

# **E-Commerce: Current Issues and Trends in Germany, the EU and US**

Brobeck Hale and Dorr

Munich

July 2, 2002

Brobeck Hale and Dorr

## Overview

	Page
• Cross-Border Jurisdictional Issues	4
• Enforceability of On-Line Agreements	17
• Privacy and Data Protection Issues	42
• Service Provider Liability	58
• Linking, Framing and Related Issues	73
• Cyber-Trespass	82
• Business Method Patents	91

## Some Recent Figures About E-Commerce in Germany / EU

- Winter 2001/2002:
  - 26,5 Million people in Germany purchased goods and services for €2,6 Billion
  - 18,5 Million “e-customers” in the UK, only 5,6 Million in Spain and 3 Mio. in France
  - Largest EU markets: Tourism (24,9 Million customers), books (20,7 Million) and computer (19,3 Million)
- EITO prognosis: €440 Billion B2B sales in 2003

# **1. 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

## *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

## Cross-Border Issues in Germany/EU: Defendant Located in the EU

- Where can we sue the defendant?
- New EUGVVO applicable since March 01, 2002
- In general:
  - Individuals must be sued in the courts where they have their legal residence (*Art. 2 para 1*)
  - Legal entities must be sued where they have their legal seat (*Art. 60*)

## Cross-Border Jurisdiction Issues: Defendant Located in the EU (cont.)

But:

- Venue of the branch (*Art. 5 No.5*)
- In contract disputes: venue of the place of fulfilment (*Art. 5 No.1* – for sales of tangible goods place of delivery)
- Consumer venue (*Art. 15, 16*): in most cases at the legal residence of the consumer

## Defendant Located Outside of the EU

- German international law of civil procedure is applicable; provisions of the ZPO are applied mutas mutandis

In general:

- Individuals must be sued at the courts where they have their legal residence (Sec. 12, 13, 16 ZPO)
- Legal entities must be sued where they have their legal seat (Sec. 17 ZPO)

## Defendant Located Outside of the EU (cont.)

In particular:

- Venue of the branch, if the claim is related thereto
- Venue where assets are located, Sec. 23 ZPO, if assets in Germany and a sufficient relation, i.e. in on-line cases:
- Is the business of the ISP directed to Germany?
- Is there a significant number of German customers?

## Defendant Located Outside of the EU (cont.)

- In contract disputes: venue of the place of fulfilment, i.e.
  - Duties fulfilled off-line: seat of the ISP regarding Delivery /residence of customer regarding Payment
  - Duties fulfilled on-line (e.g. download of software): Legal seat of the ISP

## **Applicable Laws: ISP Located within the EU – Country-of-Origin Principle**

- Introduced by the EU e-commerce Directive 2000/31/EG and the new German law on e-commerce (EKG)
- Since January 01, 2002, on-line practices of any ISP with its legal seat within an EU member state will be governed by the laws of that member state
- But: National consumer protection laws remain applicable

## Applicable Laws: ISP Located outside the EU

- International private law rules apply
- German consumer protection laws remain applicable



