consensus
  Significant US, EU and other enforcement
  US Privacy regulators

Where Are We On Privacy? -- Variables

- Plaintiffs' Bar
- No Harm from "mere" privacy loss? *Conboy*
- Regulator?
  - State AGs
  - FTC
  - EU DPA-model
- Standards Evolving
- Microsoft call for comprehensive federal privacy legislation
- ID Theft Cost-Sharing Litigation

Mind the Compliance Gaps

Ability to deliver on privacy compliance obligations is often being outpaced by market, technological, and organizational changes

- Vendors, Vendors, Vendors
- New Technologies
  - Privacy Impact Assessments
- Organizational Commitment

From Privacy Compliance To Building Brand Value and Client Trust

SIDLEY AUSTIN LLP
SIDLEY

Why is Privacy Awareness Important?

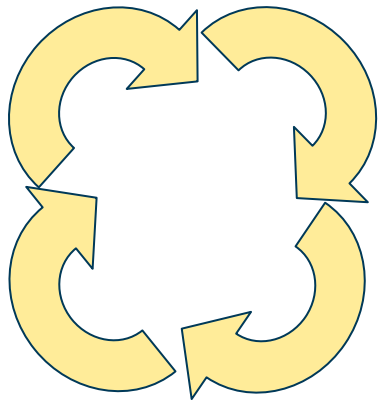
"In today's corporate environment, customer and employee privacy have become a top security initiative... All our findings indicate that companies which demonstrate and communicate a strong commitment to the protection of personal information have realized an increase in customer confidence and loyalty to their brand."

- Larry Ponemon of the Ponemon Institute
2005 Benchmark Study of Corporate Privacy Practices

Creating a Culture of Privacy

Assess

Build



Audit

Certify

Key Ingredients to a Culture of Privacy

- Organizational Commitment
- People
- Policies
- Processes to implement the policies
- Technologies that enable and enhance privacy

Key Oversight Issues in Creating a Culture of Privacy

- Regularly requiring honest assessment of risks to corporate operations and managing identified threats and vulnerabilities;
- Establishing corporate policies governing information usage and employee conduct;
- Incorporating best practices and standards;
- Ensuring sufficient funding is allocated to develop and maintain an enterprise program;
- Building the culture through education, training and measuring compliance with meaningful metrics; and
- Conducting regular reviews and audits.

Key Operational Issues in Creating a Culture of Privacy

- Education, not training
- Job Relevance
- Visible executive management support
- Tie to business / mission success
  - Building the brand
  - Maintaining public confidence / trust
  - Minimizing risk of extensive regulatory oversight
- Measurement, Recognition and Reward
- Market / Stakeholder Feedback

Global Data Privacy Assessment – Possible Items

- **Factual assessment**
  - Map how personal data are collected, stored and transferred
- **Cultural assessment**
  - Assess privacy training and employee awareness
  - How does privacy fit with the goals of the organization?
- **Legal assessment**
  - Analyze existing policies and procedures
  - EU compliance
  - Review website policies
  - Registrations with DPAs
- **Security assessment**
  - Review information security vulnerabilities and protections
- **Third party service providers and their policies.**

Global Data Privacy
Founding a Culture –Action Items

- Create or enhance a privacy structure.
  - Chief Privacy Officer / Leader
  - Coordinate Local Privacy Leaders
- Educate and train employees
- Implement compliant policies and procedures
- Create internal controls, management oversight and reporting
- Prepare for possible failure of those plans and other contingencies:
  - Dispute resolution
  - Data breach incident response
  - Information continuity planning

Global Data Privacy
Certifying Compliance – Possible Action Items

- Internal controls and management oversight
- Ensuring Compliance
  - Integrate privacy into core values and standard operating procedures
  - Exercise oversight of your business partners
  - Monitoring new laws and industry standards
  - Annual, independent verification
- Your Board is relying on internal controls over key information databases to satisfy compliance under Sarbanes-Oxley

Contact Information

Edward R. McNicholas

Sidley Austin LLP
1501 K Street, NW
Washington, DC 20005

emcnicholas@sidley.com

(202) 736-8010

www.sidley.com/cyberlaw

SIDLEY AUSTIN LLP
SIDLEY