602 Developments in eCommerce Litigation—Hope or Hype?

Vanessa L. Allen
Senior Corporate Counsel
Digex Inc.

Anthony T. Pierce
Partner
Akin, Gump, Strauss, Hauer, & Feld, LLP

Carol A. Romej
Acting General Counsel
Covisint

Faculty Biographies

Vanessa L. Allen

Vanessa L. Allen is senior corporate counsel for Digex, Incorporated, in Beltsville, Maryland, where she a transactional attorney with a concentration in intellectual property law and corporate law.

Prior to coming to Digex, Ms. Allen worked as an attorney for MCI Telecommunications Corporation in the network and facilities group handling a variety of wireless and telecommunications issues, real estate issues, and vendor matters.

Ms. Allen currently resides on the executive advisory board for AbleTV.net, the first global TV network for people with disabilities powered via the worldwide web. She is a member of the ABA subcommittee on information and technology. She also enjoys membership in the Women's Bar Association and Phi Alpha Delta Legal Fraternity. She recently founded a mentoring committee through Fannie Mae and the Black Student Fund for economically disadvantaged students who are attending private schools in the Washington metropolitan area.

Ms. Allen received a BA from Drew University after studying at Oxford University and Central Polytechnic University. She has a JD from American University's Washington College of Law and an MBA from American University's Kogod College of Business.

Anthony T. Pierce

Anthony T. Pierce is a partner of Akin, Gump, Strauss, Hauer & Feld, LLP. Since joining the firm nearly 15 years ago, Mr. Pierce has handled a variety of complex civil and criminal matters in state and federal courts, including securities, lender liability, partnership, employment, and trade secret disputes.

As a member of the firm's technology practice group, Mr. Pierce represents mature and startup technology companies in litigation matters including complex fraud, breach of contract, employee classification, executive compensation, cybersquatting, web-design, and other advertising disputes. His executive compensation work has included jury trials and arbitrations with regard to stock-option awards and independent contractor employee status.

Mr. Pierce serves on the board of trustees of the Legal Aid Society of the District of Columbia and on the U.S. District Court for the District of Columbia's advisory committee on Pro Se Litigation and the Rule 711 counseling panel. He is a member of the board of directors of the Cultural Alliance of Greater Washington. He also serves on the Minority Advisory Board of George Mason University. Mr. Pierce is a member of the District of Columbia and Virginia Bars.

Mr. Pierce received his BS from George Mason University and his JD from the Georgetown University Law Center, where he served as the case and notes editor of the *Georgetown Immigration Law Journal*.

Carol A. Romej
Acting General Counsel
Covisint

DEVELOPMENTS IN E-COMMERCE LITIGATION

By Anthony T. Pierce

Akin, Gump, Strauss, Hauer & Feld, LLP

I. PERSONAL JURISDICTION VIA THE INTERNET

A. TRADITIONAL PRINCIPLES OF PERSONAL JURISDICTION

1. Plaintiffs are not free to sue a defendant wherever they want.
2. There are limits on the power of a state's courts to exercise "personal jurisdiction" over defendants.
3. Jurisdiction over a non-resident defendant must satisfy the forum state's "long arm" statute which typically reaches non-resident defendants in suits involving matters in which the defendants
   a. transact business within a state
   b. commit a tort within the state
   c. commit a tort outside the state but the harmful effects are felt within the state
4. A state's exercise of personal jurisdiction must also comport with constitutional due process under the 14th Amendment.
5. The Supreme Court held that courts of a state may exercise personal jurisdiction over a defendant if he has such "minimum contacts" with the state that it would be fair to require him to defend a lawsuit in that state.
6. Two main prongs of jurisdictional analysis
   a. Purposeful availment of privileges and laws of forum state – defendant must make deliberate choice to relate to the forum state in some meaningful way
   b. Exercise of jurisdiction must comport with traditional notions of fair play and substantial justice

B. MINIMUM CONTACTS

1. At one end of the spectrum, defendant has no contact with the forum state, so court has no authority to exercise personal jurisdiction.
2. Casual, isolated contacts are also insufficient to support jurisdiction.
3. But, single acts may support "specific personal jurisdiction" if the lawsuit arises out of that single act.
4. On the other end of spectrum, are continuos and systematic in-state contacts, so defendant is subject to "general personal jurisdiction", meaning that defendant may be sued in the state for any claim, even one unrelated to its in-state contacts.

C. INTERNET CONTACTS

1. With expanded use and accessibility of the Internet, courts have had to look at the extent to which electronic contacts could establish a defendant's "minimum contacts" within the state.
2. Given the nature of the Internet, a defendant who operates a website that can be viewed around the world, could potentially be subject to suit nationwide.
3. Posting of a web site has presented court with special problems in the traditional personal jurisdiction analysis, because the posting of a web site does not target any specific forum – rather, it is accessible to any Internet user anywhere in the world.
4. In cases in which defendant's contacts with forum state are solely based on defendant's website, courts have looked closely at the website's interactivity.
5. Standards have emerged based on website content and interactivity.
6. There is not one answer as to the question of when Internet contacts are sufficient for the exercise of jurisdiction.

D. ZIPPO'S SLIDING SCALE

1. Zippo Mfg Co. v. Zippo Dot Com, Inc., 925 F. Supp. 1119 (W.D. Pa. 1997) is the seminal case on whether an Internet website provides the minimum contacts necessary to establish jurisdiction.
2. Zippo court found personal jurisdiction based on fact that defendant posted information about its services on its web site and entered into on-line subscription contracts with 3,000 residents of the forum state (Pennsylvania) as well as contracts with Pennsylvania Internet Service Providers
3. Established a sliding scale to determine personal jurisdiction by examining the "level of interactivity and commercial nature of the exchange of information that occurs on the web site."
    a. at one end of the scale, a defendant clearly does business over the Internet by entering into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the internet; here, the Zippo court determined that jurisdiction was proper.
    b. at the other end of the scale, are passive websites that do not allow interaction between the host of the website and a visitor of the site – these site merely provide information to a person visiting the site; passive websites do not conduct business or offer goods for sale; the Zippo court found that passive websites provide insufficient grounds for a court to exercise jurisdiction
    c. in the middle, are interactive websites where a user exchanges information with the host computer; jurisdiction depends on the level of interactivity and commercial nature of the exchange of information

E. EXAMPLES

1. Passive Websites – no jurisdiction found in these cases where the defendant's contacts merely involve the posting of information or advertisements on an Internet website which is accessible to users both within the forum state and beyond.
   a. GTE New Media Services Inc. v. BellSouth Corp., 199 F.3d 1343 (D.C. Cir. 2000) (holding that mere accessibility of website in forum state is insufficient to establish personal jurisdiction where alleged facts did not otherwise support inference of tortious activities directed at the forum).
   b. Cybershell, Inc. v. Cybershell, Inc., 130 F.3d 414 (9th Cir. 1999) (finding that internet advertising alone is insufficient to subject advertiser to jurisdiction).
   c. Mink v. AAAA Dev. LLC, 190 F.3d 333 (5th Cir. 1999) (no jurisdiction where website merely gave product information and contact information).
   d. Bensuasan Restaurant Corp. v. King, 126 F.3d 25 (2d Cir. 1997) (in an infringement claim, declining jurisdiction in New York for the creation of a website providing information about a nightclub in Missouri because defendant's site was not intended to attract business in New York).
   e. ALS Scan Inc. v. Robert Wilkins, et al (No. H-01-496 D. Md.) (finding no personal jurisdiction in Maryland over internet service provider where defendant conducts no business in Maryland and does not receive any proceeds from subscriptions to the website).
2. Commercial Websites – jurisdiction found in these cases where the defendant clearly does business over the Internet with individuals or corporations in the forum state.
   a. American Eyewear, Inc. v. Peepers Sunglasses and Accessories, Inc., 106 F. Supp. 2d 895 (N.D. Tex. 2000) (finding personal jurisdiction proper over

Minnesota eyewear sales company whose website was interactive and where sales to Texas residents occurred daily through the website and typically involved multiple transactions each day).

b. International Star Registry of Illinois v. Bowman-Haight Ventures, Inc., 1999 WL 300285, at *5 (N.D. Ill. May 6, 1999) (in claim that defendant used infringing marks on its website, finding personal jurisdiction over defendant because, even though defendant did not target its business to Illinois specifically, defendant secured an economic benefit from Internet users in Illinois – "the fact that BHV secured an economic benefit from Internet users in Illinois that purchased BHV's goods over the Internet signals that BHV purposefully availed itself of the privilege of conducting activities in Illinois").

