Hale and Dorr LLP

Counselors at Law

# International Internet and E-Commerce Issues: Surprising Results on Everyday Questions

Ken Slade

Hale and Dorr LLP

Boston Bar Association

Corporate Law Committee

November 13, 2002

# Overview

- Cross-border jurisdictional issues
- Enforceability of online agreements
- Privacy and data protection issues
- Spam
- Consumer protection
  - Not separate issue, so much as common theme affecting each of issues listed above
- Linking, framing and related issues
- Imposition of sales taxes on online transactions

# Cross-Border Jurisdictional Issues

# Cross-Border Jurisdictional Issues

- These issues are potentially more troublesome for e-commerce than for offline commerce
  - Likely to be a far greater number of interstate and international e-commerce transactions, now that Internet has created a single world market, at least for some products
    - Resolves many communications problems
    - Resolves time-zone differences
  - Likely to be a far greater number of interstate and international transactions involving consumers
  - Less likely to be negotiated contracts
    - Parties reacting only remotely
    - Emphasis on automated, mass market solutions on the Internet

# Manifestations of Cross-Border Jurisdictional Issues

- CRIMINAL: If your website is accessible from a particular country, you may be subject to the criminal laws of that country
  - American neo-Nazi sitting in jail in Germany
  - Pakistani arrest warrant for Michael Jackson
- CONSUMER PROTECTION: If problems arise from your goods and services sold through your website, you probably can be sued in the home country of your customer
- TAX: If you are doing enough business with a particular country, you might be subject to income taxes in that country
- These are new issues, not yet squarely addressed by international treaties or conventions

# Status of U.S. Law on Internet Jurisdictional

- Each U.S. state and federal district may have different rules
- Some initial decisions have found that a website alone justifies jurisdiction, although most decisions have required more
  - TESTS: Website plus interactive component? Clear effort to do business in jurisdiction? Physical presence?
  - Problem: Tension between commercial objectives and limiting jurisdictional exposure
- American Bar Association is trying to propose standardized guidelines

# Toys R Us v. Step Two, SA

- US company sought to sue Spanish company in US court because website infringed on US trademark
- Spanish company had been careful in limiting use of website to Spain
  - Only took orders for shipment to Spanish addresses
  - Prices in pesetas and Euros only
  - Spanish language site
  - Contact information only by phone, without international access code
- U.S. federal district court in New Jersey found no jurisdiction
  - Interactive site alone not enough
  - No proof that Step Two was reaching out to New Jersey

# Non-Contractual Claims: Effort to do business, or intent to cause harm?

- *Pavlovich*: out-of-state website operator marketed programs designed to defeat copy protection system used to protect DVDs
  - California court exercised jurisdiction because defendant used site to intentionally injure California businesses
  - Did not need to show that defendant tried to do business in California

# Status of EU Law on Internet Jurisdiction

- Choice of jurisdiction generally governed by contract subject to certain overriding national laws of Member States (one of which is consumer protection law)
- Draft EU regulation conforming Member States approach on choice of jurisdiction in contractual matters (UK opt out)
- GOAL – CONSUMER PROTECTION
  - Adoption of US “targeting” approach

# Status of EU Law on Internet Jurisdiction

- Article 15 - a company which "directs its activities" to consumers in another EU country can be sued in that country
- Commission rejects attempts to clarify what amounts to "directs activities" – very existence of a consumer contract suggest directed activities
- Non-contractual matters e.g. defamation / personal injury – *Godfrey v Demon* – can sue in jurisdictions where damage incurred

# Cross-Border Jurisdiction: Latin American Perspective

- Rules are different in each country
- A company directing its activities to or in a Latin American country could be sued before its courts

# Enforceability of Online Agreements

# Types of Online Agreements: Terminology

- Shrink-wrap agreement: originally, formed by user opening up the plastic "shrink-wrap" surrounding computer software
  - Subsequently, applied to an agreement formed by a user's opening and use of a product
- Click-wrap agreement: formed by user clicking on and accepting terms, either on a website or as a screen in the installation procedure for the product
- Browse-wrap agreement: formed by user visiting and/or using a website

