Update on Internet Law and E-Commerce: A U.S. Perspective

Kenneth Slade
Senior Partner, Hale and Dorr LLP
Boston, Massachusetts, USA

Asahi Law Offices
Tokyo, Japan
February 22, 2001

HALE AND DORR LLP

Overview

- Domain name problems
- Enforceability of click-and-accept agreements
- Cross-border jurisdiction issues
- Internet Service Provider (ISP) liability and safe harbors against copyright infringement suits
- Linking problems: deep linking, spidering and web crawling
- Privacy
- Spam
- Other issues

Domain Name Problems

U.S. Anticybersquatting Consumer Protection Act

- Signed into law November 29, 1999
- Permits action vs. domain name registrant purely on the basis of registration, without use and without effect on well-known trademark
- Provides basis for attacking domain name which is “identical or confusingly similar” to protected trademark or name of living person
- Domain name registrant must have “bad faith intent to profit”

Anticybersquatting Consumer Protection Act: Remedies

- If a domain name has been registered improperly, it may be canceled or forfeited to rightful owner
- Courts may award, at plaintiff's election, either actual damages or statutory damages up to US$100,000 per domain name
- Internet Alert December 7, 1999

ICANN Dispute Resolution Policy

- New Uniform Domain Name Dispute Resolution Policy adopted by principal U.S. and international domain name registrars
- Part of agreement every registrant must accept prior to obtaining a domain name
- Policy permits trademark owner to bring arbitration against registrant of domain name that is identical or confusingly similar to trademark if registrant has registered the domain name in bad faith

ICANN Arbitrations

- World Intellectual Property Organization (WIPO), National Arbitration Forum, Disputes.org/eResolution Consortium and CPR Institute for Dispute Resolution approved to act as arbiters
- Sole remedy is to cancel registration or transfer it to trademark owner
- Streamlined procedure:
  - designed to be conducted by E-Mail
  - takes less than 60 days
  - no discovery
- Internet Alert February 15, 2000

Remaining Problems

- Someone other than the trademark owner who is legitimately using the trademark as a domain name (e.g., a distributor) can continue to do so (Weber-Stephens case)
  - Internet Alert June 2, 2000
- Registrations of well-known domain name in another country without bad faith are still valid (e.g., amazon.gr)

Remaining Problems

- "Sucks.com" web sites might be difficult to shut down in certain circumstances
  - where the operator of the web site is not demanding compensation for transferring the domain name back to the trademark owner
  - where the court considers the web site to be a parody, or protected U.S. First Amendment speech
  - where the web site is not "likely to cause confusion"
- Internet Alert September 13, 2000

Enforceability of Click-and-Accept Agreements

Why use click-and-accept agreements?

- Given the volume of transactions (hopefully!), 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
- Using click-and-accept agreements discourages even large buyers from insisting on separately negotiated terms

Enforceability of Shrinkwrap Agreements

- First used for mass-market software
- No signature: use of software = assent
- Shrinkwrap agreements validated in *Pro CD v. Zeidenberg* (7th Cir. 1996) if
  - 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 terms must be printed on the outside of the product packaging.

Enforceability of Click-and-Accept Agreements

- In Groff v. America Online, Inc., Groff sues over unavailability of AOL service, due to load problems
- AOL seeks summary judgment, arguing that forum selection clause in click-and-accept agreement requires litigation to be brought in Virginia
- Court finds that Groff effectively "signed" the click-and-accept agreement by clicking on "I agree" button "not once, but twice"
- Internet Alert March 22, 2000

U.S. 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 Licensor's terms and conditions of sale.

U.S. 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

U.S. Strategy for Enforceability: Step #2 - Installation

- As part of the installation program for any downloaded software 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.

U.S. Strategy for Enforceability: Step #3 - 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.
  -

U.S. Strategy for Enforceability: Step #4 - Battle of Forms

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

Domestic Strategy for Enforceability: Step #4 (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 user's purchase order and is subject to Licensor's terms; and (ii) if the user does not accept those terms, it should return the product and Licensor will refund any amounts that the user may have already paid for that product.