3. Interactive Websites – in these cases, the user in the forum state exchanges information with the defendant through the defendant's website, and jurisdiction depends on the level of interactivity and commercial nature of the website.

a. Berthold Types Ltd. v. European Mikrograf Corp., 102 F. Supp. 2d 928 (N.D. Ill. 2000) (no personal jurisdiction over foreign manufacturer of software based on maintenance of a website where orders not taken online but rather on printed out and mailed forms and interaction is limited to submitting suggestions and downloading updates on company activity – though interactive, the website did not provide for direct sales and was not specifically targeted at forum state customers).

b. National Football League v. Miller, 2000 WL 335566, 99 Civ. 11846 (S.D.N.Y. Mar. 30, 2000) (personal jurisdiction proper in New York over a California site operator that provides information about sporting events with links to the official

NFL site, based on NFL's assertion of damage to its image and marketing efforts in New York).

c. Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998) (holding that to satisfy jurisdiction due process minimum contacts test in Internet context, there must be something more than Internet advertisement alone to indicate that defendant purposefully directed his activity in substantial way to the forum state).

d. Inset Sys. v. Instructions Set, Inc., 937 F. Supp. 161 (D. Conn. 1996) (jurisdiction proper over defendant where defendant's only contacts with Connecticut were an Internet web site that had a toll-free number, both of which advertised defendant's services to all states).

e. CompuServe, Inc. v. Patterson, 89 F.3d 1257 (6th Cir. 1996) (finding personal jurisdiction in Ohio proper over an Internet user from Texas who subscribed to a network service based in Ohio because user specifically targeted Ohio by subscribing to the service and entering into an agreement with the service to sell his software over the internet).

4. Can a cyberspace defendant be amenable to suit everywhere its Web page can be seen?

a. In a recent landmark decision, La Ligue Contre Le Racisme Et L'Antisemitisme & L'Union Des Etudiants Juifs De France v. Yahoo!, Inc., a French Court found jurisdiction over Yahoo! to hear a claim that Yahoo! violated a French criminal statute barring the public display in France of Nazi-related artifacts.

1. Because Yahoo! sites were accessible in France, it was not relevant that the Yahoo! servers might be located in the U.S.

2. "the simple act of displaying such objects in France constitutes a

violations of …the Penal Code and therefore a threat to public order."

F. CONCLUSION

1. As a general matter, courts do not take one approach to a personal jurisdiction analysis of Internet defendants.
2. Most courts, however, follow the sliding scale approach established in Zippo
3. The inquiry is always fact intensive.
4. Companies which operate largely on the Web have good reason to foresee being subject to jurisdiction throughout the globe unless they take measures to specifically restrict access from places where they have an desire to avoid being sued.
5. In sum, if a company is clearly doing business over the Internet, entering into contracts with citizens of the forum state, the state's courts will likely exercise personal jurisdiction; if the company has a website that involves interaction between individuals in a state, especially commercial in nature, the website will be classified as interactive and the courts may find jurisdiction; if a website involves no interaction and is merely a passive website or mere advertising on the web, that website is unlikely to give rise to personal jurisdiction.

II. INTERNET DEFAMATION

A. INTRODUCTION

1. The internet is different than most forms of mass communication because anyone with access to the Internet can communicate with a large cyberspace audience.
2. In Reno v. American Civil Liberties Union, 521 U.S. 844, 850 (1997), the Supreme Court opined that "the Internet is a unique and wholly new medium of worldwide human communication."
3. The Internet allows anyone with a phone line to "become a pamphleteer" or "a town

crier with a voice that resonates farther than it could from any soapbox." Id. at 870.

4. The Internet may be the place where Justice Holmes' "marketplace of ideas" could fully be realized – private individuals can now communicate with millions of people with minimal time and money -- dissemination of speech occurs in the touch of a button.
5. Given the different landscape of cyberspace, should traditional legal principles apply? Can cyberspace be regulated by traditional legal principles?
6. Ease of access and anonymity have made the Internet a haven for individuals to post defamatory information.
7. Unique problems arise when applying the tort of defamation to the Internet
   a. each private user becomes more public on the Internet
   b. the internet provides a mass forum for disseminating information in the click of a mouse and a mass forum to rebut allegedly defamatory statements
   c. the internet breeds discussion, debate, opinions
8. "Cyber-reach" – cyberspace's ability to extend the reach of an individual's voice – makes the Internet unique.

B. DEFAMATION LAW

1. Common law actions for slander and libel today fall within the tort of defamation.
2. Prior to 1964, defamation was commonly treated as a strict liability tort, but the Supreme Court gave defamation First Amendment protection in a landmark decision. (New York Times v. Sullivan, 376 U.S. 254 (1964)).
   a. established a minimum constitutional fault standard of "actual malice" in order for a public official to recover on a claim of defamation – the plaintiff can demonstrate actual malice by showing that the defendant proceeded with either

knowledge of falsehood or with reckless disregard of whether a statement was false or not

b. this holding was later extended to public figures

3. When a private individual is defamed, the minimum fault standard is negligence (Gertz v. Welch, 418 U.S. 323 (1974)) (the Court's rationale was that private individuals are more vulnerable to injury because they do not have access to the "channels of effective communication" and cannot counter false statements -- private individuals have not placed themselves in the spotlight, have not assumed the risk of increased exposure or defamatory injury).

C. INTERNET DEFAMATION LITIGATION

1. The laws of defamation apply to false statements made over the Internet – but who is liable?
2. Internet Defamation cases have focused on two different types of defendants: Internet Service Providers ("ISPs") and individuals who posted the message.
3. Early on, litigation focused on the status of ISPs – the question was whether ISPs that enable a third party to post defamatory content about the plaintiff on the internet are to be held liable as publishers of the defamatory statements.
4. under state law, publishers of defamatory statements are usually held liable
   a. distributors (ie. bookstores, libraries) are usually liable only if they knew/had reason to know about the defamatory statements.
   b. Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135, 140 (S.D.N.Y. 1991) was the first major case to address this question; the court held that Compuserve was a distributor rather than a publisher and was not liable for defamatory statements over which it had no editorial control. ("A computerized database is the functional

equivalent of a more traditional news vendor, and the inconsistent application of a lower standard of liability to an electronic news distributor such as CompuServe than that which is applied to a public library, book store, or newsstand would impose an undue burden on the free flow of information.").

5. 1996 – Congress passed the Communications Decency Act – 47 U.S.C. § 230 prohibits ISPs from being treated as publishers, where not the source of the defamatory statements.
   a. Zeran v. AOL, 129 F.3d 327, 330 (4th Cir. 1997); 4th Circuit held that AOL was immune from publisher and distributor liability for defamatory statements initiated by a third party. The statements were posted on AOL's electronic bulletin board. This was the first case to interpret §230 – holding that the CDA was intended to insulate online service providers like AOL from this type of liability. Congress enacted §230 to promote freedom of speech in the "new and burgeoning Internet medium" by eliminating the "threat [of] tort-based lawsuits" against interactive services for injury caused by "the communications of others." Id.
   b. Blumenthal v. Drudge, 992 F.Supp. 44, 50-52 (D.D.C. 1998) ; The court held that AOL was immunized from liability for defamatory statements made in the Drudge Report, an online gossip column, provided by AOL to its subscribers, despite fact that AOL had contracted with and paid Matt Drudge to provide this column. The court held that AOL was not liable in absence of evidence that it had some role in writing or editing material or creating or developing information in the column.
   c. Courts have interpreted § 230 broadly, and have accordingly granted ISPs broad

immunity in defamation litigation; see, e.g. Ben Ezra v. America Online, 206 F.3d 980 (2000) (holding internet service provider immune from liability for defamatory speech initiated by a third party).

d. Due to this immunity, defamation plaintiffs must turn their attention and focus on the individuals who originally post defamatory material; suing these individuals may be a difficult task because of the anonymity of many cyber-defendants.

6. Once lawsuits commence against the originators of the defamatory statements, what is the proper constitutional limit on state defamation liability? If a private individual is defamed on the internet, should the minimum liability standard be actual malice because the rationale of Gertz – that private individuals do not have access to communication channels to counter defamatory speech and have not assumed the risk of defamation – no longer applies in cyberspace where everyone stands on the same ground – private person has ability to rebut an offensive statement to a large audience via the Internet (only limited by ability to reach exact audience of defamatory statement).

7. Some novel 1st Am issues: when an individual criticizes a company in an online message board or chat room – because the individual is usually an anonymous critic, the company's first legal move is to get a subpoena to unmask the identity of the individual -- advocates of the First Amendment argue that this action chills protected speech – this type of litigation is dubbed "John Doe" Litigation – for example, Yahoo! and AOL have been required by subpoena to provide the actual email addresses of individuals who have postings on message boards and chat rooms – then a court order may be used to get the users' personal contract information from their ISPs.

III. CYBERSQUATTING

A. ANTICYBERSQUATTING PROTECTION ACT – 15 U.S.C. § 1125(D)

1. OVERVIEW

   a. The ACPA amended the Lanham Act to expressly provide trademark owners with a civil cause of action against cybersquatters.

   b. A cybersquatter is a person who, with a bad faith intent to profit from a mark, registers, traffics in, or uses a domain name that: is identical or confusingly similar to a distinctive mark; is identical or confusingly similar to or dilutive of that mark; or is a trademark, word or name protected by Section 703 of Title 18.

   c. ACPA provides an inexhaustive list of nine factors that may constitute bad faith, including:

      1. trademark or other intellectual property rights of the person in the domain name;
      2. extent to which domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person;
      3. person's prior use of the domain name in connection with bona fide offering of goods or services;
      4. the person's intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the goodwill represented by the mark
      5. the person's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used . . . the domain name in the bona fide

offering of any goods or services . . .

d. BUT the ACPA contains a Safe Harbor Provision which provides that bad faith intent will not be found in any case in which the court determines that the person believed and had a reasonable grounds to believe that the use of the domain name was a fair use or otherwise lawful.