## **2. 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*

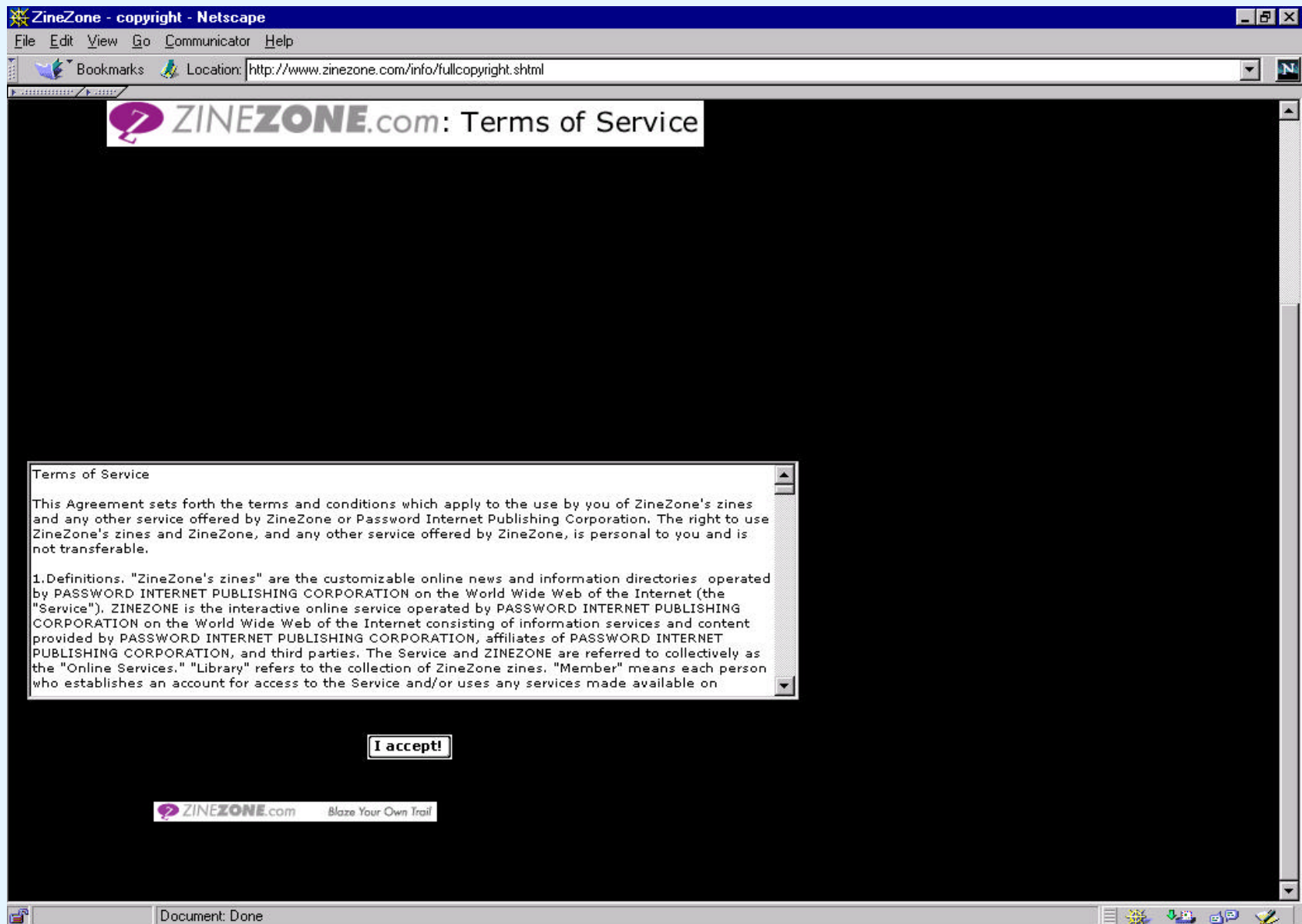
- Court concluded that mere downloading did not equal assent
- Court also rejected the idea that user could be bound to a contract without even seeing the message referring to that contract
- In addition to the way the message was shown, court found that language used was merely an invitation to agree,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

## 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





## 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:
  - Send that prospective buyer a copy of the terms and state very clearly that:
    - Seller's acceptance of the purchase order is expressly conditioned upon those terms; and
    - Seller shall not ship the product until the prospective buyer communicates its acceptance of those terms; or

## Strategy for Enforceability: Step #5 - Battle of Forms (cont.)

- (although a bit riskier) Ship the product with a packing slip that clearly and prominently states that:
  - Shipment of the product is pursuant to the buyer's purchase order and is subject to Seller's terms; and
  - 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.

## **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

# Enforceability of On-Line 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 Issues: General Terms in the B2C Area

- When concluding the agreement
  - 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



## Enforceability Issues: General Terms in the B2C Area (cont.)

Follow:

- Step#1 Method 2 (see slide 23) plus download (link or website click box) or
- Step#5 a) or b) (riskier) each plus download (see slides 28-29)

## Enforceability Issues: General Terms in the B2B Area

- B2C rules mainly not applicable, 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

## **Enforceability Issues: General Terms in the B2B Area (cont.)**

Follow:

- Step#1 Method 1 or 2 (see slides 22-23) or
- Step#5 a) or b)(riskier), see slides 28-29.