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

Terms of Use Not Necessarily Binding

- According to the recent *Ticketmaster* case, posting terms on the bottom of the first page of a web site does not make those terms legally enforceable against users of that web site
  - users were not required to assent to those terms, or even to read them
- For those terms to constitute a legally-binding contract, the web site operator must show that users knew or should have known that acceptance of those terms was a condition for using the web site
  - for example -- a "click-and-accept" on registration, download or ordering
- Internet Alert June 26, 2000

Cross-Border Jurisdiction Issues

Importance of Jurisdictional Issues

- Jurisdictional 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

Why are these problems greater for e-commerce than for offline commerce?

- Less likely to be negotiated contracts
  - parties reacting only remotely
  - emphasis on automated, mass market solutions on the Internet
- Sellers won't necessarily know where their customers are located
- Buyers face greater risks, dealing with potentially invisible sellers

Current Troublespots

- 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
- 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
  - Internet Alert January 24, 2001
- 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
- American Bar Association is trying to propose standardized guidelines

Internet Service Provider (ISP) Liability and Safe Harbors against Copyright Infringement Suits

U.S. -- 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
- New rule: "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; continue tradition of minimal government regulation of Internet
- Contrast to trend in other jurisdictions -- Internet Alert December 5, 2000

Zeran v. America Online, Inc. 129 F. 3rd 327 (4th Cir. 1997)

- If computer service providers were subject to distributor liability, they would face potential liability each time they receive notice of a potentially defamatory statement -- from any party, concerning any message. Each notification would require a careful yet rapid investigation of the circumstances surrounding the posted information, a legal judgment concerning the information's defamatory character, and an on-the-spot editorial decision whether to risk liability by allowing the continued publication of that information. Although this might be possible for the traditional publisher, the sheer number of postings on interactive computer services would create an impossible burden in the Internet context.

U.S. -- Digital Millennium Copyright Act of 1998 ("DMCA")

- Creates 4 safe harbors for ISPs from copyright infringement actions
  - in addition to other defenses under copyright and other laws
- "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
- Internet Alert April 11, 2000

DMCA Safe Harbors

- 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 travelling 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.
- Upon receiving such a notice, OSP must act expeditiously to remove/block access to allegedly infringing material
- OSP exempt from liability 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

Linking Problems: Deep Linking, Spidering and Web Crawling

Clearly Prohibited 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)
  - Internet Alert February 29, 2000
- 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)*

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
  - Internet Alert June 7, 2000
- Similar result in Dutch case (*PCM v. Kranten.com*)

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
  - Internet Alert June 9, 2000

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 presenting that data 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

Privacy

State of Confusion?

Consumer Demands

Privacy Laws

Privacy Regulations

"Self-regulation"

Foreign Practices

Fair Information Practices

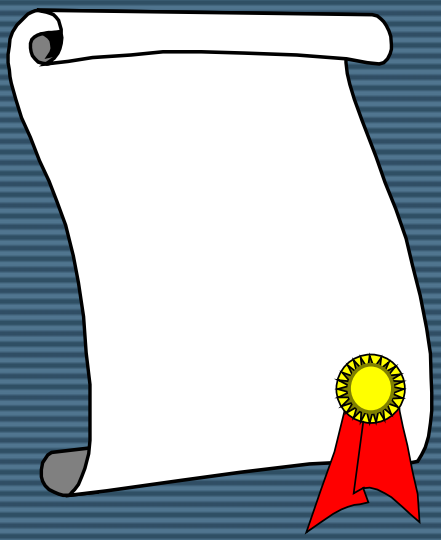
Fair Information Practices

1. **Notice**
2. **Choice**
3. **Access**
4. **Security**
5. **Enforcement**

Internet Alert May 2, 2000

Fair Information Practices

1. NOTICE



Before collection, use, or disclosure,

- Who is collecting data?
- What data is collected?
- How data is collected?
- Why data is collected? (primary uses)
- What other uses? (secondary uses)
- How data is protected?
- What choices are available?