2. EXAMPLES

a. Sporty's Farm, L.L.C. v. Sportsman's Market, Inc. 202 F.3d 489 (2d Cir. 2000) – In the first appellate consideration of the ACPA, a panel of the Second Circuit affirmed the district court order that the plaintiff (Sporty's Farm) transfer the disputed domain name, "SPORTYS.COM" to the defendant (Sportman's Market). The defendant's "sporty's" mark was protected by the ACPA and that there was sufficient evidence of the plaintiff's bad faith intent to profit.

b. Virtual Works, Inc. v. Volkswagen of America, Inc., 238 F.3d 264 (4th Cir. 2001) – A panel of the Fourth Circuit affirmed the district court's determination that Virtual Works' offer to seel the disputed domain name to Volkswagen, followed by a threat to auction the domain name to the highest bidder constituted evidence of Virtual Works' bad faith intent to profit from registering "VW.NET" which was confusingly similar to Volkswagen's protected mark.

c. FleetBoston Financial Corp. v. FLEETBOSTONFINANCIAL.COM, 138 F. Supp.2d 121 (D. Mass. 2001) – The district court dismissed plaintiff's in rem action

under the ACPA for lack of jurisdiction. Plaintiff urged the court to interpret the in rem provisions of the ACPA to permit a court to exercise jurisdiction in the judicial district where the plaintiff deposited the disputed Registration Certificate, as well as the district in which domain name registry, registrar, or other domain name authority were located. The court found that the plaintiff's interpretation of the ACPA offended traditional notions of fairness and that it had no jurisdiction under 15 U.S.C. 1125(d)(2) to adjudicate the claim.

B. ICANN & THE UDRP -- Internet Corporation For Assigned Names And Numbers And The Uniform Dispute Resolution Policy

1. OVERVIEW
   a. Formed in October 1998, the ICANN is a non-profit, private-sector corporation formed by a broad coalition of the Internet's business, technical, academic, and user communities. ICANN was created by members of the Internet community in response to a June 1998 White Paper issued by the U.S. Department of Commerce.
   b. ICANN has been recognized by the U.S. and other governments as the global consensus entity to coordinate the technical management of the Internet's domain name system, the allocation of IP address space, the assignment of protocol parameters, and the management of the root server system.
   c. All ICANN approved registrars in the .com, .net, and .org top-level domains follow the Uniform Domain-Name Dispute-Resolution Policy (often referred to as the "UDRP").
   d. Under the policy, most types of trademark-based domain-name disputes must be

resolved by agreement, court action, or arbitration before a registrar will cancel, suspend, or transfer a domain name. Disputes alleged to arise from abusive registrations of domain names (for example, cybersquatting) may be addressed by expedited administrative proceedings that the holder of trademark rights initiates by filing a complaint with an approved dispute-resolution service provider.

e. To invoke the policy, a trademark owner should either (a) file a complaint in a court of proper jurisdiction against the domain-name holder (or where appropriate an in-rem action concerning the domain name) or (b) in cases of abusive registration submit a complaint to an approved dispute-resolution service provider --- (*SUCH AS*: CPR Institute for Dispute Resolution, eResolution, The National Arbitration Forum, and World Intellectual Property Organization (WIPO)).

f. The UDRP is mandatory for respondents but not complainants – the complainant can choose whether to file a complaint in court, or to file an administrative action.

g. The benefits to pursuing administrative relief under the UDRP: expeditious resolution; lowers costs. The benefits to pursuing relief under the ACPA through the courts: ACPA is more expansive, provides less protection to cybersquatters; cancellation and transfer are the only remedies available pursuant to the UDRP (no damages).

2. EXAMPLES

a. World Wrestling Federation Entertainment v. Bosman, Case No. D99-0001 – In the first dispute resolved under the UDRP the WIPO Panel ordered the transfer of the "WORLDWRESTLINGFEDERATION.COM" domain name because it was identical or confusingly similar to the trademark in which the complainant had rights and respondent had no rights or legitimate interests in the domain name.

The respondent never made an appearance. The complainant submitted its complaint on December 2, 1999 and the panel reached its decision on January 14, 2000.

b. Raymond Weil S.A. v. Datoo Abbas, Case No. D2001-0597 – The panel was not swayed by the respondent's evidence of his right or legitimate interest in "RAYMONDWEIL.NET" by showing a bona fide offering of goods or services where there was no evidence that respondent's company, Raymonweil Traders, had participated in any trading activity since 1990, respondent failed to mention his company in response to Complainant's cease and desist letter, and explained the name of his company by noting that Mr. Raymond of the New York Times and the French Philosopher Weil were well-renowned in Somalia. The panel found that respondent's explanation "invites a degree of skepticism" and ordered the respondent to transfer the domain name to the complainant. The complaint was filed on April 25, 2001 and the Panel rendered its decision on June 5, 2001.

C. FUTURE ISSUES TO ANTICIPATE

1. Questions Concerning The Authority Of Icann

2. Allocation And Award Of Second Level Domain Names Upon Opening Of New Tld Market.

a. How the new registry operators will manage and distribute trademark domain names, *i.e.*,

SUNRISE PERIOD – by .info's registry operator, Alias provides an exclusive period of time for trademark and service mark holders to make reservations and preserve their marks during the roll-out of the new TLDs. *Problem:* Allegations of fraud registrations taking advantage of the .info

"sunrise period" - misrepresenting themselves as trademark holders in order to register .info Internet addresses before the general public gets a shot at the .info registry.

b. How the new registry operators will allocate domain names to competing parties. First in time?

3. Resolution of international trademark issues.

4. Proposed protocol that will allow the DNS to look at a name entered in a language other than English and translate it into the correct numeric internet address. Continuing concerns that because the current system is based on English, U.S. companies can - and do - unfairly dominate the internet

5. Who is privacy issues for domain name registration

Contracts in Cyberspace

American Corporate Counsel Association
October 17, 2001; Section 602

By Carol Romej
Butzel Long, Detroit

1. Contract Delivery Methods

A. A Variety of Communication tools

1. EDI

2. Facsimile

3. Website Order Forms

4. E-Mail exchange

5. Click-Wrap (I accept)

2. Electronic Transaction Primer

A. E-Commerce Security Technologies

1. Passwords

2. Tokens/Memory Cards

3. Smart Cards

4. Biometrics

5. Encryption

B. Digital Signatures – an electronic substitute for a handwritten signature; a randomized identifier that is unique to each individual.

C. Electronic Signatures – refers to any method that represents assent and acknowledgement, or an authentication of an electronic record. Under the eSign act,

defined as an electronic sound, symbol, or process attached to or logically associated with a contract or other record.

D. Certification Authorities – an entity that serves as a trusted third party, and verifies the identity of a subscriber, and then issued certification.

E. Digital Certificates – typically contains the name of the holder, the holder's public key, the name of the CA, a serial number, the validity period of the certificate, and the digital signature of the CA.

F. Technology At Work

1. Example – Verisign ServerID Product

3. Case Developments

A. Clickwrap Agreements – license terms or website visitation terms that are presented on the users screen with "I Agree/Decline" buttons following the terms.

1. Hotmail Corporation v. Van$ Money Pie where Hotmail won a preliminary injunction against Van$ Money Pie as the court determined that Hotmail would likely prevail in its breach of (online) contract claim.

2. Caspi v. The Microsoft Network, L.L.C., 732 A.2d 528 (1999) where the court refused to invalidate the online forum selection clause.

B. Shrinkwrap Agreements – contracts wrapped with the computer program product (CD/Diskette).

1. ProCD, Inc. v. Zeidenberg, 86 F. 3d 1447 (1996) found a buyer accepts a license agreement by using the software; A vendor may invite acceptance by conduct; Shrinkwrap licenses are enforceable.

2. Hill v. Gateway2000, Inc., 105 F.3d 1147 (1997) established that people who accept (a contract in the box that the computer was delivered) take the risk that the unread terms may in retrospect prove unwelcome.

C. Downloading ≠ Contract Formation

1. Specht v. Netscape Communications Corp., 150 F. Supp. 2d 585 (2001) where the mere act of downloading the software was not sufficient to indicate the users assent to the license agreement; users did not have to view the license agreement to download the software.

4. Developments - Codified

A. eSign Act (15 U.S.C.A. 7001-7031)

1. Purpose – to facilitate use of electronic records and signatures

2. Authorizes legally enforceable electronic signatures, contracts, records

3. Exempts – wills, codicils, trusts, adoption or divorce matters…

B. UETA – The Uniform Electronic Transactions Act

1. Purpose to facilitate commerce and governmental transactions by validating and authorizing the use of electronic records and signatures

2. Where parties agree to conduct business by electronic means

3. The electronic medium in which a record, signature or contract is created, presented or retained does not deny its legal effect.

