

# The Realities of Your Legal Liabilities

---

June 2006

Melise R. Blakeslee  
McDermott Will & Emery  
202.756.8362  
mblakeslee@mwe.com

[www.mwe.com](http://www.mwe.com)

---

Boston Brussels Chicago Düsseldorf London Los Angeles Miami Munich New York Orange County Rome San Diego Silicon Valley Washington, D.C.

# What are the sources?

---

- Statutory
- Your own promises (shooting yourself in the foot)
- Negligence

# Statutes

---

- These are a patch-work of regulations
- Current statutes tend towards process, i.e. requirements to inform or to handle data a certain way -- not oriented towards technology
- Fines and other sanctions through the FTC, SEC, or states' attorney generals
- Gramm Leach Bliley, HIPAA, California laws -- over 50 different laws governing diverse elements of private data, e.g. shoppers club cards to driver's license information.

## More statutes

---

- Federal privacy law is still proposed – like the others it is likely to be process and notification oriented. Consider the EU's privacy requirements for global companies.
- Sarbanes Oxley (SOX) is heavily process oriented.
- SOX doesn't directly talk to IT or IT security, but, rather, requires executives to certify to adequate *internal controls* and procedures for financial accounting.
- Financial controls are driven by IT.

# Shooting yourself in the foot

---

- Promises to consumers or to your trading partners about privacy or the handling of data.
  - Choicepoint paid \$10 million in fines and \$5 million in restitution.
- Look at the promises you are making in contracts.
  - Mastercard and its outsourcing partner

# Negligence

---

- The basic measure of negligence is “reasonable under the circumstances”
- The recent problem at the Veteran’s Administration can be used as an example. Was it reasonable for the database to be fully downloadable? Were the precautions reasonable when the entire database was taken home every day for 3 years? Was it reasonable that the employee failed to mention the burglary for more than a week?

# What is negligence?

---

- Minimally adopting trade practices is not necessarily a defense.
- In the TJ Hooper case, 1932, it was not a defense that tug boats didn't usually have radios to call for help – the fact that radios were available and not deployed was the operative factor.

# What TJ Hooper means to you

---

- The tug boat operator was held to have been negligent even though few in the industry were using radios in 1932.
- The court said: “A whole calling may have unduly lagged in the adoption of new and available devices...”
- Substitute the word “solutions,” or “services” instead of “devices”
- Industry practices are not necessarily a defense -- they are likely only a threshold.

## Aggravating factors are:

---

- Another's reliance on your promises or expertise.
- Over use of superlatives when describing your service or solutions, such as: "Best," "Guaranteed," "Highest"
- Public disclosure of private facts that are not of legitimate concern to the public
- Intentional harm

# How does this apply to web services?

---

- Unfortunately, the “circumstances” of the web services industry are likely to lead to a heightened standard
- The dangers of an open protocol are well known
- There is increasing *reliance on your expertise*
- Meta data and XML identification of information is a known danger
- Hacking is a type of sport
- Well publicized problems become lessons that need to be heeded
- Audits pointing out the problems

# What should you be doing?

---

- Recognize that not enough time is being spent protecting data “at rest” as opposed to the amount of time spent on data “in flight”
- Recognize that security is a people problem & not a technology problem
- Start talking to legal. They do not know your issues but can help if educated
- Don’t shoot yourself in the foot: examine public & contractual promises, consider your use of the words “Best practices”

## Some more action items

---

- Create an umbrella security policy. A policy is an indicator of reasonable activity
- Put into place mechanisms and resources to enforce the security policy
- Educate your employees to be your eyes and ears
- Be aware that SOX is a *de facto* standard for everyone – public or not. Act accordingly
- Conduct regular external audits  
But first, set up the audit as within the attorney client privilege!!!
- Remember the Y2K model. Ask your business partners about what they are doing. Keep your chain intact
- Insurance – transfer risk to someone else.
- Prepare for failures