

Cutting Edge Issues in Technology Law  
*Seattle December 7-8, 2006*

## Privacy & Security Recent Developments

Francoise Gilbert  
*CEO - IT Law Group*  
*www.itlawgroup.com*  
*Palo Alto, California*

IT LAW GROUP

© 2006 IT Law Group

## SECURITY TODAY

- Significant expansion of corporate obligations to ensure the security of electronic information
  - Personal Information
    - Customers (and other outsiders)
    - Employees
  - Company Information
    - Reporting requirements (e.g., SOX)
    - Record keeping requirements (e.g., evidence, tax)

IT LAW GROUP

2

## SECURITY TODAY

- **Duty to Protect:** Provide reasonable security for corporate and personal data, and information systems
  - Prevent breaches
  - Destroy data
  - Protect integrity of data; preserve evidence
- **Duty to Disclose:** Disclose security breach
  - To those who may be adversely affected by such breaches
  - To others (AG, Consumer Protection Board, State Office of Cybersecurity, Consumer Reporting Agencies)

IT LAW GROUP

3

## DUTY TO PROTECT

- **Corporate Governance Legislation**
  - Sarbanes Oxley Act Sect. 302 and 404 require significant security measures to ensure that adequate internal control structures and procedures for financial reporting are in place
  - CEO and CFO are responsible for ensuring security and quality of corporate information

IT LAW GROUP

4

## DUTY TO PROTECT

- Privacy / Security Laws, Regulations
  - Require companies to implement information security measures to protect personal data they maintain
  - GLBA places responsibility for security with the Board of Directors. The Board is required to approve the written security program
  - HIPAA, COPPA
  - State laws require companies to implement reasonable security measures (California, Arkansas, Nevada, Rhode Island, Texas, Utah)

IT LAW GROUP

5

## DUTY TO PROTECT

- Authentication, integrity, retention
  - E-Sign and UETA require all companies to provide security for storage of electronic records relating to online transactions
  - IRS regulations require companies to implement information security to protect electronic tax records
- Data destruction laws
  - FACTA Document Destruction Regulations
  - State laws

IT LAW GROUP

6

## DUTY TO PROTECT

- **Abroad and International**
  - Foreign Data Protection Laws: EU Member States, Canada, Australia, Argentina, require companies to implement security measures
  - Safe Harbor: Companies self-certifying under the Safe Harbor commit to take reasonable precautions to protect personal information from loss, misuse, unauthorized access, disclosure, alteration and destruction
  - Model contracts and BCRs: also include a requirement for security

IT LAW GROUP

7

## DUTY TO PROTECT

- **FTC and State Attorneys General**
  - Have prosecuted companies for alleged failure to provide adequate security
  - Asserted that the failure to provide appropriate information security was an unfair trade practice under Section 5 of the FTC Act, even in the absence of any false representation by the defendant as to the state of its security
  - Consent decrees require implementation of security measures and appointment of an identified Privacy / Security official responsible for compliance

IT LAW GROUP

8

## FTC v. CHOICEPOINT

- ChoicePoint provided third party's personal information to subscribers who had inadequate credentials
- ChoicePoint did not have reasonable procedures to screen prospective subscribers, and turned over consumer information to subscribers whose application raised obvious redflags
- ChoicePoint received subpoenas from law enforcement authorities in 2001 alerting CP of the fraudulent activities

● Source: Federal Trade Commission

IT LAW GROUP

9

## FTC v. CHOICEPOINT

- Settlement January 2006
  - **\$10 million** in civil penalties (the largest civil penalty in FTC history)
  - **\$5 million** for consumer redress
  - Establish, implement and maintain comprehensive information security program
  - Obtain every 2 years, for the next 20 years, an audit from a 3rd party
  - Record-keeping and reporting provisions to allow FTC to monitor compliance

IT LAW GROUP

10

## CHOICEPOINT CLASS ACTIONS

- Class actions brought on behalf of individuals whose personal data were compromised by the security breaches disclosed in February 2005, and other breaches
- Class actions brought on behalf of shareholders, who allege that ChoicePoint management failed to disclose to shareholders and potential investors that the company's security measures were inadequate and ineffective

IT LAW GROUP

11

## COMPLIANCE REQUIRED

- Entities that are regulated by specific sectoral laws that outline the security measures to be taken (e.g., financial and healthcare institutions) should comply with these laws and regulations
- Organizations that are not currently regulated should take into account the FTC rulings because they define a de facto standard

IT LAW GROUP

12

## FEDERAL TRADE COMMISSION

- Current FTC rulings require:
  - Designation of appropriate personnel to oversee privacy / security program (e.g., CPO, CSO, CISO)
  - Security Program: Identifying reasonable, foreseeable internal and external risks to security, confidentiality, and integrity of personal information
  - Conducting an annual written review by qualified persons
  - Adjusting program to fit findings from reviews, monitoring, operational changes.