Each method also requires the ability to download the terms (link/click box on website)

## **Enforceability Issues: Distance Purchases with Consumers**

- Information obligations of the seller (see the new Sec. 312 c BGB (German Civil Code) and the corresponding information directive
- Before conclusion of the agreement provide information about (inter alia): identity of the seller, address, essential features of the product or service, limitations upon obligation to make delivery, price including taxes, shipping cost, right of revocation

## **Enforceability Issues: Distance Purchases with Consumers (cont.)**

- Without delay, and no later than upon fulfilment of the agreement, vendor must provide the following information in written form (email sufficient) to the customer:
  - Sec. 312 c I: see previous slide
  - Details of revocation/return right
  - Details of seller
  - Details of services and warranties
  - If applicable, details of termination

## **Enforceability Issues: Distance Purchases with Consumers (cont.)**

Legal consequences in case of violations:

Agreement remains effective, but

- Time period for revocation right will not start before receipt of information ; it will end, however, 6 months after conclusion of the contract
- Potential damage claim of consumer (proof of damage unlikely)
- Sanctions by consumer protection groups

## **Enforceability Issues: E-Commerce Obligations, Sec. 312 e BGB**

- Inform customer about technical steps to complete the contract
- Provide the customer with adequate technical means to recognize and correct improper entries before submitting order
- Inform customer about whereabouts of copy of agreement and its accessibility
- Inform customer about language options, if available

## **Enforceability Issues: E-Commerce Obligations, Sec. 312 e BGB (cont.)**

- Notify the customer, if any vendor policies apply (e.g. privacy policies), and, if so, provide on-line access thereto
- Confirm any submitted order immediately by electronic means



## **Enforceability Issues: E-Commerce Obligations, Sec. 312 e BGB (cont.)**

Legal consequences in case of violations:

- Agreement remains effective, but:
- Time period for revocation right will not start before receipt of information; it will end, however, 6 months after conclusion of the contract
- Potential damage claim of customer
- Sanctions by consumer protection groups

### **3.**

## **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 on-line information collection
    - CHOICE regarding uses of that information

# Privacy: U.S. Perspective

- ACCESS to ensure that information is accurate, complete, and up-to-date
  - SECURITY and integrity of information collected on-line; 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 on-line 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 on-line data.

**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.

## Enforcement (cont.)

**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."

## On-Line Profiling

- On-line 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 on-line profiling companies, formulated a set of self-regulatory privacy guidelines
- Those guidelines have been endorsed by the FTC



# Privacy and Data Protection in Germany and in the EU

## Legal Sources:

- EU Directive 95/46/EG regarding personal data protection
- German Data Protection Act (Bundesdatenschutzgesetz – BDSG)
- Teleservices Data Protection Act (Teledienstschutzgesetz – TDDSG)

## Privacy: German / EU Perspective

- EU Data Protection Directive became effective on October 15, 1995; had to be transformed into national law by October 15, 1998; has been transformed into German national law by May 18, 2001
- Establishes legal principles for privacy protection and free flow of data within the EU
- Prohibits the transfer of personal data from EU countries to any countries which do not have “adequate” data protection laws
  - In other words, the United States, but see “safe harbor” principles

## EU Rights of the Data Subject

- Right to be informed of the reasons for data collection, intended recipients, and data subject's rights, at the time of collection.
- Right to obtain a copy of data about oneself.
- Right to obtain corrections, erasure or blocking of data processed in violation of the Directive.
- Appropriate security safeguards must be adopted by controllers of data.
- Data cannot be kept in identified form for longer than necessary for those purposes.

## Privacy and Data Protection in Germany: Initiate On-Line-Agreements

- 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

# Privacy and Data Protection in Germany: Tele Services Data Protection Act

- New Tele Services Data Protection Act (Teledienststedatenschutzgesetz – TDDSG) in force since January 1, 2002
- Obligations of the ISP
  - Data subject must be informed at the beginning of each process about method, purpose, scope of collecting, processing and use of personal data and, whether data is processed outside of EU

## Privacy and Data Protection in Germany: Tele Services Data Protection Act (cont.)

- On-line-consent of the data subject is only valid if the collector ensures that
  - The consent is given by an unequivocal and deliberate act
  - The consent is logged
  - The content of the consent can be retrieved by the data subject at any time

## Privacy and Data Protection in Germany: Tele Services Data Protection Act (cont.)

- Instruction to the data subject about right to revoke consent with effect for the future
- Provider has to ensure with adequate means that
  - User can disconnect the line at any time
  - Personal user data can be immediately deleted or blocked after the process
  - The process for entering data about the user is secure

## Privacy and Data Protection in Germany: Tele Services Data Protection Act (cont.)

- Data about each personal user can be processed separately
- Personal user data is only used for billing purposes
- Anonymous user profiles for marketing purposes etc. are not combined with personal data about the user



# Privacy and Data Protection in Germany: Cookies

- Not generally unlawful
- If they contain personal related data, use is problematic due to restrictive data protection laws (Sec. 3 TDDSG)
- Some consider use of cookies as violation of possession laws (Sec. 862 BGB), some as an unlawful tort (Sec. 826 BGB)

