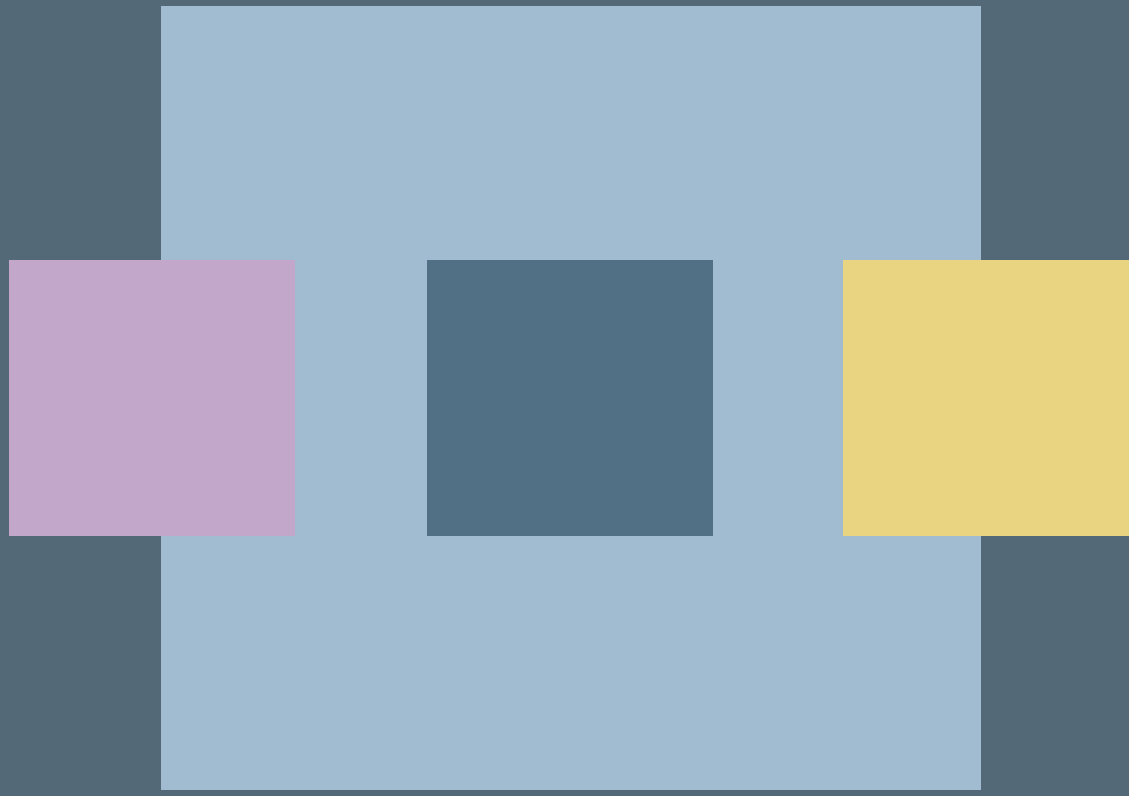
Brobeck Hale and Dorr

E-Commerce:
Current Issues in
the UK,EU and US



Ken Slade

Sarah Harrop

1 July 2002

The Technology Law Firm

Overview

- Cross-border jurisdictional issues
- Enforceability of on-line agreements
- Privacy and data protection issues
- Service provider liability
- Linking, framing and related issues
- Cyber-trespass

Brobeck Hale and Dorr

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 web site 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 web site, 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: Web site 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

Brobeck Hale and Dorr

Toys R Us v. Step Two, SA

- US company sought to sue Spanish company in US court because web site infringed on US trademark
- Spanish company had been careful in limiting use of web site 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

Effort to do business, or intent to cause harm?

- *Pavlovich*: out-of-state web site 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 law)
- Draft EU regulation conforming Member States approach on choice of jurisdiction in contractual matters (UK opt out)
- Adoption of US “targetting” approach
- 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

Enforceability of On-Line Agreements

Why use on-line agreements?

