TOP TEN E-COMMERCE WEBSITE ISSUES[1]

I. Enforceability of Online Agreements (terms of use other agreements, UETA).

A. Online agreements are enforceable.

1. Click wrap/shrink wrap model.

B. Must be clear indication of assent to agreement.

C. Are terms enforceable if there is simply a link to the terms at the bottom of the page, but there is no indication of assent to those terms? *Specht v. Netscape Communications Corp.*, 2001 U.S. Dist. LEXIS 9073 (S.D.N.Y. Jul. 5, 2001)

1. Mechanics of demonstrating assent.

2. Record keeping.

3. Who could testify in litigation re: assent.

D. Terms must be conspicuous, clearly presented, easily available, not hidden.

E. Terms must not be unconscionable.

1. Arbitration clause.

2. Limitations on liability, warranties enforceable, etc.

F. Hypos

1. Litigation ensues over a transaction consummated via the company's e-commerce web site. How does the company prove that the customer agreed to the terms of the site?

II. Digital signatures.

A. Federal Electronic Signatures in Global and National Commerce Act (E-Sign)

---

[1] Michael Silverman and Sandra Jeskie are partners in the international law firm of Duane Morris, LLP and members of the Firm's Information Technologies and Telecommunications Practice Group, which Mr. Silverman chairs. Ms. Jeskie has 16 years of experience as a computer scientist and is resident in the Firm's Philadelphia office, 215-979-1000. Mr. Silverman is resident in the Chicago office, 312-499-4700. They can be reached at mjsilverman@duanemorris.com and jeskie@duanemorris.com.

B. Uniform Electronic Transactions Act (UETA)

1. adoption throughout U.S. except Georgia, Illinois, New York and Washington

2. legal enforceability of electronic signatures

3. authenticity of electronic signatures

a. Security procedures

b. Encryption

C. Hypos

1. If a signature is validated through the use of a PIN number without using a trusted third party, is the signature entitled to an evidentiary presumption of validity?

III. Terms of Use.

A. What constitutes acceptance of terms?

B. Registration for site use.

C. Privacy policy.

D. Authorized users, passwords, security procedures.

E. Appropriate use of website

1. Postings, upload functionality or other communications tools available on the site?

a. Offensive language

b. IP infringement

c. Illegal conduct (eg – trade associations may have anti competitive behavior concerns)

d. Spam, bulk communications, solicitations, etc.

e. Upload/post/send viruses, malicious code or other technology intended to harm system.

f. Collect/store personal data of others.

g. Right to pre-screen and remove content posted to site.

h. Compliance with foreign country's local rules re: use of system and content.

i. User grants worldwide, royalty-free, non-exclusive license to company re: any communications posted/transmitted over site.

2. Prohibit reproduction of any IP or data from site.

3. No resale or other commercial exploitation of content or services from site.

4. Prohibit linking to particular portions of site.

5. Users accept risk of their use of content from site.

6. Users agree to disclosure of information by company to comply with process, enforce Terms of Use, respond re: IP or other claims re: postings, protect the site/public.

7. Information transmitted to company via site (credit card numbers, etc.) are accurate and authorized.

8. Ability to form a contract using the site.

9. Prohibit violation of export control laws or use in countries where not authorized.

F. User indemnifies company (3rd party claims, IP infringement, breach of Terms of Use).

G. User acknowledges company's proprietary rights in site, data, software, etc. and protection of same under law.

1. Grant of limited license to user.

2. User agrees not to reverse engineer, create derivative works, modify, etc.

3. Trademark information.

H. Disclaimers/Limitations of warranties.

1. Links to other sites.

2. Site availability, functionality, accuracy, error free, etc.

3. Use at own risk.

4. Disclaim all the usual warranties

5. Product/service warranties for items purchased will be as set forth in invoice, warranty with product, etc.

I. Limitation of liability.

J. Copyright infringement notices and procedures (DMCA).

K. Company may revise terms of use and/or site at any time.

L. Termination of users' rights to use site.

M. Additional terms.

1. Choice of law, forum, arbitration.

2. Contractual limitations period.

3. Entire agreement, except for additional terms that may arise out of purchase of goods/services from site, affiliates, etc.