C. UCITA – Uniform Computer Information Transaction Act

1. Scope - Limited to Computer Information Transactions

2. Provisions facilitate E-Commerce

3. Supplements consumer laws

4. Drafting Tips

A. Presentation and location of Links (Terms, Legal, Copyright) - conspicuous

B. Terms that are fair and reasonable

C. Do not allow services or product to be purchased without receiving users assent – "I Accept" click

D. Have user warrant that he is authorized to act on behalf of an entity he seeks to bind.

5. Comments on Privacy and Security

ACCA's 2001 Annual Meeting - October 17, 2001
"Session 602 – Developments in eCommerce Litigation" Outline

Vanessa L. Allen[1], Senior Corporate Counsel, Digex, Incorporated

INTRODUCTION

With the proliferation in the use of the Internet and technology as a mission critical business necessity, e-commerce litigation has taken a pre-eminent role in defining our relationships and contractual rights. Many of the issues that arise from e-commerce litigation are unique not only to contract and intellectual property law but also to insurance law and litigation. These issues require new analysis, new drafting requirements and new application of legal theories.

This outline and presentation will address some of the manners in which in-house counsel and business people can mitigate their exposure to, and the costs of, litigation. Your clients can implement policies and procedures that may make the initiation and defense of litigation easier. Moreover, there are preventative steps that your clients can follow to prevent the amount of damages that they pay, including the purchase of new forms of Internet-related insurance.

[1] Vanessa L. Allen is Senior Corporate Counsel at Digex, Incorporated in Beltsville, Maryland. The views expressed in this presentation, however, are those of Ms. Allen and are in no way meant to be attributed to Digex, its parent company or any of its affiliates.

Many of the preventative measures implemented by your client will be critical to any insurance audit or request for additional types of coverage. Traditional insurance coverage has several drawbacks when applied to e-commerce business and liability issues. Prior to the special uses and requirements of businesses who utilized the Internet, property was defined as tangible property only and business interruption was tailored to fire, flood and other natural disasters to physical property. Your client may wish to revise its insurance policies to complement the rapidly changing terrain of e-commerce litigation. Court decisions have not fully addressed whether e-commerce-based losses are covered by standard commercial property insurance policies. Year 2000 litigation and subsequent litigation regarding insurance coverage for loss of computer data under standard commercial policies is still ambiguous. Insurers and insureds may find themselves litigating to determine the extent to which traditional policies can be interpreted to cover e-commerce losses.

OUTLINE

I. Litigation – E-Commerce Related Discovery

A. Prior to Litigation – An In-house Perspective

1. Data Storage and Management

2. Data Retention Policy

Lewy v. Remington Arms Co., 836 F.2d 1104 (8th Cir. 1988)

Stanton v. Nat'l R.R. Passenger Corp., 849 F.Supp. 1524 (M.D. Ala. 1994)

3. Staff Responsible for Data Management
   a. GTFM, Inc. v. Wal-Mart Stores Inc., 2000 WL 335558 (S.D.N.Y. 2000)
   b. Linnen v. A.H. Robins Company, Inc., et al. 1999 WL 462015 (Mass.Super.)
4. Systems' Contents and Capabilities
   a. Retrieving the data
   b. Storing and Sorting the data
5. Employee Concerns
   a. Use of company's computers and email, including Internet access[2]
   b. Tele-commuters

B. During Litigation
   1. Communication between in-house counsel and outside counsel[3]
   2. Discovery Requests and Responses

[2] User warnings should remind employees and other users that unauthorized access to confidential information and unauthorized disclosure and transmission of confidential information is punishable by termination of employment, civil penalties and criminal penalties.

[3] One should give special security and risk management analysis to software applications that enable outside counsel or third parties to access any corporate department's database by way of the Internet. There are two notable approaches to less secure Remote-Access software, but there are various software and hardware products that can provide secure connections, encryption of data, password protection, and secure electronic mail transmissions to further protect confidential information that needs to be transmitted via electronic means. Remote access control allows you dial up your personal computer directly at the office and operate it remotely as if you were actually in the office. Although you must remain on a phone line, you do not have to duplicate files on your home computer. On the other hand, File Transfer Protocol allows you to access documents stored on your office computers and downloads them to a computer at home/other location in order to edit documents using duplicates of the relevant programs. Using FTP, you would simply upload (i.e. transfer back) completed documents to your office computer without using a modem or accumulating.

C. Post-Litigation

1. Lessons Learned
2. Policy Implementation with Client's management and with outside counsel, if necessary (e.g. privacy, email or security policies)
3. Re-Evaluation of Insurance Coverage

II. Insurance Coverage

A. Pre-requisites

1. What are your client's risks?
   - Product – shipping, specifications
   - Financial – Electronic payment, credit
   - Media – Online content, defamation
   - Identity – Privacy, Data Protection, Authentication
   - Professional - Internet Errors & Omissions; Directors & Officers
   - Security – Hacks, Denial of Service Attacks[4], Ddos[5]
2. What is your client's traditional insurance coverage? Is additional coverage required for its e-commerce/online exposure?
3. What is the process for obtaining e-commerce insurance?

[4] Denial of Service attacks use a single computer to attack another single computer. One party (ie. a customer) sends a ping requesting technical information but the return IP address is a spoof so the computer continues to respond to an address with no information. The loop is continuous and therefore the computer becomes "stalled."

[5] Distributed denial of service attacks occur when someone uses many computers to attack by installing a "slave" or "zombie" program on other computers and remotely control those programs.

Stand-alone policies require a different underwriting process, which includes allowing insurance companies to audit your client's IT or security systems. Certifications granted by third party auditors (e.g. SAS70 security certification) to your client make the underwriting process easier.

4. Is computer data tangible property, covered by insurance? Can computer data be subject to physical loss and damage?
   - Home Indemnity Co. v. Hyplains Beef, L.C. 893 F.Supp. 987 (D. Kan. 1995), aff'd without opinion 89 F.3d 859 (10th Cir. 1996) – Is computer data capable of physical damage?
   - Magnetic Data, Inc. v. St. Paul Fire & Marine Insurance Co., 442 NW.2d 153 (Minn. 1989) – Erased computer data barred under a control of property exclusion because it was under the control of the insured at the time of loss; thus, the status of computer data as tangible or intangible was not fully addressed
   - Retail Systems, Inc. v. CNA Insurance Cos., 469 NW.2d. 735 (Minn. App. 1991) – Computer data on a tape is merged with the physical tape and therefore, if the tape is lost, a loss of tangible property results; however, the data itself was not characterized as tangible property
   - St. Paul Fire & Marine Insurance Co.v. National Computer Systems, Inc., 490 NW.2d. 626 (Minn. App. 1992) – Court

used Retail Systems and Magnetic Data to hold that loss of an insured's pricing data was not a loss of tangible property because the binders in which the information were stored were not lost or damaged and the information was still usuable. The court argued that the real issue was a loss of exclusive use of pricing information rather than a loss of the information entirely. Therefore, no commercial general liability coverage was available because there was no loss of tangible property only damage to the competitor's right to use the property.

5. What do your client's contracts say about liability and insurance?
6. Is there an opportunity to maximize Parent Company and Affiliate Coverage?

B. Traditional Forms
   1. Comprehensive General Liability
   2. Business Interruption
   3. Property Damage
   4. Errors and Omissions/ Directors and Officers
   5. K & R (Kidnap and Ransom)

C. Supplements to Traditional Forms
   1. Reasons to Supplement
      a. Guard against loss of revenue – unavailability of websites and/or networks to generate revenue

b. Rebuild or prevent loss of reputation – damaged reputation due to hacks, outages or unavailability

c. Guard against loss of additional assets

d. Cover stolen trade secrets, patents and business data – hackers and disgruntled employees may steal customer lists, intellectual property, marketing or financial data

e. Cover defamation and copyright infringement claims - Electronic Publishing Liability

f. Guard against network liability

2. Supplemental Policies

a. Property Loss for Intangible Assets – Intellectual Property

b. Cyber-Extortion – Coverage for paying for a private investigator and/or ransom demands

c. Professional Services Liability – Coverage for failure to perform professional service, negligence and error/omission in professional service

d. Network and Security Liability – Coverage for third party liability claims; Cover for first party claims

D. Litigation Issues

1. Do commercial property policies, un-amended, provide coverage for denial of service attacks and other loss of use or impairment of use losses?

2. Will commercial property insurers extend legal liability coverage to the insured's liability for financial injury caused by the use of information of others that had been in the insured's care, custody or control but that was stolen?

3. The Future

   - American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc., 200 U.S. Dist. LEXIS 7299 (D.Ariz. Apr. 18, 2000) – When computer data is stored in a computer and then altered, the computer has suffered "physical loss or damage" rather than the data; thus, under the business interruption policy, loss of computer data was physical damage to the insured's computer equipment. Physical destruction may not be limited to physical destruction of computer equipment and can include loss of functionality and loss of use.

E. International Issues – Check with your insurer about limitations in other countries (For example, Europe and England have refused to include computer virus coverage in reinsurance policies)

III. Questions and War Stories

SAMPLE CONTRACT PROVISIONS & INSURANCE OFFERINGS

A. SAMPLE CONTRACT INSURANCE PROVISIONS

(A) During any time period when customer is provided physical access to any facilities, hardware or other property owned or leased by, or otherwise under the control of, vendor (collectively, "Vendor Property") pursuant to this Agreement, customer shall (i) maintain insurance in reasonable amounts covering any damage or destruction to Vendor Property (collectively, "Damage") and (ii) reimburse Vendor for all expenses incurred by Vendor in replacing or repairing, as the case may be, any Damage caused by customer.