## 4. Service Provider Liability

# 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))

# US-Communications Decency Act of 1996 (cont.)

- 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
- “On-line service provider” or OSP defined broadly - a provider of on-line services or network access, or the operators of facilities therefor
  - Do not need to be in the business of providing on-line services

## U.S. -- Digital Millennium Copyright Act of 1998 (cont.)

- 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

# ISP Liability: German / EU Perspective

- EU E-Commerce Directive:
  - ISPs are not liable for infringing third party content unless they know or could have known about the illegal content
  - No obligation to monitor
  - However, once ISP learns that particular content is illegal, ISP must block access to such content

## ISP Liability in Germany – Tele Services Act

- New Tele Services Act (Teledienstegesetz – TDG) in force since Jan. 1, 2002
  - Teleservices include, inter alia
  - Electronical distribution of advertisements for goods and services
  - M-commerce
  - Offers to use the internet
  - Offers of products or services within interactive electronic data banks
- Thus ISP's and entities which offer on-line-agreements are included

## ISP Liability in Germany – Tele Services Act (cont.)

- Country-of-Origin principle, Sec. 4 TDG
  - German/EU providers are subject to the laws where they have their legal seat
  - Exemptions (inter alia):
    - Local consumer protection laws apply
    - Local copyright, industrial property and anti trust law rights apply
    - Local data protection laws apply
    - No different choice of law

## ISP Liability in Germany – TDG Information Duties

- Sec. 6: detailed information about the provider
  - Name and address; legal entities have to name their representatives
  - An e-mail contact address which enables quick contact
  - Registration No., e.g. from the Commercial register, if applicable
  - VAT No., if available

## ISP Information Duties (cont.)

- Any authority or professional regulatory organization to which the provider is subject, its correct professional name and professional rules with a link (if applicable)
- All information should be easily visible and accessible and present – thus be present on the homepage (as an imprint)
- Fines of up to € 50000 per violation

## ISP Liability in Germany – Liability Privileges, Sec. 8-11 TDG

- Sec. 9: No ISP liability for mere conduit (Durchleitung), if
  - Transfer was not caused
  - No selection of addressees
  - No selection or choice of information

## ISP Liability in Germany – Liability Privileges, Sec. 8-11 TDG (cont.)

- Sec. 11: No ISP liability for storing information of third parties, if
  - No positive knowledge or grossly negligent ignorance of unlawful information or
  - Immediate action to delete or block information after ISP has knowledge
  - Website guest books have to be controlled at least once a week (Regional Court Trier (4 O 106/00))



## **5. 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

## Who Owns Linking? (cont.)

- 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)

## Clearly Prohibited Linking Practices (cont.)

- 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*)

## Linking, Framing: German / EU Perspective

- Linking to a page protected by a trademark is considered lawful due to an implied consent of the trademark owner (OLG Düsseldorf MMR 1999, 729; but see opposite view LG Hamburg CR 2001, 265)
- Deep linking is unfair trade practice (disputed)
- Framing is unfair trade practice
  - Framing may be considered to be misleading, Sec. 3 UWG and unlawful, Sec. 1 UWG
  - UK: Shetland Times (EIPR 1 (1996), 723)

## 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



## 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 – Steinhöfel)

## 6. 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

## Spam (cont.)

- 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

## Spam: German / EU Perspective

- 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 have to be recognizable for the recipient (Sec. 7 TDG)

## Spam: German / EU Perspective (cont.)

- Regional Court Frankfurt/M. (CR 2002, 220 – web.de):
  - Search engine operator is not liable according to Sec. 1 Unfair Competition Act (UWG) for “index-spamming” i.e. flooding with links to the spammer’s own homepage. Nor is it reasonable for the operator to block the information acc. to Sec. 5 IV TDG.

# 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

# **7. Business Method Patents**

## The State Street Bank Patent

- U.S. Patent No. 5,193,056, entitled “Data Processing System for Hub and Spoke Financial Services Configuration”
- Claims were for an apparatus, including a computer, storage, and arithmetic logic circuits for providing processing for managing a particular financial services configuration
- The U.S. Court of Appeals for the Federal Circuit in 1998 expressly endorsed business method patents, describing the courts’ earlier “business method exception” to patentable subject matter as “ill-conceived”

# What is a Business Method Patent?

- Not defined in State Street Bank case
- Often involve Internet-based business models
- Often similar to old business models, but adjusted for application to the Internet
- Frequently include software or hardware components