# Why use online agreements?

- Given the volume of transactions online, it is impractical to have separately negotiated agreements
- Given the nature of the Internet, both buyers and sellers want the convenience of "agreeing to terms" online
  - Can apply to any goods and services ordered online, even if delivered through conventional means
- Using online agreements discourages even large buyers from insisting on separately negotiated terms
  - Inability of consumers to negotiate terms may lead to enforceability problems (see *PayPal* case)

# *ProCD Incorporated v. Zeidenberg*

- Shrink-wrap agreements are enforceable, provided that:
  - Their terms are "commercially reasonable" and not otherwise unconscionable or subject to any other defense available under contract law
    - on unconscionability, see *PayPal* case
  - User has right to reject terms upon opening package and to receive a full refund
- Rejected argument that all of the terms and conditions of a shrink-wrap agreement must be printed on the outside of the product packaging.

# Extension of *ProCD* to Enforceability of Click- and Browse-Wrap Agreements

- *Groff v. America Online, Inc.* (R.I. Superior Ct. 1998)
- *Ticketmaster Corp. v. Tickets.com* (C.D. Cal. 2000)
- *Williams v. America Online, Inc.* (Mass. Superior Ct. 2001)
- *Specht v. Netscape Communications, Inc.* (S.D.N.Y. 2001)
- *Comb v. PayPal, Inc*. (N.D.Cal. Aug. 30, 2002)

# So when are online agreements enforceable in the US?

- In order to bind a buyer to an online agreement, seller must meet a two-part test
  - Buyer must be aware of the requirement that a contract be entered into
    - *Pollstar v. Gigmania Ltd.* (E.D.Cal. 2000): in dicta, court notes that a hyperlink to a browse-wrap agreement, presented in small gray text on gray background and not underlined, might not be enough to make buyer aware
  - Buyer must affirmatively manifest his or her assent, by taking a demonstrable step
- Even if the buyer is bound, whether specific provisions are enforceable will depend on the availability of normal contractual defenses, such as unconscionability

# Current Status of Shrink-Wrap Agreements, based on current statutes and advice of foreign counsel

- Likely to Be Enforced: U.S., Canada, France, Italy, Spain, Netherlands, Scandinavia, Brazil, Saudi Arabia, Hong Kong
- Likely to Be Enforced, Subject to Consumer Protection Laws: Mexico, Argentina, Chile
- Less Certain: Japan and Korea
- Unlikely to Be Enforced: Germany, United Kingdom, Australia (?), China -- yet still worth trying
- Click-wrap easier to enforce (buyer sees terms before accepts) -- but still not likely to be enforced in China
- Browse-wrap is suspect everywhere

# Enforceability of Online Agreements in Germany

- Shrink-wrap
  - Although common in some areas (e.g. software), still considered ineffective under German law
  - Option in the B2B area: Choose another law where shrink-wraps are accepted, if one party has legal residence there (see above)
- Browse-wrap
  - Considered ineffective under German law

# Enforceability of Online Agreements in Germany

- When concluding a click-wrap agreement with consumers:
  - Make an express reference to the terms
  - Utilize clear and transparent terms
  - Enable the customer to receive notice in a reasonable way
  - Consent of the customer
  - Inclusion in an order confirmation or invoice will not be effective
- B2C rules generally not applicable in B2B, but in order for the transaction to be legal
  - Clear reference to the terms necessary
  - Chance for other party to receive notice
  - Inclusion by reference in order confirmation is sufficient
  - No objection from other party

# Click-Wrap Agreements: Latin American Perspective

- Traditional transactional formalities and law are still influenced by XIX Century civil code principles
- Uncertainty as regards validity and enforceability: a challenge for e-comm
- However, many Latin American countries have recently enacted legislation regarding electronic documents, electronic transactions and digital signatures

