E-COMMERCE AND THE LAW: HOTLINKS, SECURITY AND PRIVACY

Nelson G. Dong
Dorsey & Whitney LLP
Minneapolis, MN

DORSEY & WHITNEY LLP

Topics

- Background Issues
  - Business to Business e-commerce (B2B)
  - Business to Consumer e-commerce (B2C)
- Hotlinking
- Information Security and Encryption
- Privacy Law Developments

Growth of E-Commerce

- Glamorous, sensational stories in media about consumer-driven e-commerce ("B2C")
- Gartner Group estimates: 4 or 5X more business done in industrial and inter-company uses of e-commerce ("B2B") than in B2C
- B2B e-commerce raises numerous unique, unprecedented legal issues for corporations, particularly those doing business on multinational basis

Hotlinks

- "Hotlinks": hypertext technology to allow instantaneous access to related information at other websites (often highlighted in different color)
- Specific disclaimers about nature and extent of implied incorporation, endorsement, ratification, etc.
- Control and regulation of own website may be completely undercut by what is said (or not said) on hotlinked sites
- Disclaimers must be strategically placed on website

3M's Disclaimers for Hotlinks

- Basic: "3M makes no representations or warranties whatsoever about any other Web site which you may choose to access through this Web site."
- Links provided by 3M to such Web sites are provided solely for your convenience and should not be deemed to imply that 3M endorses those Web sites or any content therein. IN NO EVENT WILL 3M BE LIABLE TO ANY PARTY FOR ANY DIRECT, INDIRECT, SPECIAL OR OTHER TYPES OF CONSEQUENTIAL DAMAGES FOR USE OF THIS WEB SITE OR ANY OTHER HYPERLINKED WEB SITE INCLUDING SPECIFICALLY, BUT NOT EXCLUSIVELY, ANY LOST PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, EVEN IF 3M IS EXPRESSLY ADVISED ABOUT THE POSSIBILITY OF SUCH DAMAGES.

3M's Limitation of Liability (Basic and Hotlink)

- IN NO EVENT WILL 3M BE LIABLE TO ANY PARTY FOR ANY DIRECT, INDIRECT, SPECIAL OR OTHER TYPES OF CONSEQUENTIAL DAMAGES FOR USE OF THIS WEB SITE OR ANY OTHER HYPERLINKED WEB SITE INCLUDING SPECIFICALLY, BUT NOT EXCLUSIVELY, ANY LOST PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, EVEN IF 3M IS EXPRESSLY ADVISED ABOUT THE POSSIBILITY OF SUCH DAMAGES.

Effectiveness of Disclaimers

- "Advertising agencies and website designers are responsible for reviewing the information used to substantiate claims. They may not simply rely on an advertiser's assurance that the claims are substantiated."
- "Disclaimers and disclosures must be clear and conspicuous. . . . [A] disclaimer or disclosure alone usually is not enough to remedy a false or deceptive claim."

FTC, Rules of the Road: Advertising and Marketing on the Internet 2 (1998)

"Friendly"-Style Disclaimers

"Here is a list of other Web Sites you might want to check out.

While 3M has provided the links listed here, we are not responsible for the information contained in these sites. If you choose one of these links, you will leave our website.

If you wish to return to the 3M website after viewing one of these links, use the back arrow key. Or you may wish to bookmark our site for future access."

-- (http://www.mmm.com/surgicaldrapes/on_links.html)

Consequences of Non-Compliant Advertising or Ineffective Disclaimers

- FTC monitors Internet periodically for potentially false or deceptive advertising claims
- If non-compliant, a company may face FTC enforcement actions or civil lawsuits
- Increasing action by state attorneys general and even local county prosecutors

Privacy and Security

- Need for consumer, supplier or customer privacy
- Drive toward use of “strong” encryption
- Regulations on deployment of encryption tools
- Push for new privacy rules and laws

Information Security and Encryption

- Issues summarized in acronym "CAN IT?"

  Confidentiality of message — who can read it?

  Authenticity of message — who actually sent it?

  Non-repudiation of message — can it be denied later?

  Integrity of message — was it received as sent?

  Time of message — when was it sent and received?

Information Security and Encryption (Cont.)

- Robust public key encryption central to continued global expansion of e-commerce
- Historic tension between broader dissemination of encryption technology for commercial deployment vs. law enforcement and national security concerns
- Long-running conflict between industry and government (FBI, NSA, DOD, et al.) over degree of deregulation of "strong" encryption for export outside United States
- With growing power of available computers, size of databases and network connections, "crackers" and "hackers" pose significant risks to stability and growth of e-commerce

Information Security and Encryption (Cont.)

- Former "gold standard" of DES (56 bit key length) too easily broken and now officially recommended by NIST as insufficient for protection of critical domestic data of U.S. Government, banks, etc.
- Minimum key length should be at least 128 bit, given current generation of computers readily available to general public
- Projected "cracking" time of 0.066 second for 56 bit key length vs. 9.8 quadrillion years for 128 bit key length
- Industry, commercial pressures finally forced Clinton Administration's hand and overwhelmed NSA, FBI lobbying

Information Security and Encryption (Cont.)