## Famous Examples of Business Method Patents

- Amazon.com's U.S. Patent No. 5,960,411: Method and System for Placing a Purchase Order via a Communications Network (1-click shopping)
- Priceline's U.S. Patent No. 5,794,207: Method and Apparatus for a Cryptographically Assisted Commercial Network System Designed to Facilitate Buyer-Driven Conditional Purchase Offers (reverse auctions)
- Open Market's U.S. Patent No. 5,715,314: Network Sales System (payments, shopping carts)

## How will Business Method Patents be Interpreted and Treated?

- Narrow interpretations likely
- Lack of enablement or inadequate written description arguments may be more difficult than in the biotech context
  - The technology is often relatively simple
- But “obviousness” presents a promising defense
  - Particularly with broad claims

# Protection

- Protection of Software
  - Sec. 69a *et seq* German Copyright Act (UrhG)
  - Directive 91/250/EC
- Protection of Business Methods
  - Unfair competition law
  - Contractual

Slight 1



# Protection

- Patents may
  - Lead to a better and more secure position in the market
  - Prohibit others from using the SW/BM
  - Be a source of license fees
- Patents are assets to attract investors

Slight 2

## Examples

- Airline X creates a "Frequent Flyer" program
- E-commerce company develops Software which can be used to find the best offer on the Internet
- Software company develops a computer device which contains a SW-based process for language analysis

**Slight 3**

## Pro and Contra

- Cons
  - Patents lead to a monopoly position and obstruct competition
- Pro
  - Patents encourage competition by providing incentives for developing technology
- See also "Open Source" Discussion

Slight 4

# Legal Background Germany I

- Sec. 1 of the Patent Act (PatG):
  - Para 1: Patents shall be granted for any inventions which are
    - New
    - Based on an inventive step
    - Commercially applicable
  - Para 2 No. 3: Programs for computers among other things are not regarded as inventions
  - Para 3: However, Para 3 excludes patentability only to the extent that the inventor **as such** seeks patent protection for the computer program

Slight 5

## Legal Background Germany II

- “Technical nature of an invention“
- Federal Court decisions (old)
  - "Antiblockiersystem", 1980 ("core doctrine")
  - "Seitenpuffer", "Tauchcomputer", 1992 ("overall view whether technical or not")
  - "Chinesische Schriftzeichen", 1992 ("not technical but language science")

Slight 6

## Legal Background Germany III

- Recent Federal Court decisions
  - „Logikverfahren“, 1999 ("extensive technical (engineering) skills")
  - „Sprachanalyse-Einrichtung“, 1999 („installed on a computer device“)
  - „Zeichenketten“, 2000 (“implementation on data processing media alone is not sufficient”)

Slight 7

## Legal Background US

- 35 USC § 101:  
“Whoever invents...any new and useful process, machine, manufacture, or composition matter...may obtain a patent.”
- State Street Decision 1998:  
“any subject matter may be patentable which is new and useful, regardless of any technical contribution.”

Slight 8

# Legal Background Europe I

- EPO: “An invention is a technical response to a technical problem”:
  - Vicom Decision 1987
  - IBM Decisions I and II, 1999

**Slight 9**



## Legal Background Europe II

- Draft Directive on Patentability of Computer-Implemented Inventions, 2002
  - “Technical contribution”
  - “No patents for computer programs only because they are implemented on a carrier”
  - Business Methods are not patentable

Slight 10

# Legal Background Summary

- Germany:**
- Technical effect
  - If implemented on a computer device
  - No patentability of business methods
- US:**
- New and useful, including business methods
- EU (Future):**
- Technical contribution
  - No patentability of business methods

Slight 11

# IP Strategy

- Patents may be:
  - Expensive
  - Disclose trade secrets
  - Not efficient (product dependent)
- Alternatives:
  - Trademark strategy
  - Non-disclosure agreements
  - Non-competition clause
  - Non-solicitation clause
  - Non-disclosure of the source code/escrow agreements

Slight 12

## For further information:

- Hale and Dorr Internet Alerts at [http://www.haledorr.com/internet\\_law/e\\_alerts.html](http://www.haledorr.com/internet_law/e_alerts.html)
- Ken Slade at +1-617-526-6184 or [kenneth.slade@haledorr.com](mailto:kenneth.slade@haledorr.com)
- Dr. Christian Breuer at +49-89-24-213-107 or [breuer@bhd.com](mailto:breuer@bhd.com)
- Dr. Florian von Baum at +49-89-24-213-101 or [baum@bhd.com](mailto:baum@bhd.com)