# Recent and Pending Legislation in Latin America

- Argentina: Presidential Decree 427 (1998), digital signatures for the public sector; Digital Signature Law (2001), digital signatures for the private sector
- Brazil: In 2001, the Brazilian Government officially launched the Brazilian Public Key Infrastructure in order to guarantee the legal validity and integrity of e-documents through digital certification. Proposed E-commerce Bill (2001) includes provisions on electronic signature and digital certification

# Recent and Pending Legislation in Latin America

- Mexico: E-Commerce Act (2001) amends the Civil Code, Commercial Code, Consumer Code and Rules of Civil Procedure, and regulates privacy, digital signature, electronic documents and electronic transactions
- Peru: Electronic Signature Bill (1999)
- Venezuela: Law on Data Messages and Electronic Signatures (2001), assigns electronic messages and signatures the same validity and legal treatment as handwritten signatures and paper documents

# General Issues Affecting International Enforceability

- Translate terms into local language
- Comply with localization requirements
  - Spain:  all packaging in Spanish
  - France: documentation and online help in French
- European Union Software Directive
  - Cannot block assignments of software licensed for lump-sum amounts
  - Cannot prohibit reverse engineering required to ensure interoperability

# Special Consumer Protection Issues Affecting International Enforceability

- Variations in consumer warranty requirements
  - EU legislation has provided for certain minimum term warranties that affect consumers and businesses. These are not yet in force in UK, which is still going through a "consultative process on implementation"
- European Union Distant Selling Directive (Articles 5 and 6): buyer must receive written confirmation or confirmation "in another durable medium"; 7-day right of return runs from receipt of confirmation
- Most consumer protection laws will ignore consumer's acceptance of choice of law and dispute resolution provisions which choose a foreign law or forum
  - Japan (?), the Netherlands, Norway and the United Kingdom (?) are the exceptions

# Strategy for Using Click-Wrap Agreements Internationally - #1

- As much as we might like to think to the contrary, concede that it is, under current law, impossible to apply a single click-wrap agreement worldwide
- Develop a U.S./Canadian contract that serves as an "international default" agreement
- Have foreign counsel review that agreement for key markets and then, once you approve changes, translate agreement into their language
  - For most U.S. companies, those are typically UK, Germany, France, Italy, Japan and maybe Spain and Brazil
  - Shortcut for cost-sensitive clients: ask foreign counsel to translate only, but in the course of translation, alert you if they see any "big issues"

# Strategy for Using Click-Wrap Agreements Internationally - #2

- Many foreign counsel advise that choice of law, dispute resolution and other provisions might not be enforceable
  - Don't concede issue -- leave choice of law and dispute resolution provisions as is
    - No harm in trying to impose those provisions
    - Those provisions still might be enforceable vs. pirates and with respect to IP issues
  - As a precaution, make changes in substantive provisions, so that agreement will still be enforced, even if local law is applied before local courts

# Strategy for Using Click-Wrap Agreements Internationally - #3

- A smaller group of foreign counsel advise that choice of law and dispute resolution provisions will not be enforceable, and must be changed
  - For limitations on liability to apply, must submit to local law (France)
  - Attempt to choose U.S. law and U.S. dispute resolution may invalidate entire agreement, including substantive provisions (e.g., Sweden and Denmark)
  - Stipulating a prohibited governing jurisdiction and forum for arbitration is a false or misleading representation (Quebec)
  - Special case -- Germany: choice of U.S. law and forum will not invalidate agreement, but may lead to order that company cease using these provisions
- In those countries (with exception of Germany), choose local law, local courts and make substantive changes recommended by foreign counsel

# Privacy and Data Protection Issues

# Privacy: U.S. Perspective

- There is no general privacy legislation in the U.S.
- If you have a privacy policy, the Federal Trade Commission is looking at how that policy addresses the widely-recognized privacy principles of:
    - NOTICE about online information collection
    - CHOICE regarding uses of that information
    - ACCESS to ensure that information is accurate, complete, and up-to-date
    - SECURITY and integrity of information collected online; and
    - ENFORCEMENT to provide effective recourse for improper breaches of personal privacy
- Federal Trade Commission or state consumer protection agencies may go after a website operator:
    - If it does not follow the privacy policy which it has adopted; OR
    - If it violates the privacy policy of another website from which it has "data mined"