Fair Information Practices

2. CHOICE

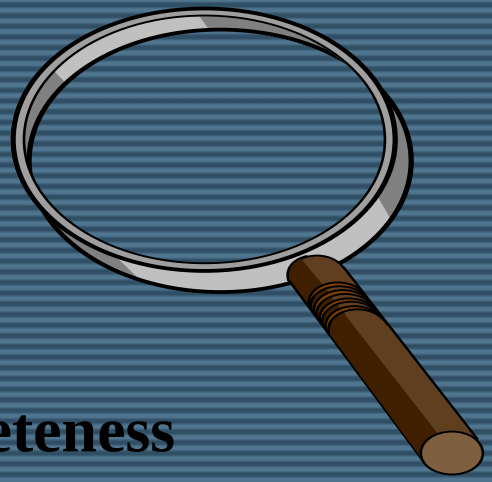
Consent to secondary uses of data:

Opt-in

Opt-out

Fair Information Practices

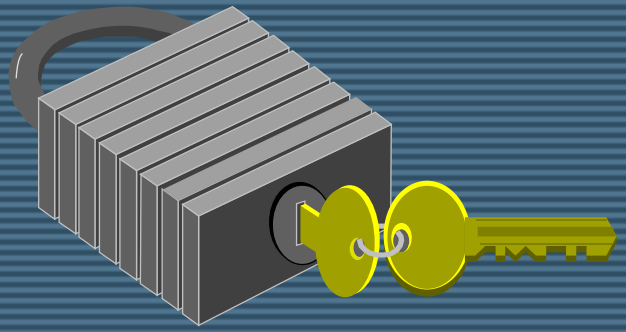
3. ACCESS



- Right to **view** data about oneself
- Right to contest **accuracy** & **completeness**
- **Procedures** for viewing & requesting revisions

Fair Information Practices

4. SECURITY



- **Data Integrity**
  - Trusted sources
  - Up-to-date
  - De-identification
- **Data Security**
  - Managerial safeguards
  - Technical safeguards
  - Physical safeguards

Fair Information Practices

5. ENFORCEMENT

- Complaint procedure
- Investigation
- Redress
- Sanctions

Federal Internet Privacy Mandates

Internet privacy mandates follow a **"sectoral"** approach:

- **Children's privacy**
- **Health data privacy**
- **Financial data privacy**

Mandates expand upon Fair Information Practices:

Notice: Timing, placement & content
Choice: Prior consent

Federal Mandates: Children's Privacy

Children's Online Privacy Protection Act

Law enacted 1998

FTC regulations took effect **April 21, 2000**

- Protects **"personal information"**
- Collected by web sites and online services
- From children **under 13**

Focus on

Notice to parents

Advance parental **consent**

- Internet Alert February 11, 2000

Federal Mandates: Electronic health data

- HHS regulations issued December 28, 2000; to become effective in February 2003

- Protects **electronic, identifiable health data** handled by: Health plans; Health care providers; Health care "clearinghouses" (claims processors); and Business partners

- Consent required for uses other than **treatment, payment and "health care operations."**

- **Exceptions** for research, public health, law enforcement, emergencies, etc.

- Internet Alert November 2, 1999

Federal Mandates: Financial Data

Gramm-Leach-Bliley Act enacted November 1999
Final rules issued May 2000

Protects **"nonpublic," personally-identifiable** information handled by **"financial institutions" "significantly engaged"** in financial activities with consumers.

Notice requirements:

- Initial notice at start of customer relationship
- Annual notices to customers
- Notice to consumers prior to disclosure

Choice requirements:

- Opt-out of disclosures to nonaffiliated third parties

Self-regulation

FTC is watching for voluntary implementation of FIPs:

Websites with posted privacy policies

1998 survey:	2% overall, 44% of busiest websites
1999 survey:	44% of sampled websites
1999 survey:	81% of busiest websites
2000 survey:	96% of sampled websites

- **Congress might not wait…** Current proposals could
  - Restrict use of "cookies"
  - Require opt-out of online tracking

- Internet Alerts May 2 and May 26, 2000

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. Settlement authorized sale only to "qualified purchaser."