(B) Consultant will obtain and maintain, during the term of this Agreement and any Service Order, insurance of the kinds and in the minimum amounts specified below, or in amounts required by law, whichever is greater. Client may require, and Consultant will furnish, certificates of insurance evidencing such coverage and naming Client as an additional named insured. Client may terminate this Agreement or any Service Order without further notice in the event Consultant fails to provide such certificates within thirty (30) days of the date requested.

A. Worker's Compensation Insurance affording protection in accordance with the Worker's Compensation Law of the State(s) in which the services are to be performed.

B. Comprehensive General Liability Insurance in amounts not less than $1,000,000 per occurrence with an annual aggregate of $1,000,000 for bodily injury and $1,000,000 for property damage. Such insurance must include coverage for liability assumed under this Agreement or any Service Order, completed operations coverage and damage to the property of others in the care, custody or control of the insured.

C. Comprehensive Automobile Liability Insurance in amounts not less than $1,000,000 per occurrence with an annual aggregate of $1,000,000 for bodily injury and $1,000,000 for property damage.

B. SAMPLE CONFIDENTIALITY AGREEMENT

This Agreement, made as of the date of the later signature below (the "Effective Date"), by and between _____, having a place of business at _____ ("), and _____, ("Company"), sets forth the terms and conditions of the confidential disclosure of certain information between the parties. The party from time to time disclosing Confidential Information, as herein defined, shall be referred to as the "Discloser" and the party from time to time receiving such Confidential Information, as herein defined, shall be referred to as the "Recipient." The term "Confidential Information" shall refer to the Confidential Information disclosed by either party, as the case may be.

1. "Confidential Information" shall mean the information described at the end of this Agreement, which is disclosed to Recipient by Discloser in any manner, whether orally, visually or in tangible form (including, without limitation, documents, devices and computer readable media) and all copies thereof. Tangible materials that disclose or embody Confidential Information shall be marked by Discloser as "Confidential," "Proprietary" or the substantial equivalent thereof. Confidential Information that is disclosed orally or visually shall be identified by Discloser as confidential at the time of disclosure and reduced to a written summary by Discloser, who shall mark such summary as "Confidential," "Proprietary" or the substantial equivalent thereof and deliver it to Recipient by the end of the month following the month in which disclosure occurs. Recipient shall treat such oral or visual information as Discloser's Confidential Information pending receipt of such summary.

2. Except as expressly permitted herein, for a period of three (3) years from the Effective Date (the "Nondisclosure Period"), Recipient shall maintain in confidence and not disclose Confidential Information.

3. Recipient shall have the right to use Confidential Information solely for the purpose of _____ _____ ____ (the "Permitted Purposes").

4. Recipient shall disclose Confidential Information only to those of its employees who reasonably require such information for the Permitted Purpose.

5. Confidential Information shall not include any information that Recipient can demonstrate:
   a. Was in Recipient's possession without confidentiality restriction prior to disclosure thereof by Discloser hereunder;
   b. Was generally known in the trade or business in which Discloser is involved at the time of disclosure to Recipient hereunder, or becomes so generally known after such disclosure, through no act of Recipient;
   c. Has come into the possession of Recipient without confidentiality restriction from a third party and such third party is under no obligation to Discloser to maintain the confidentiality of such information; or
   d. Was developed by Recipient independently of and without reference to Confidential Information. If a particular portion or aspect of Confidential Information becomes subject to any of the foregoing exceptions, all other portions or aspects of such information shall remain subject to all of the provisions of this Agreement.

6. Recipient agrees not to reproduce or copy by any means Confidential Information, except as reasonably required to accomplish Recipient's Permitted Purpose. Upon termination of this Agreement, Recipient's right to use Confidential Information, as granted in paragraph 3 above, shall immediately terminate. In addition, upon demand by Discloser at any time, Recipient shall return promptly to Discloser or destroy, at Discloser's option, all tangible materials that disclose or embody Confidential Information.

7. Recipient shall not remove any proprietary rights legend from, and shall, upon Discloser's reasonable request, add any proprietary rights legend to, materials disclosing or embodying Confidential Information.

8. In the event that Recipient is ordered to disclose Discloser's Confidential Information pursuant to a judicial or governmental request, requirement or order, Recipient shall promptly notify Discloser and take reasonable steps to assist Discloser in contesting such request, requirement or order or otherwise in protecting Discloser's rights prior to disclosure of Confidential Information.

9. Discloser understands that Recipient develops and acquires technology for its own products, and that existing or planned technology independently developed or acquired by Recipient may contain ideas and concepts similar or identical to those contained in Discloser's Confidential Information. Discloser agrees that entering into this Agreement shall not preclude Recipient from developing or acquiring technology similar to Discloser's, without obligation to Discloser, provided Recipient does not use the Confidential Information to develop such technology.

10. Other than as expressly specified herein, Discloser grants no licenses or other rights to Recipient, at the expense of Discloser to use or reproduce Confidential Information.

11. This Agreement and all actions related hereto shall be governed by the laws of the State of Maryland, excluding its choice of law principles.

12. This Agreement expresses the entire agreement and understanding of the parties with respect to the subject matter hereof and supersedes all prior oral or written agreements, commitments and understandings pertaining to the subject matter hereof. Any modifications of or changes to this Agreement shall be in writing and signed by both parties hereto.

13. Unless earlier terminated in accordance with the provisions hereof, this Agreement shall remain in full force and effect for the duration of the Nondisclosure Period, whereupon it shall expire. Either party may terminate this Agreement at anytime, without cause, effective immediately upon written notice of termination. In the event this Agreement is terminated, its provisions shall survive, for the Nondisclosure Period, with respect to Confidential Information disclosed prior to the effective date of termination. Any causes of action accrued on or before such expiration or termination shall survive until the expiration of the applicable statute of limitations.

Confidential Information

"Confidential Information" shall include trade secrets, computer software, source code, object code, data, flow charts, inventions, experiments, developments, equipment, prototypes, computer hardware, drawings, blueprints, manufacturing procedures, test procedures, business activities and plans, financial information, Company lists, operational methods, marketing strategies, sales information, and other information relating to the business or prospects of Discloser of any nature whatsoever, whether in intangible or tangible form.

Contacts

A. Company designates the following individual(s) as its contact(s) for receipt of Confidential Information:

_____

_____

B. ___designates the following individual(s) as its contact(s) for receipt of Confidential Information:

C. Each party reserves the right to change their contact(s), and will endeavor to notify the other party in such event.

By:	_____	**By:**	_____
Name:	_____	**Name:**	_____
Title:	_____	**Title:**	_____
Date:	_____	**Date:**	_____

C. SAMPLE INSURANCE COVERAGE

First Party Coverage

I. Network Extortion – Money and/or goods surrendered by or on behalf of the insured to meet an extortion demand

- Due to the introduction of a virus/disabling device to corrupt or destroy information
- Due to the disclosure of information on the insured's computer network

II. Loss of Funds or Property – Funds transfer, payment or delivery of funds or property, established any credit, debited any account or given value

- Due to the fraudulent input of information into a processing or communications system
- Due to the fraudulent modification or fraudulent destruction of information or during the transmission to the insured's processing system
- Due to the fraudulent preparation or modification of a computer program
- Due to a virus

III. Loss, Damage and Destruction of Information – Destruction, damage or loss of information by reason of

- Robbery, burglary, larceny, theft, misplacement, mysterious unexplainable disappearance or malicious act
- Malicious alteration or malicious destruction
- Any accidental alteration or destruction
- Malicious copying, malicious recording, or malicious sending of information which would constitute a trade secret
- A virus

IV. Business Interruption and Extra Expense – A business interruption loss due to

- A virus
- Malicious alteration or malicious destruction of information
- Malicious alteration or malicious destruction of computer programs
- Lost, damaged or destroyed electronic record as a result of robbery, burglary, larceny, theft, misplacement, mysterious unexplainable disappearance or malicious act
- Accidental alteration or accidental destruction of information
- Illegitimate use
- Denial of service

Third Party Coverage

V. Multimedia or Intellectual Property – A breach of duty, negligent act, error or omission causing actual or alleged loss due to

- Libel, defamation, disparagement or slander
- Invasion of privacy or breach of confidentiality
- Infringement of copyright, title, trademark or trade name
- Plagiarism
- False Advertising
- Patent

VI. Breach of Security – The liability due to a third party loss arising from the failure of the insured's computer(s) or computer network to prevent

- Denial of service attack
- Virus introduction

- Theft of data
- Unauthorized access
- Destruction or corruption of data

VII. Hosting – A breach of duty, negligent act, error or omission causing actual or alleged loss resulting from

- Web hosting activities
- Conduct of e-Commerce

Miscellaneous Coverage

VIII. Public relations expense – Reasonable expenses incurred by the insured to re-establish the reputation and market share of the insured subsequent to the loss

IX. Defense expenses – Necessary and reasonable legal fees and expenses incurred by the insured in defending a claim from a covered event.