# U.S. Sectoral Privacy Mandates

- Internet privacy mandates supplement these principles on a “sectoral” basis
- Children’s privacy -- Children’s Online Privacy Protection Act (COPPA)
- Health data privacy -- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Financial data privacy -- Gramm-Leach-Bliley Act
- Location data privacy -- Wireless Communications and Public Safety Act of 1999

# EU Data Protection Directive

- Establishes legal principles for the processing of personal data within the EU
  - Where a company carries out a "regular practice" of processing personal data in the EU, then any processing of EU personal data carried out by the company will be caught by the Act. It is not necessary that the company be incorporated in the EU.
- “Personal data” is data from which a living individual can be identified (alone or combined with other data)
- “Data Controller” is the entity that dictates the manner and purpose for which personal data is processed
- Processing is widely defined and covers even the mere obtaining of data

# Rights of the Data Subject

- Must give “specific” and “informed” consent to processing
- Must be informed of the purposes of the processing at time of collection
- Data must be accurate and up to date and not kept longer than necessary to fulfill the stipulated purposes
- Must be appropriate security measures in place to guard against unauthorized use or accidental loss
- Data must NOT be transferred outside EU unless adequate level of protection is available in the country to which export is made
  - Levels of protection in US are NOT adequate
- Upon request, to obtain a copy of the data

# Privacy and Data Protection, As Applied in Germany

- Obligation to inform the customer about collection and use of personal related data at the beginning of the process
- Active and conscious “informed“ consent of the user
- Provide clear information about data protection law before any data regarding the data subject can be entered
- Instruction has to be separate from general terms or distance purchase law instructions

# US-EU Safe Harbor Guidelines: Seven Privacy Principles

- NOTICE: State why the information is collected
- CHOICE: Individuals must be allowed to opt-out of purposes other than purpose for which data was originally collected
- ONWARD TRANSFER: Personal information may be transferred to third party only if such transfer is necessary for the original purpose and the third party agrees to comply with the safe harbor principles
- SECURITY: Take reasonable precautions to protect vs. loss, misuse and unauthorized access, disclosure, alteration and destruction

# US-EU Safe Harbor Guidelines: Seven Privacy Principles

- DATA INTEGRITY: Take reasonable steps to ensure that data is reliable for intended use, accurate, complete and current
- ACCESS: Individuals must have access to their data to ensure accuracy
- ENFORCEMENT: Opportunity to pursue complaints and disputes
- Companies must provide enforcement mechanisms by:
  - Complying with private-sector self-regulatory programs;
  - Complying with applicable privacy law or regulation for enforcement; OR
  - Committing to cooperate with EU data privacy protection authorities

# Possible Reasons for Slow Response to US-EU Safe Harbor

- Rely instead on exceptions to EU Directive
  - EU persons may “consent unambiguously” to international data transfers
  - Data transfers required to perform a contract
- Perceived lack of immediacy
  - Enforcement of Directive was delayed until June 2001
  - Germany and some other EU countries were late in enacting legislation

# Possible Reasons for Slow Response to US-EU Safe Harbor

- Benefits are not guaranteed
  - Some EU data sources may insist upon additional safeguards, such an explicit consent, in order to avoid liability under local data privacy laws
- Contractual alternatives
  - EU currently developing model contractual provisions
  - By following these models, US companies may avoid subjecting themselves to FTC oversight under the safe harbor program

# Canada's Personal Information Protection and Electronic Documents Act

- Some privacy provisions came into effect on January 1, 2001 for federally regulated industries (e.g., airlines, banking, telecommunications, broadcasting)
  - Health information: January 1, 2002
  - All other private sector entities that collect, use or disclose personal information: January 1, 2004
    - Unless applicable provincial legislation is enacted by that date

# Canada's Personal Information Protection and Electronic Documents Act

- Federal legislation, but expected to be followed by provincial legislation (already enacted in Quebec; Ontario revised draft legislation ready for presentation to House most likely after upcoming provincial elections (and larger than federal act); other provinces likely to follow)
  - Effort to make Canadian standards consistent with international data protection standards
  - Desire to avoid EU countries from blocking data transfers to Canada