- New Commerce Department encryption export policy announced on September 16 and confirmed in new January 14 regulations (65 Federal Register 2492)
- "Sinister Seven" (Cuba, Iran, Iraq, Libya, North Korea, Syria and Sudan) ("T-7 countries") still off-limits for any exports or reexports of encryption
- Either decontrolled completely (other than "Sinister Seven") if < 64 bit key length or subject to "license exception" ENC if > 64 bit
- Basic license exception ENC rules: After one-time technical review by BXA (approx. 30 days), exporters may ship encryption of any key length to non-governmental end users anywhere in world, other than "Sinister Seven"

Information Security and Encryption (Cont.)

- ENC not applicable for exports of encryption tools with open cryptographic interfaces unless to foreign subsidiary of U.S. exporter
- Users of 3rd party encryption tools must obtain verification of export control status of tools from original vendors prior to export under ENC
- General "deemed export" rule under Export Administration Regulations not applicable to non-U.S. employees who have access to encryption tools as developers or users

Information Security and Encryption (Cont.)

- ISPs and non-U.S. telecommunications companies may receive U.S.-source encryption products per new policy
- New policy recognizes e-commerce applications explicitly: where old policy restricted deployment to "internal use," new rules will permit deployment throughout supply chain and distribution channels
- Modest reporting requirements for exports under ENC (excluding: U.S. sub's, financial tools, TSU products, retail products to individual users, free/anonymous downloads, banks)

Privacy (U.S. and European Rules)

- Growing concern about personal privacy protection in Internet age — data security, data accuracy, data integrity and data sharing
- Radin & Appleman: *"Information in computers never dies."*
- Technology allows unprecedented, unimaginable speed for data collection, retrieval, correlation, storage and transmission through the Internet
- Governments concerned about own internal data, individual citizen data and private databases

Privacy (U.S. and European Rules) (Cont.)

- Profiling: Using collected data on consumer's interests/preferences to infer future purchases
- Predictive Modeling: Using algorithms to find patterns in consumer's past behavior and/or personal data to predict future purchases
- Collaborative Filtering: Using matches of a consumer's past behavior and/or personal data with those of other similar consumers to predict future purchases

Privacy (U.S. and European Rules) (Cont.)

- E-commerce growth and stability depends on business community and general public confidence in "privacy" of data
- Major reason for intensity of industry pressure on encryption decontrol
- *Laissez faire* approach: each e-commerce vendor provide warnings about use, storage and sharing of data and let "user beware"
- Critical factor: is user "aware" and truly informed?
  - e.g., planted "cookies"

Privacy (U.S. and European Rules) (Cont.)

- Original U.S. industry position: private industry standards and self-policing sufficient without government regulation or intervention except for traditional "wire fraud," deception, etc.
- World Wide Web Consortium's "Platform for Privacy" (P3P) for self-enforcement of privacy policies (but clouded by Intermind patent claim)
- "Good Housekeeping" or "Better Business Bureau" stickers, such as TrustE, BBB Online, WebTrust
- Commercial websites posting own privacy policies and commitments

Privacy (U.S. and European Rules) (Cont.)

- Federal Trade Commission: thus far willing to listen to industry but wants tougher corporate "fair information policies" to protect consumer privacy
- Major FTC cases where website operators violated own stated privacy standards: *GeoCities* (August 1998); *Liberty Financial* (April 1999)
- Children's Online Privacy Protection Act of 1998 and new FTC regulations

Privacy (U.S. and European Rules) (Cont.)

- State cases: e.g., Minnesota Attorney General case under Fair Credit Reporting Act against U.S. Bank
- Northwest Airlines on-line ticket purchasing snafu
- RealNetworks' covert data collection and apology
- CD Universe extortion threat and publication of customers' personal credit data

Privacy (U.S. and European Rules) (Cont.)

- United States no longer alone or even dominant in legal systems
- European Union's Directive 95/46 on Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data
- Potential collision regarding data transfers between U.S. and E.U. member countries and also between U.S. and non-E.U. countries who are emulating E.U. Data Privacy Directive 95/46 in own national laws

Privacy (U.S. and European Rules) (Cont.)

- If local privacy law is deemed "inadequate" when compared to E.U. privacy law, then multinational data flow may be disrupted
- New "safe harbors" provision finally negotiated between U.S. Commerce Dept. and E.U.: (1) public notice; (2) choice; (3) 3rd party limits; (4) access; (5) security; (6) integrity; and (7) enforcement and dispute resolution
- E.U. has announced official action in International Court of Justice against France, Luxembourg, The Netherlands and Germany for inadequate data privacy legislation to conform to E.U. Directive

Privacy (U.S. and European Rules) (Cont.)

- "Vendor" cautions:
  - establish a comprehensive company privacy policy which tracks with FTC advice and E.U. Data Privacy Directive
  - educate own staff and other third party participants in supply/distribution chain with access to data about company policy
  - adhere to company policy, internally and externally
  - track data and control third party data access, especially via online Web access points (e.g., extranets, intranets)
  - appreciate and tap IP value of data and databases

Privacy (U.S. and European Rules) (Cont.)

- "User" cautions:
  - before transaction, understand vendor's privacy policy, if any
  - assess reliability and credibility of vendor and vendor policy
  - monitor data provided and seek confirmation, if needed
  - challenge vendor policy or uses of data, if appropriate

Conclusion

- Legal supervision needed for 3rd party content and links, especially through hyperlinks, to corporate websites and e-commerce operations
- Corporate security concerns must become paramount in construction and operation of corporate websites, conduct of e-commerce
- Relaxed encryption export control rules still require corporate compliance measures
- Corporate privacy policies must track new, evolving laws in multi-national regulatory environment