Common e-Business Exclusions

1. Any prior acts which you were aware of or should have been aware as of the beginning of the policy period;
2. Any actual or alleged violation of the Employee Retirement Income Security Act of 1974;
3. Any actual or alleged violation of the Racketeer Influenced Corrupt Organization Act;
4. Any actual or alleged violation of any state or federal securities, antitrust or unfair trade practices;
5. Any action or proceeding brought or maintained by or on behalf of any governmental or quai-governmental regulatory agency or authority, including the seizure, confiscation, nationalization or destruction of information assets by order of any governmental or public authority;
6. Any actual or alleged violation of your employment practices liability;

7. Your assumption of any liability under any contract or agreement;
8. Any act of war;
9. Any act of God, fire, smoke, explosion, lightning, wind, flood, earthquake, volcanic eruption, tidal wave, landslide or hail;
10. The interruption or failure, howsoever caused, of any component of the Internet or of any infrastructure supporting the Internet, unless such component or infrastructure was under your direct control, or of any power or other utility service;
11. Any dishonest, fraudulent, malicious or criminal act committed by you or your board of directors;
12. Any dishonest, fraudulent, malicious or criminal act committed by any of your director, officers or employees or independent contractors, if such act occurs after you (or any of your directors or officers not in collusion with such director, officer, employee or independent contractor) learn of any other fraudulent, dishonest or criminal act previously committed by such director, officer, employee or contractor;
13. Any actual or alleged bodily injury, sickness, mental anguish, emotional distress, disease or death of any person;
14. Any actual or alleged over-redemption of coupons, awards, or prizes from advertisements, promotions, games, sweepstakes and contests;
15. Any physical property damage, including normal wear and tear or gradual deterioration of your information assets;
16. Your actual or alleged misuse or unauthorized release of, or failure to safeguard the confidentiality of or otherwise prevent from disclosure, any information or data, acquired or developed by you as a result of your e-business activities;

17. Costs of upgrading, updating, maintaining, improving or remedying our covered systems or software programs;
18. Any actual or alleged breach of any warranty, express or implied, of fitness or suitability;
19. Any actual or alleged infringement of any patent or trade secrets;
20. Any satellite interruption or failure;
21. Any actual, alleged or threatened exposure to or generation, transportation, discharge, emission, dispersal, release, escape, treatment, storage, removal or disposal of any pollutants;
22. Any claim against an insured that is brought by or on behalf of another insured or any business entity that is owned, managed or operated, directly or indirectly, by an insured;
23. Any claim based upon or arising out of the inaccurate, inadequate, or incomplete description of the price of goods, products or services or failure of goods, products or services to conform with an advertised quality or performance.

Developments In E-Commerce Litigation

By Anthony T. Pierce

Dtp10786

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Personal Jurisdiction Via The Internet

- **Traditional Principles of Personal Jurisdiction**
  - Plaintiffs are not free to sue a defendant wherever they want.
  - There are limits on the power of a state's courts to exercise personal jurisdiction over defendants.
  - Jurisdiction over a non-resident defendant must satisfy the forum state's "long arm" statute:
    - Transact business within a state
    - Commit a tort within the state
    - Commit a tort outside the state but the harmful effects are felt within the state.

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Personal Jurisdiction Via The Internet

- **Traditional Principles of Personal Jurisdiction**
  - Constitutional due process under the 14th Amendment.
  - "Minimum contacts" test.
  - Two main prongs of jurisdictional analysis:
    - Purposeful availment of privileges and laws of forum state
    - Fair play and substantial justice.

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Personal Jurisdiction Via The Internet

Minimum Contacts

Defendant has no contact with the forum state	Casual, isolated contacts	Continuous and systematic in-state contacts
↓	↓	↓
Court has no authority to exercise personal jurisdiction.	Insufficient to support jurisdiction.	Defendant is subject to "general personal jurisdiction."

But, single acts may support "specific personal jurisdiction" if the lawsuit arises out of that single act.

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Personal Jurisdiction Via The Internet

- **Internet Contacts**
  - With expanded use and accessibility of the Internet, courts have had to look at the extent to which electronic contacts could establish a defendant's "minimum contacts" within the state.
  - A defendant who operates a website that can be viewed around the world could potentially be subject to suit nationwide.
  - Posting of a website – special problems in the traditional personal jurisdiction analysis.

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Personal Jurisdiction Via The Internet

- **Internet Contacts**
  - If defendant's contacts with forum state are solely based on defendant's website, courts look at the website's interactivity.
  - Standards have emerged based on website content and interactivity.
  - No one answer to the question of when Internet contacts are sufficient for the exercise of jurisdiction.

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Personal Jurisdiction Via The Internet

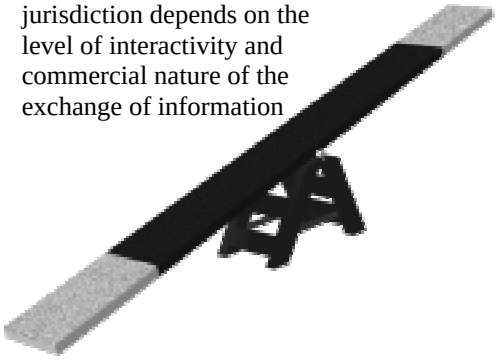
- ***Zippo's* Sliding Scale**
  - *Zippo Mfg Co. v. Zippo Dot Com, Inc.*, 925 F. Supp. 1119 (W.D. Pa. 1997)
    - Personal jurisdiction — defendant posted information about its services on its website and entered into on-line subscription contracts with residents of the forum state as well as contracts with state ISPs.
    - Sliding scale → examine the "level of interactivity and commercial nature of the exchange of information that occurs on the web site."

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Personal Jurisdiction Via The Internet

Interactive websites where a user exchanges information with the host computer → jurisdiction depends on the level of interactivity and commercial nature of the exchange of information

Passive websites → no jurisdiction



Defendant clearly does business over the Internet by entering into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet → jurisdiction

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Examples

- **Passive Websites – no jurisdiction.**
  - *GTE New Media Services Inc. v. BellSouth Corp.*, 199 F.3d 1343 (D.C. Cir. 2000) (mere accessibility of website in forum state is insufficient to establish personal jurisdiction where alleged facts did not otherwise support inference of tortious activities directed at the forum).
  - *Cybershell, Inc. v. Cybershell, Inc.*, 130 F.3d 414 (9th Cir. 1999) (Internet advertising alone is insufficient to subject advertiser to jurisdiction).
  - *Mink v. AAAA Dev. LLC*, 190 F.3d 333 (5th Cir. 1999) (no jurisdiction where website merely gave product information and contact information).

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Examples

- **Passive Websites – no jurisdiction.**
  - *Bensuasan Restaurant Corp. v. King*, 126 F.3d 25 (2d Cir. 1997) (in an infringement claim, declining jurisdiction in New York for the creation of a website providing information about a nightclub in Missouri because defendant's site was not intended to attract business in New York).
  - *ALS Scan Inc. v. Robert Wilkins, et al.* (142 F. Supp. 2d 703 (D. Md. 2001) (no personal jurisdiction in Maryland over Internet service provider where defendant conducts no business in Maryland and does not receive any proceeds from subscriptions to the website).

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Examples

- **Commercial Websites – jurisdiction found.**
  - *American Eyewear, Inc. v. Peepers Sunglasses and Accessories, Inc.*, 106 F. Supp. 2d 895 (N.D. Tex. 2000) (personal jurisdiction over Minnesota eyewear sales company whose website was interactive and where sales to Texas residents occurred daily through the website and typically involved multiple transactions each day).
  - *International Star Registry of Illinois v. Bowman-Haight Ventures, Inc.*, 1999 WL 300285, at *5 (N.D. Ill. May 6, 1999) (personal jurisdiction over defendant because, even though defendant did not target its business to Illinois specifically, defendant secured an economic benefit from Internet users in Illinois).

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Examples

- **Interactive Websites – jurisdiction depends on the level of interactivity and commercial nature of the website**.
  - *Berthold Types Ltd. v. European Mikrograf Corp.*, 102 F. Supp. 2d 928 (N.D. Ill. 2000) (no personal jurisdiction over foreign manufacturer of software based on maintenance of a website – though interactive, the website did not provide for direct sales and was not specifically targeted at forum state customers).

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Examples

- **Interactive Websites – jurisdiction depends on the level of interactivity and commercial nature of the website.**
  - *National Football League v. Miller*, 2000 WL 335566 (S.D.N.Y. Mar. 30, 2000) (personal jurisdiction proper in New York over a California site operator that provides information about sporting events with links to the official NFL site, based on NFL's assertion of damage to its image and marketing efforts in New York).

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Examples

- **Interactive Websites – jurisdiction depends on the level of interactivity and commercial nature of the website.**
  - *Blumenthal v. Drudge*, 992 F. Supp. 44 (D.D.C. 1998) (to satisfy jurisdiction due process minimum contacts test in Internet context, there must be something more than Internet advertisement alone to indicate that defendant purposefully directed his activity in substantial way to the forum state).

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Examples

- **Interactive Websites – jurisdiction depends on the level of interactivity and commercial nature of the website**.
  - *Inset Sys. v. Instructions Set, Inc.*, 937 F. Supp. 161 (D. Conn. 1996) (jurisdiction proper over defendant where defendant's only contacts with Connecticut were an Internet website that had a toll-free number, both of which advertised defendant's services to all states).