- Given the volume of transactions on-line, 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" on-line
  - can apply to any goods and services ordered on-line, even if delivered through conventional means
- Using on-line agreements discourages even large buyers from insisting on separately negotiated terms

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
  - 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.
- Later extended to on-line agreements (called "click-through" or "click-and-accept agreements") and terms of use of web sites (called "browse-wrap agreements")

Specht v. Netscape Communications

- Court found that users were not bound by Netscape's arbitration clause in its browse-wrap agreement, for those users never assented to terms
- Free download
  - Terms only visible by scrolling down screen, below download button, to message, and then clicking on link from message
  - Message "Please review and agree to the terms of Netscape . . . License before downloading and using the software"

Specht v. Netscape Communications

- Court concluded that mere downloading did not equal assent
- Court also rejected the idea that user could be bound to a contract without even seeing the message referring to that contract
- In addition to the way the message was shown, court found that language used was merely an invitation to agree, rather than a requirement for use of the software

Enforceability of On-Line Agreements Under English Law

- Significant legal difficulties surround enforceability of shrink wrap licences:
  - Contract with retailer – offer / acceptance / consideration
  - Contract with manufacturer – offer / acceptance / consideration
  - Scottish law experience – Adobe Case
- Click wrap agreements avoid the problems of Shrinkwrap as direct contractual relationship, provided properly concluded:
  - E-commerce Directive
  - Distance Selling Directive
  - Authority to bind
  - Terms included prior to formation
  - Outsourcing: active agents
- Non-clickable terms and conditions still useful to give users notice of certain facts:
  - Ownership of copyrights and trademarks
  - Data privacy

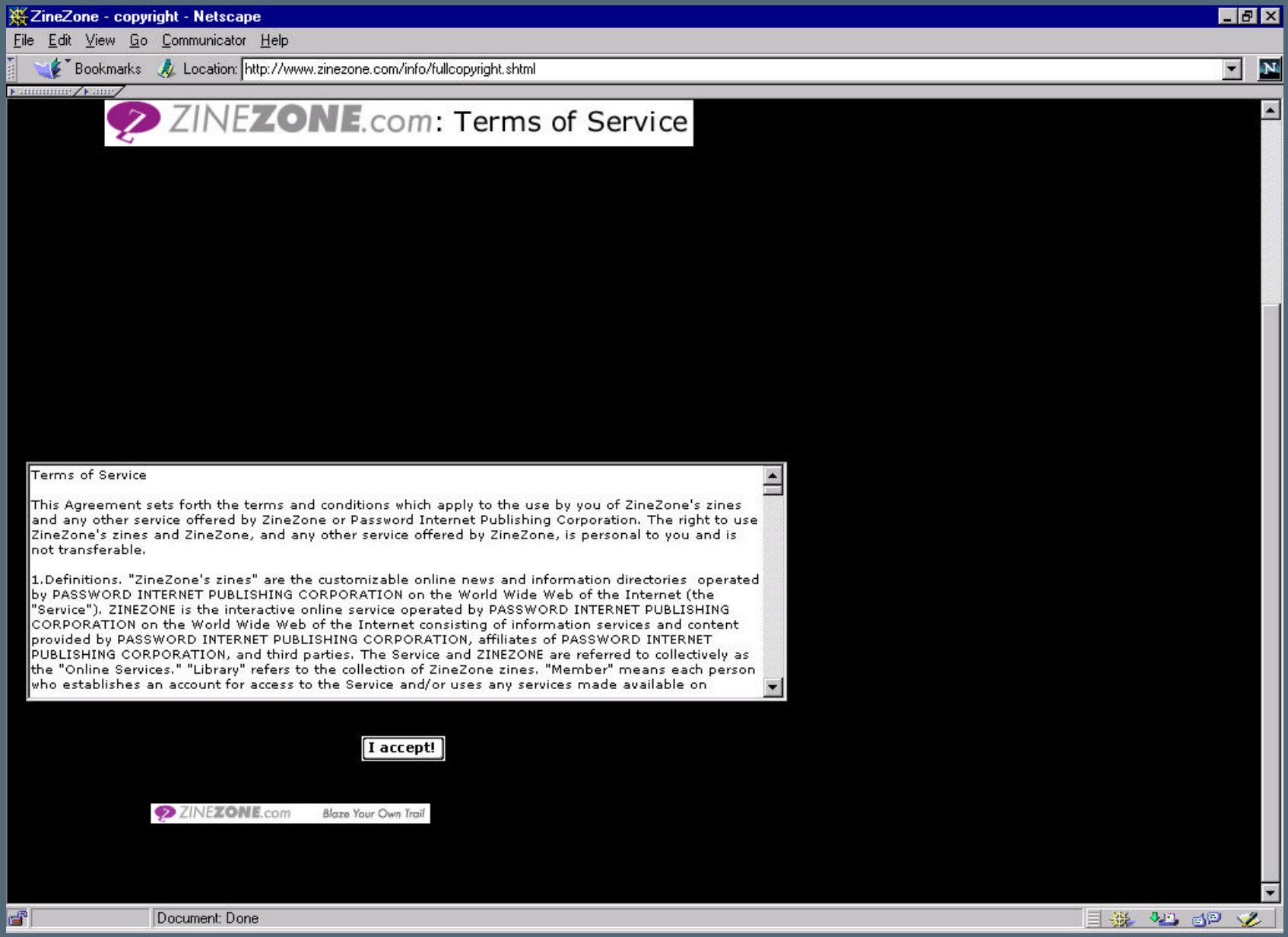
Strategy for Enforceability: Step #1 - Before Submitting Order

