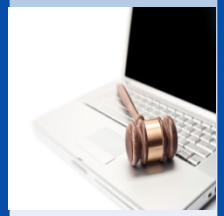
Duty to Protect Consumer Information

Emerging Legal Trends

Ann Geyer, JD
Tunitas Group



ISACA
April 1, 2009

Tunitas group

Information Protection is Expanding

Separating information from computer assets
- Protecting information ownership
- Recognizing consumer privacy rights

Safe Harbors
- Limiting liability if security is implemented

Duty to protect
- Imposing legal duties and liability to control, to warn, to avoid disclosures

Legal Perspective on Liability

Liability means

- To be accountable to another or society
- Enforceable by civil remedy or criminal punishment

Legal Perspective on Liability

Liability means

- To be accountable to another or society
- Enforceable by civil remedy or criminal punishment

In other words

- A *duty* – that is breached, that creates a wrong, that is compensable

Tunitas group

Duty is Established in Two Ways

Case Law

- Court decisions rendered in private lawsuits

Statutory Law

- Laws, regulations and enforcement actions

Private Lawsuits

Individuals sue for a legal remedy

Tort Theories

- Negligence-ordinary or professional
- Breach of fiduciary duty--directors, officers, attorneys, trustees, agents, spouses, guardians . . .
- Invasion of Privacy—disclosure of private facts
- Emotion distress—pain & suffering, fear, anxiety
- Misrepresentation—false statements inducing reliance

Contract Theories

- Breach of contract
- Breach of warranty

Tunitas group

Plaintiff's Have a High Burden under Negligence

Plaintiff must prove—Duty, Breach, Causation, Injury

Duty

- General duty -- Reasonable care to a foreseeable person
- Special duties – Duty to warn, to control, to rescue

Tunitas group

Negligence

Breach

- Balancing Test
  - Gravity/Likelihood of harm to Consumer
  - Burden/Utility to Company
- Unexcused statutory duty
- Probably negligent

Negligence

Causation—Is it reasonable to hold this defendant liable?

- Defendant's conduct is the actual cause of injury
- The injury is foreseeable
- No independent intervening force

Negligence

- Injury
  - Differs for different torts
  - Negligence
    - Must first establish personal injury or property damage
    - Emotional damages or economic losses can then be tacked on

Low Success Rate for Plaintiffs

Several recurrent difficulties

- No actual injury shown
- Can’t prove security breach caused the injury
- Injury characterized as pure economic harm
- Medical monitoring arguments not well accepted

Contract Theories

Plaintiff must have an “agreement” with the breaching party

Must have promised – *Privacy & Security Statements*

- To protect privacy
- Not to disclose
- Provide state of the art security
- Your data is safe with us

Main Contract Theory Problems

- Was the information given in exchange for the privacy statement?
- Are the damages legally certain?

Tunitas group

Security Breach Awareness Builds

100 million consumers affected by security breaches annually

Technical arms race between criminals and infosec professionals is escalating

Businesses must do better to protect consumers

Politically necessary to hold someone responsible

Identity Theft Top FTC Consumer Complaint

Rank	Complaint	No.	%
1	Identity Theft	313,982	26
2	Collection Agencies	104,642	9
3	Telemarketers	52,615	4
4	Internet Services	52,102	4
5	Check Scams	38,505	3
6	Credit Bureaus	34,940	3
7	Sweepstakes & Lotteries	33,340	3
8	TV/Cable	25,930	2
9	Banks and Lenders	22,890	2
10	Telephone Services	22,387	2
11	Computers	21,442	2
13	Internet Auction	17,294	1
15	Health Care	16,275	1

Tunitas group

FTC Steps In

Federal Trade Commission (FTC) Act

- Gives FTC broad authority to enforce consumer protection laws

Key theories applied to data security

- Deceptive or unfair trade practice (FTC § 5)
- Safeguards Rule (Gramm-Leach-Bliley)
- Fair Credit Reporting Act (FCRA)