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Examples

- **Interactive Websites – jurisdiction depends on the level of interactivity and commercial nature of the website.**
  - *CompuServe, Inc. v. Patterson*, 89 F.3d 1257 (6th Cir. 1996) (personal jurisdiction in Ohio proper over an Internet user from Texas who subscribed to a network service based in Ohio because user specifically targeted Ohio by subscribing to the service and entering into an agreement with the service to sell his software over the Internet).

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Examples

- **Can a cyberspace defendant be amenable to suit everywhere its Web page can be seen?**
  - *La Ligue Contre Le Racisme Et L'Antisemitisme and L'Union Des Etudiants Juifs De France v. Yahoo!, Inc.*, a French Court found jurisdiction over Yahoo! to hear a claim that Yahoo! violated a French criminal statute barring the public display in France of Nazi-related artifacts.

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Conclusion

- As a general matter, courts do not take one approach to a personal jurisdiction analysis of Internet defendants.
- Most courts follow the sliding scale approach established in *Zippo*.
- The inquiry is always fact intensive.
- Companies which operate largely on the Web should foresee being subject to jurisdiction throughout the globe unless they take appropriate measures.

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Conclusion

- **In sum:**
  - ***Jurisdiction likely*** if a company is clearly doing business over the Internet, entering into contracts with citizens of the forum state.
  - ***May be jurisdiction*** if the company has a website that involves interaction between individuals in a state, especially commercial in nature.
  - ***Jurisdiction unlikely*** if a website involves no interaction and is merely a passive website or mere advertising on the web.

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Internet Defamation

- **Introduction**
  - Internet can communicate with a large cyberspace audience.
  - *Reno v. American Civil Liberties Union*, 521 U.S. 844, 850 (1997) – "the Internet is a unique and wholly new medium of worldwide human communication." The Internet allows anyone with a phone line to "become a pamphleteer" or "a town crier with a voice that resonates farther than it could from any soapbox." *Id.* at 870.
  - "Marketplace of ideas" – dissemination of speech occurs in the touch of a button.

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Internet Defamation

- **Introduction**
  - Given the different landscape of cyberspace, should traditional legal principles apply?
  - Ease of access and anonymity.
  - Unique problems arise when applying the tort of defamation to the Internet:
    - Each private user becomes more public on the Internet
    - The Internet provides a mass forum for disseminating information in the click of a mouse
    - The Internet breeds discussion, debate, opinions
  - "Cyber-reach" – cyberspace's ability to extend the reach of an individual's voice.

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Internet Defamation

- **Defamation Law**
  - Defamation: slander and libel.
  - *New York Times v. Sullivan*, 376 U.S. 254 (1964) – gave defamation First Amendment protection.
    - ***"Actual malice"*** required for a public official to recover on a claim of defamation
    - This holding was later extended to public figures
  - ***Negligence*** required for private individuals (*Gertz v. Welch*, 418 U.S. 323 (1974)).

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Internet Defamation

- **Internet Defamation Litigation**
  - The laws of defamation apply to false statements made over the Internet – but who is liable?
  - Internet Defamation cases have focused on two different types of defendants: ISPs and individuals who posted the message.
  - Status of ISPs – whether ISPs that enable a third party to post defamatory content about the plaintiff on the Internet can be liable as publishers of the defamatory statements.

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Internet Defamation

- **Internet Defamation Litigation**
  - Under state law, publishers of defamatory statements are usually held liable.
    - Distributors (i.e. bookstores, libraries) are usually liable only if they knew/had reason to know about the defamatory statements.
    - *Cubby, Inc. v. CompuServe, Inc.*, 776 F. Supp. 135, 140 (S.D.N.Y. 1991) – Held Compuserve was a distributor rather than a publisher and was not liable for defamatory statements over which it had no editorial control.

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Internet Defamation

- **Internet Defamation Litigation**
  - *Zeran v. AOL*, 129 F.3d 327, 330 (4th Cir. 1997) – AOL was immune from publisher and distributor liability for defamatory statements initiated by a third party.

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Internet Defamation

- **Internet Defamation Litigation**
  - *Blumenthal v. Drudge*, 992 F. Supp. 44, 50-52 (D.D.C. 1998) – AOL was immunized from liability for defamatory statements made in the Drudge Report, an online gossip column, provided by AOL to its subscribers, despite fact that AOL had contracted with and paid Matt Drudge to provide this column.

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Internet Defamation

- **Internet Defamation Litigation**
  - Courts have interpreted § 230 of the Communications Decency Act broadly, and have accordingly granted ISPs broad immunity in defamation litigation; *see, e.g.*, *Ben Ezra v. America Online*, 206 F.3d 980 (2000) (holding Internet service provider immune from liability for defamatory speech initiated by a third party).
  - Suing the individuals who posted the defamatory material difficult because of the anonymity of many cyber-defendants.

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Internet Defamation

- **Internet Defamation Litigation**
  - Once lawsuits commence against the originators of the defamatory statements, what is the proper constitutional limit on state defamation liability?
  - If a private individual is defamed on the Internet, should the minimum liability standard be actual malice?
    - The rationale of *Gertz* – that private individuals do not have access to communication channels to counter defamatory speech and have not assumed the risk of defamation – no longer applies in cyberspace where everyone stands on the same ground.

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Internet Defamation

- **Internet Defamation Litigation**
  - First Amendment Issues:
    - "John Doe" Litigation – Yahoo! and AOL have been required by subpoena to provide the actual email addresses of individuals who have postings on message boards and chat rooms.
    - ISPs are resisting such subpoenas, citing privacy laws.

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Cybersquatting

- ***Anticybersquatting Protection Act – 15 U.S.C. § 1125(d)***
  - Overview
    - The ACPA amended the Lanham Act to expressly provide trademark owners with a civil cause of action against cybersquatters.
    - ***Cybersquatter*****:** person who, with a bad faith intent to profit from a mark, registers, traffics in, or uses a domain name that is identical or confusingly similar to a distinctive mark; is identical or confusingly similar to or dilutive of that mark; or is a trademark, word or name protected by Section 703 of Title 18.

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Cybersquatting

- ***Anticybersquatting Protection Act – 15 U.S.C. § 1125(d)***
  - Overview
    - ACPA's factors that may constitute bad faith:
      - Intellectual property rights in the domain name;
      - Legal name of the person;
      - Person's prior use of the domain name;
      - The person's intent to divert consumers from the mark owner's online location;
      - The person's offer to assign the domain name to the mark owner or any third party for financial gain.

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Cybersquatting

- ***Anticybersquatting Protection Act – 15 U.S.C. § 1125(d)***
  - Overview
    - ACPA's Safe Harbor Provision – bad faith intent will not be found in any case in which the person believed and had a reasonable grounds to believe that the use of the domain name was a fair use or otherwise lawful.

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Cybersquatting

- ***Anticybersquatting Protection Act – 15 U.S.C. § 1125(d)***
  - Examples
    - *Sporty's Farm, L.L.C. v. Sportsman's Market, Inc.*, 202 F.3d 489 (2d Cir. 2000) – Ordered the plaintiff (Sporty's Farm) to transfer the disputed domain name, "SPORTYS.COM" to the defendant (Sportsman's Market).
    - *Virtual Works, Inc. v. Volkswagen of America, Inc.*, 238 F.3d 264 (4th Cir. 2001) –Virtual Works' offer to sell the disputed domain name to Volkswagen, followed by a threat to auction the domain name to the highest bidder, constituted evidence of Virtual Works' bad faith intent to profit from registering "VW.NET" which was confusingly similar to Volkswagen's protected mark.

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Cybersquatting

- **Internet Corporation for Assigned Names and Numbers (ICANN) and the Uniform Domain Name Dispute Resolution Policy (UDRP)**
  - ICANN
    - Formed in October 1998
    - Non-profit, private-sector corporation formed by a broad coalition of the Internet's business, technical, academic, and user communities.
    - Created by members of the Internet community in response to a June 1998 White Paper issued by the U.S. Department of Commerce.
    - Recognized by the U.S. and other governments as the global consensus entity to coordinate the technical management of the Internet's domain name system, the allocation of IP address space, the assignment of protocol parameters, and the management of the root server system.

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Cybersquatting

- **Internet Corporation for Assigned Names and Numbers (ICANN) and the Uniform Domain Name Dispute Resolution Policy (UDRP)**
  - ICANN
    - All ICANN approved registrars in the .com, .net, and .org top-level domains follow the UDRP.
    - Under the policy, most types of trademark-based domain-name disputes must be resolved by agreement, court action, or arbitration before a registrar will cancel, suspend, or transfer a domain name.
    - Disputes alleged to arise from abusive registrations of domain names (for example, cybersquatting) may be addressed by expedited administrative proceedings that the holder of trademark rights initiates by filing a complaint with an approved dispute-resolution service provider.

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Cybersquatting

- **Internet Corporation for Assigned Names and Numbers (ICANN) and the Uniform Domain Name Dispute Resolution Policy (UDRP)**
  - ICANN
    - To invoke the policy, (a) file a complaint in a court of proper jurisdiction against the domain-name holder or (b) in cases of abusive registration submit a complaint to an approved dispute-resolution service provider.
    - The UDRP is mandatory for respondents but not complainants.
    - The benefits under the UDRP: expeditious resolution; lowers costs.
    - The benefits under the ACPA through the courts: ACPA is more expansive, provides less protection to cybersquatters; cancellation and transfer are the only remedies available pursuant to the UDRP (no damages).