# Canada's Personal Information Protection and Electronic Documents Act

- Legislation creates a consent-based system which permits individuals to withhold consent in connection with the collection, use or disclosure of their personal information
- Incorporates 10 privacy principles which are based on Canadian Standards Association's Model Code for Protection of Personal Information
  - Very similar to US-EU safe harbor principles

# Canada's Personal Information Protection and Electronic Documents Act

- Federal statute applies to organizations in respect of "***personal information***" that they collect, use or disclose in the course of "***commercial activity***" across provincial or international boundaries
- Other provisions apply to employers in federally regulated industries (e.g., telecomm, broadcasting, banking and airlines) which collect personal information on employees

# Scope of Canadian Privacy Legislation

- Covers “personal information” about an identifiable individual
  - But excludes the name, title or business address or telephone number of an employee of an organization
- Personal information provided by Canadian users and collected by a U.S. company through its website is probably covered
- BUT enforcement and jurisdiction are separate issues

# Two-Step Analysis of Applicability of Canadian Privacy Law to U.S. Data Collectors

- What is the situs of the personal information collection activity?
  - Determination to be made by Canadian Privacy Commissioner
- Is collection in the course of commercial activity?
  - Will depend on the purpose of website (i.e., advertising? selling goods? purely informational?)

# Latin American Privacy Overview

- Latin American countries are enacting privacy legislation for three main reasons:
  - To remedy past privacy violations
  - To promote e-commerce
  - To ensure EU data exchange
- Most Latin American countries are enacting comprehensive privacy laws for both the public and private sector, in some cases complemented with particular laws for specific types of information
- Right to privacy recognized in most Latin American constitutions (e.g., Argentina, Brazil, Chile, Mexico, Peru)

# Recent and Pending Legislation

- Argentina Constitution (1994). Privacy Data Protection Act (2000), follows EU Data Protection Directive
- Brazil Constitution (1988). Code of Consumer Protection and Defense (1990), grants consumers the right to access and correct their personal information. Various pending bills: Data Privacy Bill following OECD guidelines (1996); bill requiring ISPs to keep personally identifiable data of its users (2001); and bill regulating collection and dissemination of users personal data through the Internet (2001)
- Chile Constitution (1980). Law for the Protection of Private Life (1999), also addresses use of financial, commercial and banking data and use of personal data by governmental entities

# Recent and Pending Legislation

- Mexico Constitution (1917). E-Commerce Act (2001) includes privacy provisions concerning the private sector. Federal Transparency and Access to Public Government Information Law (effective May 2003) allows access to information held by government agencies
- Peru Constitution (1993). Data Protection Law (2001) covering private credit reporting agencies. Transparency and Access to Information of the Public Administration Law (2002) allows access to information held by the public administration
- Paraguay Data Protection Act (2000)

# Latin America Follows the EU Standard

- Most Latin American privacy laws and bills follow EU Directives very closely
  - rights of data subjects (Argentina, Chile, Peru and 1996 proposed law in Brazil)
    - **Argentina:** The Personal Data Act sets forth that any communication for advertisement purposes by mail, phone, e-mail, Internet or any other remote means, shall expressly mention the possibility to request the total or partial elimination or blocking of the data subject´s name from the data base.
  - Data processing rules
  - Liability and enforcement
  - Blocks transfer to other countries without adequate laws (Argentina and proposed 1996 proposed bill in Brazil)
    - Safe harbor rules with the United States may need to be negotiated
- By following the EU standard, there is an expectation that privacy laws will be harmonized between Latin American countries

# Japanese Internet Privacy

- Currently, there is no uniform Japanese law on privacy
- Recognized as a constitutional right under case law
- Public sector:
  - "Act for Protection of Computer Processed Personal Data Held by Administrative Organs" (1988), applied to the administrative organs of the central government
  - "Personal Data Protection Ordinances", promulgated by many local governments
- Private sector:
  - No comprehensive legislation
  - Self-regulation policy