FTC is a Formidable Adversary

Has both regulatory and enforcement authority

- Investigates
- Files charges
- Adjudicates
- Issues injunctions
- Levies fines
- Consent decrees

Named Enforcement Agency

- Anti-trust/monopolies
- False advertising
- Credit fraud
- Debt collection
- Truth in lending
- Health warnings
- Product labels
- Medical privacy

Deceptive or Unfair Practices

FTC positions itself as the arbiter of corporate data security

- Initially targeted privacy statements on websites
- Moved on to implied promise to protect information from disclosure
- Any breach is a disclosure
- Failure to implement reasonable security measures

45+ Complaints since 2000

Failure to provide reasonable security to protect sensitive customer data

Many Prominent Names

Geocities	Tower	CardSystems	Seisint
Eli Lilly	PETCO	DSW	TJX
Microsoft	BJ Wholesale	Guidance	Hannaford
Guess	ChoicePoint	LexisNexis	Geek.com

Consistent Charges

Failure to implement reasonable security measures

Using default or common passwords

Storing unencrypted consumer information

Transmitting unencrypted data on internal networks

Retaining data longer than necessary

Failing to implement detective controls

Using shared passwords for distinct administrator functions

Failing to prevent wireless access to network

Failing to employ IDS products or review audit logs

Consistent Settlements

10-20 year consent agreements

Fines from $100K to $15M

Specific requirements

- Assign a designated security official
- Implement a managed security program
- Assess risk to consumer data
- Implement reasonable security safeguards/controls
- Proactively monitor security status
- Respond to changing risk environments

FTC Targets

Companies with low security expectations and priorities

- Weak or obsolete security controls
- Limited detective controls
- Lacking a well-defined and professionally managed security program
- Failed to detect & correct problems in timely manner

FTC Security Principles

1. All companies have a legal duty to implement reasonable security
2. Security procedures must be appropriate for the level of sensitivity of the information
3. Reasonable and appropriate security measures may insulate a breach
4. Laws may be violated without a breach
5. Static security measures are not acceptable

FTC Standards for Safeguarding Customer Info

Defines reasonable security

- Designate a coordinating person
- Identify and assess risks and evaluate controls
- Design and implement program to address risks
- Regularly test and monitor effectiveness of program
- Oversee service providers who have access to protected information
- Evaluate and adjust program to address weaknesses or new risks

Tunitas group

Reasonable Security means Good Governance

Data Security is considered a Fiduciary Duty

The Board, CEO, CFO, Sr. Management

Must approve the security program

Oversee development, implementation, & maintenance

Be informed through regular reporting

In short—data security must be a visible part of corp governance

Tunitas group

Reasonable Security means Defined Process

General focus is on *process of security*
- not any specific security policy, product or standard

Legal standard is at a minimum
- Defined process--documented and communicated
- Managed process--monitored and measured

Tunitas group

A Defined Process for Reasonable Security

1. Identify the assets to be protected
   Both under company control and outsourced

2. Assess risk
   Identify and evaluate threats, vulnerabilities, and damages
   Consider available options

3. Manage by means of a documented security program
   That is responsive to the risk assessment
   That addresses the required categories of controls

4. Continually monitor, reassess, and adjust
   To ensure it is effective
   To address new threats, vulnerabilities, and options

5. Address third parties

Tunitas group

States React

- Legislation
  - Notice laws
  - Strict Liability laws
- State Unfair Trade Practice Laws
- Bully Pulpit
  - CT AG demands payment
  - No court case or statute

March 2008 Texas AG and CVS Settlement

Overhaul information security program

Implement new employee training program

Designate an employee to oversee compliance

Create anonymous reporting process for failure to comply w/order

Post signs in each store - proper records storage and disposal procedures

Conduct unannounced compliance checks at 3% of stores every six months

Pay a $315,000 fine

General Summary of Trends

The general duty to provide security for consumer information is being expanded and clarified

A legal standard for reasonable security is emerging from government enforcement activities and case law

Reasonable security is based on

- Governance
- Defined process

Failure to provide reasonable security creates legal liability

Tunitas group