- Immediately above key where customers submit orders, cause customer to accept terms and conditions
- Two alternative methods
- Method #1: Use of this product is subject to your acceptance of Licensor's terms and conditions of sale.

Strategy for Enforceability: Step #1 - Before Submitting Order

- Method #2: Terms and Conditions visible through scroll field.
- Below scroll field:
  - By submitting this order, I accept the terms and conditions set forth above.
  - “Submit Order” or “I accept” button

Brobeck Hale and Dorr



The Technology Law Firm

Strategy for Enforceability: Step #2 - Accessibility of Terms

- Make terms easily accessible, both before and after acceptance
- Available on web site or by fax
- Set out in full within delivered product
  - Behind “About Product” box, under “Help” menu
  - Printed version in brochure within package or in user manual (if there is one)

Strategy for Enforceability: Step #3 - Installation

- As part of the installation program for any downloaded product, show those terms and conditions again (after all, installer may not be downloader).
  - The user must be able to scroll down through the agreement if he so chooses. The user must hit an "Accept Terms" key TWICE before he can complete installation and then use the product.
  - If he hits the "Reject Terms" key, the installation program aborts and the user will not be able to use the product.

Strategy for Enforceability: Step #4 - Splash Screen and Help Menu

- Once installed, the user would not be asked again to accept the terms.
- However, every time the user enters the product, the splash screen for the product will display, in addition to the typical copyright and trademark notices, the statement (after all, user may not be installer or downloader):
  - Use of this product is subject to the terms and conditions found under this product's Help Menu.

Strategy for Enforceability: Step #5 - Battle of Forms

- If seller receives a purchase order from a prospective buyer, then it must either:
  - (a) send that prospective buyer a copy of the terms and state very clearly that: (i) Seller's acceptance of the purchase order is expressly conditioned upon those terms; and (ii) Seller shall not ship the product until the prospective buyer communicates its acceptance of those terms; or

Strategy for Enforceability: Step #5 (continued)

  - (b) (although a bit riskier) ship the product with a packing slip that clearly and prominently states that: (i) shipment of the product is pursuant to the buyer's purchase order and is subject to Seller's terms; and (ii) if the buyer does not accept those terms, it should return the product and Seller will refund any amounts that the buyer may have already paid for that product.

- The product then shipped to that buyer will also have to follow Steps #2, #3 and #4 described above.

Brobeck Hale and Dorr

International Enforceability, based on current statutes and advice of foreign counsel

- Shrink-wraps: 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-through easier to enforce (buyer sees terms before accepts) -- but still not likely to be enforced in China

Privacy and Data Protection Issues

Privacy: U.S. Perspective

- There is no general privacy legislation in the U.S.
- At a philosophical level, balancing the protection of an individual's privacy against the commercial value of information about that individual
- At a practical level, companies need to develop an adequate privacy policy and then stick to it
- Manifestations:
  - No longer enough just to have a policy; Federal Trade Commission is looking at how that policy addresses the widely-recognized privacy principles of:
    - NOTICE about online information collection

Privacy: U.S. Perspective

- 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 web site operator:
  - If it does not follow the privacy policy which it has adopted; OR
  - If it violates the privacy policy of another web site 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

Enforcement

"Self-regulated" DOES NOT MEAN "unregulated"...
…FTC can act without new Internet privacy laws:

GeoCities (1998): Registration data released to third parties contrary to stated restrictions. First Internet privacy settlement based on FTC charges of "unfair" and "deceptive" use of online data.

ReverseAuction (2000): Collected addresses of eBay users and sent spam misrepresenting that eBay IDs were about to expire, in violation of eBay's terms of use. "[B]eyond self-regulation, those who violate consumers' privacy should be promptly called to task." FTC action "is an effort to buttress, not supplant or detract from, initiatives of private parties. . . who develop and implement their own privacy arrangements."