Online Profiling

- Online profiling is seen as particularly invasive, even if the profile is not “personally identifiable”
- 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
- Internet Alert August 28, 2000

Looking Ahead

- Pressure to self-regulate
- More FTC enforcement
- Additional sectoral legislation
- Emerging case law
- International standards

Spam

Spam -- Judicial and Legislative Restrictions

- Spam is unsolicited commercial mass E-Mail messages
- April 1999: California Superior Court ruled that spam sent to Intel Corporation's employees constituted an illegal trespass of Intel's proprietary computer system
  - Internet Alert July 26, 1999
- Proposed legislative limitations
  - allow ISPs to sue unauthorized senders of unsolicited bulk e-mail

Spam -- Judicial and Legislative Efforts

- impose criminal penalties on senders who hide behind false domain names
- allow recipients to "opt-out" of future mailings
- California has imposed a controversial labeling requirement
- expand the existing federal law which already bans unsolicited commercial faxes
- proposed state laws prohibiting spam, but subject to constitutional challenge
  - Internet Alert November 29, 2000

Other Issues

Open Access

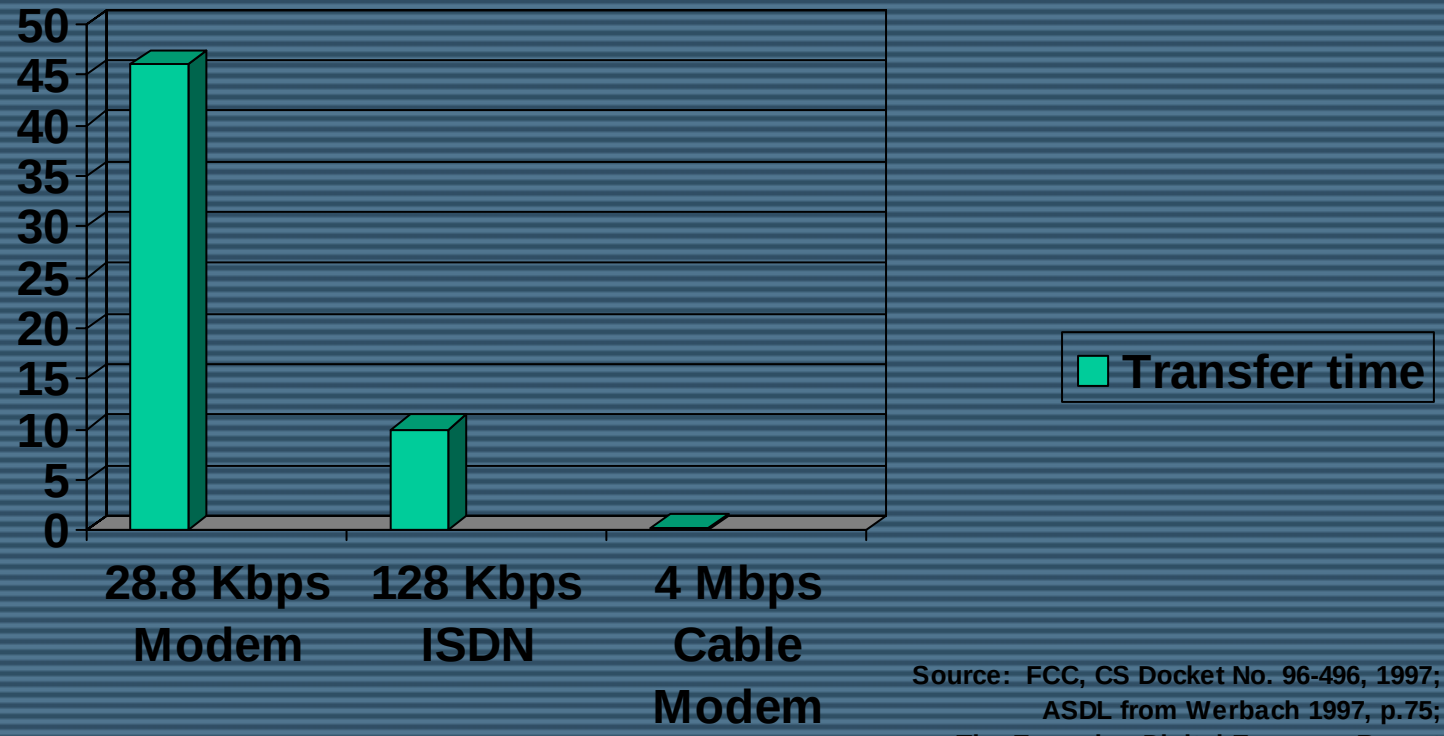
Lotteries, Sweepstakes and Contests

Business Method Patents

State Taxes

UCITA

Open Access: Fight over Internet Access Speeds (e.g., time to download 3.5 min. video clip)



Source: FCC, CS Docket No. 96-496, 1997; ASDL from Werbach 1997, p.75; The Emerging Digital Economy Report

Open Access May Not be Coming Quickly

- AT&T v. City of Portland -- Ninth Circuit did not allow municipality to condition transfer of cable franchise on AT&T's opening up of its cable system to competing ISPs
- Federal Communications Commission has the power to regulate cable broadband, but so far has not done so and has instead adopted a wait-and-see policy
- Internet Alert February 4, 2000

FCC's Latest Position on Open Access

- January 11, 2001: FCC conditioned its approval of cable license transfers in the AOL-Time Warner merger on AOL agreeing not to require customers to go through an ISP affiliated with AOL in order to reach their own preferred ISPs
- BUT: Newly-appointed Chairman Powell has spoken about taking a more "purely deregulatory" approach

Lotteries, Sweepstakes and Contests