# Japanese Internet Privacy

- "Guidelines for Protection of Personal Data in Telecommunications Business" (1991), "Guidelines for Protection of Subscribers' Personal Data Regarding Broadcast Viewers" (1996) and "Guidelines for Protection of Communicators' Personal Data in Utilization of Services of Notifying Communicators' Data" (1996), issued by the Ministry of Posts and Telecommunications
- "Guidelines for Protection of Computer Processed Personal Data in Private Sector" (1997), issued by the Ministry of International Trade and Industry

- First systematic survey of consumer privacy was not organized until 1999
- General view that national legislation is needed
  - For uniformity
  - To cover private collection of data
  - For sake of complying with international standards (i.e., EU Data Protection Directive)

# Proposed Japanese Act for Protection of Personal Data

- Approved by Japanese Cabinet March 27, 2001
- Originally expected to be in force from April 2003
  - Opposition from the press and opposition parties have pushed back effective date
- Clarifies basic principles for both private and public sectors
- Provides for various responsibilities generally applicable to all “personal data handling entrepreneurs”

# Japanese Legislation: Basic Principles for Handing Personal Data

- Information should be used for specific purposes, and only to the extent necessary (consent)
- Information should be obtained by proper methods (notice)
- Information's accuracy should be maintained (data integrity)
- Information should be used only after appropriate safeguards are in place (data security)
- Individuals whose information is collected should be able to demand correction or deletion of personal details (access)

# Proposed Japanese Legislation

- Includes criminal penalties
- Exemptions proposed for news media, academic research, and religious and political activities
- Not yet clear whether or not the Japanese legislation would be deemed adequate under the EU Data Protection Directive

# Conclusions on International Trends in Internet Privacy

- The number of jurisdictions with formal privacy laws is expanding rapidly.
- There is no single privacy standard being adopted in those jurisdictions.
- Compliance with the toughest standard (i.e., European Union) does seem to satisfy substantive requirements of the less demanding jurisdictions.
- Even if EU standard is followed, there may still be registration and record-keeping requirements in other jurisdictions

# Spam

# Regulation of Spam in the U.S.

- No federal legislation
- State legislation tends to prohibit fraud or use of bogus sender addresses, require an opt-out and/or require labeling as an advertisement
  - Washington and California statutes were challenged on Dormant Commerce Clause arguments, with mixed results
- Through the tort of cybertrespass
  - *Intel Corp. v. Hamidi:* California Superior Court ruled that spam sent to Intel Corporation's employees constituted an illegal trespass of Intel's proprietary computer system
  - Recognized by California and now New York courts
  - Key: What harm need to be shown to constitute this new form of trespass?

# Spam: German / EU Perspective Until May 2002

- EU E-Commerce Directive requires
  - Unsolicited commercial e-mail (i.e., spam) to be clearly identified as such
  - Providers must regularly consult opt-out registers
- Sending unsolicited commercial e-mail violates German competition law (unfair trade practice, Sec. 1 UWG)
- After “opt in” of the user, commercial e-mails are considered lawful
- Each commercial e-mail and the sender has to be recognizable for the recipient (Sec. 7 TDG)

# Regulation of Spam in EU After May 2002

- Directive on the Processing of Personal Data in the Electronic Communications Sector: prohibits EU companies from sending spam for the purposes of marketing to individuals unless
  - With prior consent; or
  - To existing customers who are given an opportunity to "opt-out" at the time their information is initially collected, and at the time of each subsequent message
- Curiously, this Directive does not apply to spammers based outside the EU who do not have operations subject to the jurisdiction of any EU Member States
  - However, sending a U.S. spammer an EU company's distribution list is probably a problem under the EU Data Protection Directive

# Spam: Latin American Perspective

- Most Latin American countries have no specific legislation as regards spamming
  - Proposed rules in Argentina
    - Draft Electronic Mail Protection Law: regulates spam through labeling, no false sender addresses, opt-out and registry to block spam messages
    - Draft Regulations of Electronic Mail Commercial Communications for Advertisement Purposes: allows recipients and ISPs to sue spammers for damages if messages are sent to recipients on registry