ToysMart (2000): Proposed bankruptcy sale of customer data would violate stated privacy policy forbidding release to third parties.
FTC Settlement authorized sale only to "qualified purchaser."
Bankruptcy court rejects settlement

Online Profiling

- Online profiling is seen as particularly invasive, even if the profile is not “personally identifiable”
  - Tracks Internet usage of user and develops profile
  - Sells “targeted advertising” which matches user’s profile with specific products and services
- Network Advertising Initiative (NAI), a coalition of several leading online profiling companies, formulated a set of self-regulatory privacy guidelines
- Those guidelines have been endorsed by the FTC

EU Data Protection Directive

- Establishes legal principles for the processing of personal data within 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
- 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 unauthorised 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
- Upon request, to obtain a copy of the data

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 unauthorised 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

Service Provider Liability

ISP Liability

- Growing international consensus that immunity necessary for:
  - Acting as a transmission host
  - Automatically caching user requested resources
  - Hosting resources under control of third party
  - Providing search and directory facilities

- Growing international consensus immunity will be lost if:
  - ISP fails to comply with court order to remove material
  - ISP exercises positive control over the material e.g. by editing [monitoring?] [EXCEPTION – United States]
  - ISP hosts a resource, immunity lost once unlawful nature of resource becomes known to it

US - Communications Decency Act of 1996

- Old rule: carrier may become a publisher by editing content, and thus could be liable for knowingly or negligently distributing defamatory material
  - Newspaper is liable, while telephone company is not
- Communications Decency Act: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." (47 USC 230 (c)(1))
- Policy rationale:
  - Impossible for ISP to screen all postings
  - Don't discourage ISPs from self-policing; immunize them as a publisher, so that they can self-police without assuming additional liability; continue tradition of minimal government regulation of Internet

Extension of Communications Decency Act Into Other Areas

- *Stoner v. eBay*: CDA shields ISPs from suits for unfair business practices under a California statute
  - Also applied to bar suits based on negligent dissemination of e-mail, intentional infliction of emotional distress and posting of allegedly inaccurate stock price information
- BUT in *Gucci America, Inc. v. Hall & Assoc.*, not a shield against trademark infringement actions
  - CDA states that it may not be "construed to limit or expand any law pertaining to intellectual property"

U.S. -- Digital Millennium Copyright Act of 1998

- Imposes criminal sanctions for removing security features
  - Russian programmer visiting U.S. was arrested in 2001 for tampering with Adobe eBooks software's security features
- "Online service provider" or OSP defined broadly - a provider of online services or network access, or the operators of facilities therefor
  - Do not need to be in the business of providing online services
- Creates 4 safe harbors for OSPs from copyright infringement actions (in addition to other defenses under copyright and other laws):
  - Storing material at request of user
  - Referring users to material at another location
  - System caching, where OSP makes temporary copy for delivery to subsequent users (applies to both material placed on line by someone other than OSP ("Originator") and material transmitted by Originator through OSP to user)
  - Acting as conduit for material traveling between other parties

Notice and Take-Down Provisions

- OSP must designate, to U.S. Copyright Office and on its service, contact information
- Notice from copyright owner must be in writing, signed, include specified info.
  - Napster and ALS Scan v. RemarQ Communities cases have raised questions as to type of notice required before an OSP can be held liable, and level of detail required in that notice
- Upon receiving such a notice, OSP must act expeditiously to remove/block access to allegedly infringing material
- OSP exempt from liability for copyright infringement when it in good faith removes or blocks access to material

Notice and Pullback Provisions

- OSP must take additional steps to protect content provider, which may lead to putting material back in system
- OSP must take reasonable steps to notify content provider, who in turn may send “counter notification”
- OSP must provide copy of counter notification to copyright owner that sent original notice
- Unless copyright owner notifies OSP that it has filed an action to restrain the alleged infringement, OSP must replace or unblock the material within 10-14 days of receiving the counter notification

Limitations on ISP Liability

- Contracts used to regulate liability (with accompanying problems of on-line contracting / jurisdiction / consumer legislation)
- Contracts do not assist ISP in actions by third parties or for criminal liability
- English Law
  - Copyright – Copyright, Designs and Patents Act 1988
  - Obscenity and indecency – Obscene Publications Act 1959
  - Defamation – UK Defamation Act 1991 – Godfrey v Demon
- **EU E-Commerce Directive**
  - Art 12 Mere Conduit
  - Art 13 Caching
  - Art 14 Hosting
  - Art 15 No obligation to Monitor
- **UK draft implementing regulations are the FSMA 2000 (Financial Promotion)(Amendment)(Electronic Commerce Directive)Order 2002.**

Linking, Framing and Related Issues

Who Owns Linking?