N. Hypos

1. Trade Association wants to have an online bulletin board/blog for members.

2. Company wants to allow its customers to post public comments on company products and to recommend other products.

3. Company wants to post its warranties on its web site and not include warranties with the products ordered from site.

IV. Privacy.

A. Identify data flows through the organization

1. employment data

2. medical data

3. consumer data

4. third party data

5. global data flows

B. Identify relevant limitations on data

1. federal laws

2. state laws

3. foreign laws

a. safe harbor

4. contractual limitations

C. design and implement privacy practices

D. privacy policy

E. privacy audits

F. privacy officer

V. Security.

A. Management of data obtained from transactions on company web site.

1. Ensure compliance with privacy policy no matter where the data goes within the company.

2. Consider privacy-related laws in implementing the security standards and protocols for web sites and in developing the terms of use.

B. What Needs to be Protected?

1. Types of information:

a. Trade secrets

b. Copyrighted information

c. Proprietary and/or confidential information

d. Customer data

e. Employee health care information

f. Pricing information

g. Computer code

2. Legal Issues

a. COPPA

b. GLB

c. HIPAA

d. Sarbanes Oxley

e. Critical Information Infrastructure

f. State Laws

C. What are the Data Management Risks?

1. Top Ten Risks (Gartner Study)

2. Respondents rate how critical each of the following security threats is to their organization ("1" means no concern at all; "10" means extremely concerned)

a.	Viruses and Worms	7.6
b.	Outside Hacking or Cracking	7.1
c.	Identity Theft and Phishing	7.0
d.	Spyware	6.8
e.	Denial of Service	6.6
f.	Spam	6.3
g.	Wireless and Mobile Device Viruses	6.2
h.	Insider Threats	6.2
i.	Zero Day Threats	5.9
j.	Social Engineering	5.9
k.	Cyber-Terrorism	5.6

l. Conducted in May 2005, the survey included responses from 133 North American organizations with global operations and revenues exceeding $750 million. Six of 10 surveys were completed by IT managers, with 91% overall answered by employees in IT departments.

D. What Needs to be Done to Protect the Data?

1. Privacy Policies

2. Security Policies

3. Document Retention Programs

E. What Happens When the Data Gets Out?

1. Reporting Requirements

a. SB 1386

b. SOX

c. Critical Information Infrastructure

d. Civil Liability

e. Criminal Liability

f. Incident Response/Mitigation Plans

2. European Union Requirements

F. Don't forget to specify security requirements in project documents used for developing the company's e-commerce site.

VI. Online Liability Exposure.

A. Infringement of intellectual property rights

1. copyright

2. trademark

3. passing off

4. linking

5. framing

B. Spyware

C. Unauthorized collection or misuse of data

D. Breach of a confidence or infringement of a right to privacy

E. Defamatory statements

F. Transmission of computer virus, worm, logic bomb, Trojan horse

G. Cookies

H. Phishing

I. Hypos

VII. Marketing

A. SPAM

1. Controlling The Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM Act")

a. false and misleading transfer of information prohibited

b. valid opt-out required

c. identified as an advertisement

2. State Spam Laws

a. federal preemption

b. false or deceptive commercial e-mail

3. Opt-in vs. Opt-out

4. Commercial e-mail vs. transactional or relationship messages

5. Commercial faxes

6. Hypos

a. As a multi-state marketing organization, how do should I deal with individual state spam laws

b. A consumer makes a one-time e-mail inquiry concerning one of your products, are future e-mails to the consumer considered relationship messages which are exempt from the spam laws?