IT LAW GROUP

13

## ENTERPRISE SECURITY PLAN

- Crucial components for a viable enterprise security program:
  - *Budget*
  - *Individual(s) responsible for driving the project*
  - *Asset assessment*
  - *Risk assessment*
  - *Security policies and procedures*
  - *Education and training*
  - *Monitoring and testing*
  - *Review and upgrade*
  - *Same as above for third party relationships*

IT LAW GROUP

14

## DEALING WITH THIRD PARTIES

- Remember that:
  - China, India, the Philippines and other offshoring countries *do not have data protection laws, or information security laws, and may have a deficient judicial system*
  - *Some countries that do have data protection laws do not have a data protection culture. Privacy is also a cultural issue*

IT LAW GROUP

15

## DEALING WITH THIRD PARTIES

- Conduct thorough due diligence of service provider before entering into a contract
- Evaluate privacy and security policies, incident response, enforcement
- Ensure contract provides for data use restrictions, security procedures, disclosure of security breaches
- Conduct periodic audits during performance of the contract

IT LAW GROUP

16

## DUTY TO DISCLOSE

- 34 States have enacted Security Breach Disclosure Laws; there are discrepancies between these laws
- Covered entities:
  - Entities that own or license personal information (data collectors)
  - Entities that maintain third party information (service providers)
- Breach:
  - Unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of protected personal information

IT LAW GROUP

17

## DUTY TO DISCLOSE

- Protected information:
  - Individuals' name (or signature, phone number, address) in combination with
  - (a) SSN number; or (b) Driver's license number; or (c) account number, debit or credit card number and access code (or insurance policy number, passport number, medical information)
- Failure to notify:
  - Injunction
  - Injured customer may (or may not) institute civil action to recover damages
  - Cumulative rights and remedies; treble damages

IT LAW GROUP

18

## FIRE DRILL

- Given the urgency requirements in making the disclosures, and the discrepancies between applicable laws, organizations should be prepared to respond to a security breach ahead of time
- Draft and implement **Incident Response Plan**
  - *How security incident is reported internally, to whom*
  - *Core team (from Privacy, Legal, IT, Security, Communications groups)*
  - *Decision makers*
  - *Phased approach: information collection; initial assessment, etc.*
  - *Collect information to allow determination of whether notices to individuals, governments, or credit bureaus are required or recommended*
  - *Relationships w. law enforcement agencies, credit monitoring services*

IT LAW GROUP

19

## ACTION ITEMS

- Ensure appropriate measures are in place to protect personal information (Enterprise Security Plan, Incident Response Plan, as well as Disaster Recovery, Business Continuity plans)
- Weave privacy and security into M&A and corporate agreements
- Protect information held or accessible by third parties, subcontractors, outsourcing providers
  - Obligation to have adequate security measures
  - Obligation to immediately disclosure security breach
  - Periodic audits
- Review insurance coverage

IT LAW GROUP

20

## ATTORNEY'S ROLE

- Attorneys play an important role in the development and implementation of an Enterprise Security Program:
  - Develop plan, define goals and budget
  - Assess data flows, and evaluate risks
  - Understand (and communicate) compliance requirements and applicable laws
  - Create policies (high level) and procedures (daily use)
  - Provide training, and disseminate policy
  - Monitor application and revise policy as necessary
  - Establish process for enforcement, discipline of the infringers

IT LAW GROUP

21

## SUMMARY

- *Numerous laws, regulations, standards* control the collection, use, and transfer of data; and what must be done if certain data are lost How a company handles information (personal or corporate) is *critical to the balance sheet and share value*
- Any mistake will dramatically affect individuals who may be facing identity theft
- PR disaster will sink the company
- Compliance with data protection and information security laws must be addressed at the *C-Level*

IT LAW GROUP

22

<b>FOR MORE INFORMATION...</b>	
	<p><a href="mailto:fgilbert@itlawgroup.com">fgilbert@itlawgroup.com</a></p> <p>650-804-1235</p> <p><i>IT Law Group</i> 555 Bryant Street # 603 Palo Alto, CA 94301</p>
<b>IT LAW GROUP</b>	23