- British Telecom claims that it owns a 1989 patent that covers hyperlinking, and it is currently suing an ISP to enforce that patent
- *Markman* claim interpretation: BT's patented invention involves the use of a single computer serving information to multiple terminal devices
  - Some analysts believe that hyperlinking is not covered by the patented invention, as so interpreted
- Prior art: 1945 *Atlantic Monthly* article; 1968 demonstration
- BT claims that administrative impracticality would prevent it from suing individual Internet users
  - But royalties which ISPs might have to pay to BT could be passed on to users in the form of higher fees

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 web site 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*
  - *Kelly v. Aribba Soft Corp:* Clicking on thumbnail image and displaying it within search engine's screen is framing, and distinguishable from pure hyperlinking

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*)

Metatags

- Html code often used to describe the subject matter of a web site
  - invisible to visitor of web site
  - 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 web site) does not necessarily avoid trademark infringement liability
- UK case – Reed Executive v. Reed Business Information

Linking and Framing – EU Perspective

- Activities of Re-User:
  - Copying third party content and posting copy to own web page
  - Including third party content in own web page by a visible link
  - Including third party content in own web page by an invisible link
- Express Licences (accompanied by problems of contracting on line)
- Implied Licences:
  - Saphena Computing Ltd v Allied Collection Agencies Ltd 1995
  - Trumpet Software Pty Ltd v Ozmail Pty Ltd 1996
  - Shetland Times v Shetland News 1997

Brobeck Hale and Dorr

Cyber-trespass

Spam

- Spam is unsolicited commercial mass E-Mail messages
- *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
- On appeal, *Hamidi* court found that, even assuming Intel has not demonstrated sufficient "harm" to trigger entitlement to nominal damages for past breaches, Intel showed Hamidi was disrupting its business by using its property and therefore is entitled to injunctive relief
  - Specifically, the court referred to the disruption of Intel's business based on the time spent by Intel employees in reading spammed email messages and blocking further messages

Spidering

- Use of “spiders,” “bots” or other automated means to derive information from publicly-accessible web sites
- *eBay, Inc. v. Bidder’s Edge, Inc.*: use of automated means to collect data from auction site for other purposes constitutes cybertrespass
  - Violation of eBay’s right to exclude others from its computer systems

Spidering – How Much Damage is Required for Cyber-trespass?

- *Oyster Software v. Forms Processing, Inc*.:
  - Defendant argued that his bots placed a negligible load on Oyster's computer system, and therefore the physical harm done to Oyster was also negligible
  - Court nonetheless agreed with Oyster's assertion that use of bots to copy Oyster's metatags was sufficient for Oyster to prevail on its trespass claim, and issued injunction.
    - "While the *eBay* decision could be read to require an interference [with property] that was more than negligible, this Court concludes that *eBay*, in fact, imposes no such requirement."

Spidering – How Much Damage is Required for Cyber-trespass?

- *Register.com, Inc. v. Verio*
  - Use of automated bots to search Register.com's WHOIS database
  - Although there was no specific physical harm to Register.com's web site, court issued injunction, finding that Register.com's loss of control over its web site was "possessory interference," which was sufficient harm to constitute trespass

Web Crawling

- Monitoring of web sites for various reasons
  - Confirming compliance with contractual commitments (e.g., affiliate networks)
  - Checking pricing of competitors
    - Unlike spidering, not collecting data and displaying that data publicly for other purposes
- Unclear area of law, so take precautions
  - Obtain consent of monitored party
  - Only monitor sites whose terms of use do not prohibit such use
    - Under Ticketmaster case, when are those terms binding? click-and-accept? simple posting?
  - Seek indemnification from company offering web crawling services

Brobeck Hale and Dorr

For further information:

- Hale and Dorr Internet Alerts at http://www.haledorr.com/internet_law/e_alerts.html
- Sarah Harrop at +44-20-7645-2524 or harrop@bhd.com
- Jorge Contreras at +44-20-7645-2508 or contreras@bhd.com
- Ken Slade at +1-617-526-6184 or kenneth.slade@haledorr.com