# Spam: Latin American Perspective

- In most Latin American countries, spammers could be sued if damage is proven under traditional Civil Code provisions
- Brazil -- application of Consumer Code provisions, E-Commerce Bill (specific provision). First decision against spamming involved a journalist who had sent 11.000 e-mails (July 2002)

# Linking, Framing and Related Issues

# Clearly Prohibited Linking Practices

- Linking to material which you know to be infringing on the copyrights of a third party can subject the linker to liability for copyright infringement (*Utah Lighthouse Ministry* case)
- Linking to a website engaging in criminal activities can subject the linking party to criminal liability for aiding and abetting those activities (Japanese pornography case)
- Framing another site's content within your own site "detracts from persona of the linked site" and constitutes an unfair trade practice
  - US*: Total News;* UK: *Shetland Times*

# Deep Linking

- Linking to pages “deep” within the linked site, bypassing home page and advertising
- Deep linking was upheld in *Ticketmaster Corp. v. Tickets.com, Inc.* case
  - Not copyright infringement (not copying, just transferring)
  - Not violation of terms of use, unless linked site can show that linking party accepted those terms
  - Not unfair competition, as long as there is no attempt to mislead users about source of linked information/goods/services
- Similar result in Dutch case (*PCM v. Kranten.com),* but some recent Danish and German cases, relying on EU database rights, have prohibited deep linking

# Metatags

- Html code often used to describe the subject matter of a website
  - Invisible to visitor of website
  - Detected by search engine
- *Eli Lilly & Co. v. Natural Answers*: use of another party's trademark is probative of wrongful intent to confuse consumers and is significant evidence of intent to confuse and mislead, a required element of any trademark infringement claim
- Although some cases go the other way, use of trademark as a metatag (without using the trademark in the visible text of a website) does not necessarily avoid trademark infringement liability
- UK case – *Reed Executive v. Reed Business Information*

# Metatags: German Perspective

- Metatags can create trademark violation (OLG München CR 2000, 461)
- Massive use of metatags can be unfair trade practice (Sec. 1 UWG)
- Metatags can violate the name rights, if no relation to the site (LG Hamburg CR 2002, 374 – Steinhoefel)

# Imposition of Sales Taxes on Online Transactions

# U.S. -- Sales Tax Issues Looming

- 1998: Internet Tax Freedom Act established a three-year moratorium on new or discriminatory state and local taxes applied to e-commerce
- 2001: moratorium extended through November 1, 2003
- As yet, no consensus has emerged
  - Dot.coms want to make the moratorium permanent
  - State governments see sales tax receipts dropping
  - Brick-and-mortar stores feel that they are being put at an unfair disadvantage

# Moratorium Extended, but . . .

- Arkansas has passed a law requiring out-of-state e-retailers to collect sales tax if the e-retailer has a substantial interest in a business with an in-state physical presence
- California is increasingly aggressive in imposing sales and use taxes on online booksellers which are utilizing in-state agents and representatives (e.g., their brick-and-mortar affiliates)

# EU VAT Tax on Online Transactions

- EU's Council of Economic and Finance Ministers have proposed that, starting in mid-2003, non-EU companies be required to collect taxes on digital deliveries to EU consumers
  - Generally ranges 15-20%
  - US supplier would register for VAT in the EU country of its choice, but would then have to account for VAT at the various national rates (e.g., 19.6% on sales to French customers, 17.5% on sales to UK customers, etc.)
  - de minimis registration level will be adopted,
    - Non-EU suppliers will not need to register for VAT in any EU Member State where their annual sales to EU customers are less than $87,400 (based on value of Euro as of March 2002)
  - Not imposed on sales to EU business customers

# For Further Information:

Ken Slade

Hale and Dorr LLP

617-526-6184

Kenneth.slade@haledorr.com

Sign up for Hale and Dorr Internet Alerts at

www.InternetAlerts.net