B. Pop-Ups

C. Spyware

1. Federal and State law

2. Trespass to chattels

VIII. Key elements of website development agreement that relate to the e-commerce functionality of the site.

A. Project requirements

1. Establish requirements early and document them well.

2. Be careful when establishing the requirements is part of the development contract itself.

3. Consider alternative project management methodologies, such as agile methodologies like XP (extreme programming) in which requirements are developed in an iterative process.

    a. Contracting for such methodologies can be quite difficult.

4. Consider the risks of incorporating other technologies into the project.

5. Beware open source!

6. Specify project management/systems development methodologies to be used on the project.

B. Project management and schedules.

1. Milestones.

2. Commitment of resources by customer/vendor.

3. Proper staffing (quantity, quality, expertise, executive authority).

4. Coordination of multiple vendors/developers

    a. Who has responsibility?

    b. With whom was the other vendors' contract executed?

5. Consider the overall length of time it will take to complete the project in light of possible changes in technology, resource allocation, business environment, executive commitment, etc. (and consider vendor's and customer's perspectives on the above).

C. Change Control

1. Change control is probably the most serious risk to projects – "Scope Creep."

2. Client and vendor should restrain themselves from numerous changes.

3. Client/vendor should execute change orders, supported by realistic estimates of impact on time, cost, quality.

D. Deliverables and Acceptance Testing

1. Identify each deliverable

2. Identify objectives for each deliverable

3. Identify testing methodology for measuring success in meeting objectives, thereby requiring acceptance.

4. Contractual provision that submission of a deliverable for acceptance testing is a representation from vendor that deliverable meets objectives and was developed in accordance with methodology.

5. How do you turn the objectives/requirements into contractual commitments, and how do you cover them with warranties.

E. Performance criteria.

1. Establish appropriate criteria for performance, load handling.

2. Transaction volumes, number of users, number of active shopping carts, etc.

3. Allow for spikes during high traffic periods.

F. Ownership and Rights

1. Jointly developed technology.

2. Right to use outsourced service provider, maintenance company or host.

3. Ability to terminate vendor and bring in a replacement.

   a. Can be a very sticky negotiation point, particularly where vendor is also developing requirements.

   b. Vendors really do not want their competitors to have access to their technology, thought processes, tools, etc.

4. Appropriate licenses for developer's tools and software used on the project.

5. Specify who is responsible for procuring all licenses, IP rights.

G. Confidentiality

1. Clear specification of customer and vendor confidential information and trade secrets and of requirements for protection of those secrets.

2. For vendors, their software should be considered a trade secret and treated as such in the contract and the project.

H. Dispute resolution

1. Use of escalating dispute resolution process that requires alternative dispute resolution methodologies prior to litigation.

2. Specify in the contract the particular titles/positions of individuals who will have to participate in process.

a. It's helpful to have people who are not too deeply involved in the project and who have executive authority sufficient to resolve matters.

IX. Third party services.

A. Use of third party technologies/services to support functions of web site.

B. Examples

1. Credit card processing

2. Automated information gathering (i.e. use of business data (D&B, Equifax, etc.) to generate information for online applications for credit approvals).

C. Key considerations for relationship/contract.

1. Coordination of policies (privacy policies, terms of use, etc.) between company and 3rd party service provider.

2. Use of data obtained through the provision of 3rd party services.

a. Implicates coordination of privacy policies and application of laws related to data collected by the 3rd party service provider or the company.

b. Implicates trade secret, competition issues.

3. Use of marks, branding, technology, instructions, etc. of the 3rd party service provider (and vice verse).

a. Joint marketing, press releases.

b. Proper licenses and procedure for maintaining control over marks and other IP is essential.

4. Clear description of the scope of allowable use of the 3rd party services.

5. Linking to 3rd party service's site.

6. Indemnity

7. Termination and unwinding the relationship.

8. Warranties from 3rd party re: availability of service, response times, capacity, etc.

9. Trouble-shooting, help desk, problem-resolution systems from 3rd party service provider.

X. Upcoming Hot Topics

A. Website accessibility

1. Target ADA opinion