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Cybersquatting

- **Examples**
  - *World Wrestling Federation Entertainment v. Bosman*, Case No. D99-0001 – WIPO Panel ordered the transfer of the "worldwrestlingfederation.com" domain name because it was identical or confusingly similar to the trademark in which the complainant had rights and respondent had no rights or legitimate interests in the domain name.
  - *Raymond Weil S.A. v. Datoo Abbas*, Case No. D2001-0597 – The panel ordered the respondent to transfer the domain name to the complainant.

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Cybersquatting

- **Future Issues to Anticipate**
  - Questions concerning the authority of ICANN.
  - Allocation and award of second level domain names upon opening of new TLD market:
    - How the new registry operators will manage and distribute trademark domain names, i.e.,
      - SUNRISE PERIOD
    - How the new registry operators will allocate domain names to competing parties. First in time?

AKIN GUMP STRAUSS HAUER & FELD, L.L.P.

Cybersquatting

- **Future Issues to Anticipate**
  - Resolution of international trademark issues.
  - Proposed protocol that will allow the DNS to look at a name entered in a language other than English and translate it into the correct numeric Internet address.
  - WHOIS privacy issues for domain name registration.

Minimizing E-Commerce E-Litigation: A In-House Practical Guide

Vanessa L. Allen, Esq.
Digex, Incorporated
October 17, 2001

Digex, Incorporated

Agenda

- Trends - Data Accumulation and Retention
- Trends - Legal
- Prior to Litigation
- During Litigation
- Post-Litigation

Digex, Incorporated

Trends

Fed. R. of Civ. Proc.

1970 - Electronic Data Compilations subject to production Paper Storage

Pre-1990s

Proliferation of Automation & Corporate & Legal Adoption of Technology

Common, Affordable Tools for Communication

1990s

Laptops/ Desktops

Fax Machines

Text Pagers/Cell Phone/PDAs

Instant Messaging

E-Mail/ Doc. Attachment

Data Storage; LAN & WAN

Internet/Hosting

Today

Digex, Incorporated

Tools Of Technology

INTERNET

WIRELESS PHONES; PDAs

HANDHELD DEVICES

LAPTOP AND DESKTOPS

Digex, Incorporated

Trends

- **E-Mail Storage & Communication**
- Litigation involving electronic data, e-commerce and in-house & courtroom technology
- **Application of Fed. Rules of Evidence/Spoliation**
- Specialized Courts & e-filing; More Savvy Judges

Digex, Incorporated

Trends

- Firms that Manage and Restore Data
- Corporate Electronic Policies & Procedures
- Insurance Coverage for E-Commerce
- E-Contracts

Digex, Incorporated

Prior to Litigation

- Preventative Measures
  - ADR
  - Know your state's courts, experience & view
  - Document Management and Retention
    - Can your client produce relevant data
    - How do your client avoid destroying data
    - How or how long does your client retain data
    - Know your duties: to produce, to preserve, to store
    - Attorney-Client Privilege for E-mail

Digex, Incorporated

Data Retention - Legal Overview

- Fed. Rules of Civ. Procedure
  - 34 & 26(1)(a)(1)(B)
- State-specific Concerns
  - Statute of Limitations
  - Spoliation

Digex, Incorporated

Data Retention - Legal Overview

- Courts have not squarely addressed whether computer data is tangible property.
- Insurance Companies have not squarely addressed what property will be covered by traditional policies

Digex, Incorporated

Data Retention - Legal Overview

- Relevant Cases
  - Lewy v. Remington Arms Co., Inc. (data retention policy)
  - Stanton v. Nat'l R.R. Passenger Corp.(data retention policy)
  - Linnen v. A.H. Robins Company, Inc., et al. (staff responsible for data management; witnesses)
  - Home Indemnity Co. v. Hyplains Beef, L.C. (computer data subject to physical damage)

Digex, Incorporated

Data Retention - Legal Overview

- Relevant Cases
  - Magnetic Data, Inc. v. St. Paul Fire & Marine Insurance Co. (erased data barred under a control of property exclusion because it was under insured's control)
  - Retail Systems, Inc. v. CAN Insurance Cos. (computer data on tape is merged with the physical tape and therefore, if the tape is lost, a loss of tangible property results related to the tape)
  - St. Paul Fire & Marine Insurance Co. v. National Computer Systems, Inc.

Digex, Incorporated

Data Retention - Policy

- Data Retention Policy
  1. Is it committed to a writing?
  2. Does your client's data retention policy meet reasonableness standards considering the facts & circumstances surrounding documents
  3. Have lawsuits concerning a complaint or related complaints been filed? What are the frequency of complaints and what is the magnitude of complaints?
  4. Was the retention policy implemented in good faith? (e.g. year, purpose, scope, etc.)

Digex, Incorporated

Data Handling - Employee Issues

- Training
  - Company's data retention and E-mail policies; business v. personal E-mail
  - Audit for compliance
  - Work with IT to understand internal systems
- Insurance Coverage
  - Errors & Omissions; Professional Liability

Digex, Incorporated

Business Problem Areas

- Adequately defining & protecting data
- Support from your client - who to engage?
  - IT
  - Risk Management/ Finance
  - Executive Team
- Legacy Systems and data
- Role of the Internet and telecommuting capabilities
- Know your corporate culture - Perception of Technology

Digex, Incorporated

Prior To Litigation - Benefits

- Protect Trade Secrets & Other IP
- Lower Costs of Discovery; Maintain Control of Document Production
- Lessen the Impact on Daily Corporate Function
- Demonstrate Good Faith Approach to Data Management; Favorable Judicial View
- Use Internal Systems and Outside Counsel More Efficiently and Advantageously
- Due Diligence Requests

Digex, Incorporated

During Litigation

- ✔Maintenance of Data (regardless of Retention Policy); Organization for Later Suits
- ✔Availability of Witnesses
- ✔Assessment of Contractual Liability and Insurance Exposure
- ✔Good Faith Management of Electronic Data and Documents

Digex, Incorporated

Post-Litigation Assessment

- Are there problems with my clients' internal policies? *Data management/retention, Telecommuting, Responses to potential suits, etc.*
- What information do I require on appeal?
- Where did we go wrong/right, and how do we improve?
- Was insurance coverage helpful? Did my client require new types of coverage?

Digex, Incorporated

Insurance

- "Many of the fast-paced online firms are so focused on rapid growth that they neglect to look closely at network security and legal liabilities."
  - Insuretrust.com, USA Today, June 7, 2000
- Online investors sued E-Trade for network outages

Digex, Incorporated

Insurance:What Do I Have, What Do I Need?

- Client's assets
  - Tangible v. Intangible
- Value of Client's information, profit stream and reputation
- Client exposure to liability
- Client's current insurance coverage
  - Original policy date? For what business?
- Affordability & Need Assessment

Digex, Incorporated

Insurance - Avoid Pitfalls

- What leverage does the client have with the insurer?
- What is the reputation and experience of the insurer?
- What alternative risk transfer mechanisms are available to finance e-commerce risks?
- Compare terms/price of stand-alone policy and amendments to traditional policy

Digex, Incorporated

Insurance

- Enhance traditional commercial liability coverage with e-commerce ("online") policies
  - Lost revenue reimbursed (Lloyd's of London, AIG)
  - Tarnished reputation improved with funds for PR firm to create a damage-control plan (Fidelity & Deposit)
- E-commerce coverage ← $1M - $250M

Digex, Incorporated

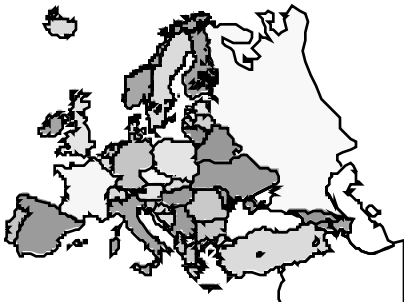
How Do I Get Sufficient Coverage?

- **Amend traditional policies and/or add additional policy coverage**
- **Specialized coverage such as Net Secure from Marsh**
- **Evaluate e-commerce insurance to cover any "gaps" in traditional coverage**

Digex, Incorporated

Insurance: International Issues

- *Insured should determine how its policies apply to e-commerce activity and computer data (incl. Vendor & customer)*
- *United Kingdom & Europe are expressly excluding or limiting coverage for losses caused by computer virus*



Digex, Incorporated

Making Counsel's Job Easier

- Work with the Risk Management Team
- Talk to vendors & partners about their insurance
- Review existing agreements
- Review client contract templates
- Educate your executive team, employees and customers on data retention
- Enforce… consistently! Reward and Sanction
- Have good outside counsel manage the issues

Digex, Incorporated

Digex, Incorporated

Cost-Benefit Tug of War

- Legal Protection Cost (contract enforcement, litigation, premiums)
- Business practices implementation costs
- Cost of storing or insuring everything, everywhere
- Value of the information at risk
- Legal statutory and common law requirements
- Likelihood of need insurance funds

Digex, Incorporated

Conclusion

- SOUND POLICIES - internal and external
- ESTABLISH good client relationships
- MONITOR state & federal law
- RE-EVALUATE often

Digex, Incorporated