- PRIZE awarded via CHANCE in exchange for some CONSIDERATION = LOTTERY
- Sweepstakes: NO CONSIDERATION --contests in which participants are not required to pay anything for a chance to win; need for alternative free method of entry
- Contests: NO CHANCE -- must be based on skill
- Some countries and U.S. states impose bonding and other requirements for any chance promotions
- Internet Alert November 23, 1999

Business Method Patents

- U.S. Patent Office is issuing a rapidly increasing number of e-commerce and business method patents
  - applications subclass for electronic shopping (e.g., remote ordering) increased by100% from 1998 to 1999
- examples include amazon.com's "single click of mouse" and referral system patents
- amazon.com used its "single click" patent to stop Barnes & Nobles from using this methodology during 1999 Christmas rush
- companies are considering developing their own patent portfolio, for defensive purposes
- Internet Alerts May 22 and December 21, 2000

State Tax Issues Looming

- Internet Tax Freedom Act established a three-year moratorium on new or discriminatory state and local taxes applied to e-commerce
  - Internet Alert August 1, 1999
- moratorium ends on October 21, 2001
- 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

Uniform Computer Information Transactions Act ("UCITA")

- New name for proposed Article 2B of the Uniform Commercial Code, for ALI would not approve
- Scope of UCITA
  - "computer information" means digital information, regardless of form
  - applies to transactions involving creation, modification, transfer or licensing of computer information
- Current status: so far, enacted only in Virginia and Maryland
- Text and official comments at http://www.law.upenn.edu/bll/ulc/ulc_frame.htm
- Internet Alert February 23, 2001

UCITA -- Issues

- Shrink-wrap and click-and-accept agreements enforceable
- Electronic self-help
- Impact on products that include software
- Contract modification
- Disclaimers of warranties
- Right of return

For Further Information

- Subscribe to Hale and Dorr Internet Alerts at www.haledorr.com/internet_law/e_alerts.html

- Contact Ken Slade
  - kenneth.slade@haledorr.com
  - telephone: 1-617-526-6184
  - fax: 1-617-526-5000
  - mailing address:
    - 60 State Street
    - Boston Massachusetts 02109
    - USA