

COMMERCIAL TRANSACTIONS

THE EVOLVING RELATIONSHIP OF THE INTERNET AND THE LAW

While there are emerging new uses of the Internet in government, education, science, medicine and the arts, commercial transactions between buyers and sellers are at the heart of Internet growth. These transactions can be business-to-business or business-to-consumer. They can involve any kind of produced goods or services. They can use traditional means of distribution and order fulfillment or new electronic means. Equally important, these transactions, the parties to them and the products involved, can all be subject to regular commercial law principles and, often, to government regulation at federal, state or international levels.

While Internet transactions and the growth of the Internet as a commercial medium of exchange both occur at very high speed, the law moves at a much slower pace. The result is often delay, doubt or confusion as to whether, and how, commercial law or government regulation apply to particular kinds of transactions. Nonetheless, traditional forums of rule making authority have expanded their guidance to the Internet. For example, the Federal Trade Commission now applies more than thirty of its rules and guides to Internet transactions. The Federal Trade Commission has numerous useful publications on its website located at <http://www.ftc.gov/bcp/menu-internet.htm>.

This state of flux and transition between the law and the Internet means that anyone developing an Internet site for commercial transactions needs to pay careful attention to issues like jurisdiction, taxation, digital signatures, advertising and

unsolicited e-mail, privacy and the formation of contracts. These and other subjects are addressed in the sections which follow.

THE INTERNET AND JURISDICTION

The Basis Of Personal Jurisdiction

Businesses operating on the Internet face the possibility that such activities may subject them to liability in other jurisdictions. Since the Internet transcends geographical boundaries, one may be subject to a lawsuit in another state and even in another country.

In the United States, the extent to which one is subject to litigation in other forums is determined by the concept of personal jurisdiction. A court must have personal jurisdiction over the litigants and the claims at issue in order to enter an enforceable judgment. To determine jurisdiction, courts look to the long-arm statute of the state in which litigation is initiated. Most long-arm statutes are similar, and have requirements that the party over which jurisdiction is sought be (1) "transacting business" within the state, (2) "committing a tortious act" within the state, or (3) "committing a tortious act" outside the state that causes injury within the state.

If the long-arm statute is met, the court then must determine whether the exercise of jurisdiction would be consistent with the constitutional requirements of due process. Due process may be satisfied if defendant's contacts with the state are sufficient to give rise to general jurisdiction. If there is no general jurisdiction, specific jurisdiction exists if (i) defendant "purposefully availed" himself/herself of the privilege of acting in the forum state, (ii) the cause of action arose from the defendant's activities in the forum state, and (iii) defendant had sufficient "minimum contacts" with the forum state to make the exercise of jurisdiction "reasonable," i.e., in conformance with notions of "fair play and substantial justice." See, *World-Wide Volkswagen Corp. v. Woodson*, 444 U.S. 286 (1979).

Personal Jurisdiction And The Internet

Traditional tests of personal jurisdiction are applied to cases involving Internet activity. Presence on the Internet will not automatically subject one to jurisdiction anywhere. Recent cases indicate that merely posting information on a web site with no contact or interaction with the forum state will not subject one to jurisdiction. See *Bensusan Restaurant Corp. v. King*, 937 F.Supp. 295 (S.D.N.Y. 1996). There must be more. Basically, courts must consider whether messages on a web page that are available to residents of a jurisdiction have been “deliberately directed toward the forum” or have merely arrived there through no direct intention of the defendant.

In a Minnesota case, *Minnesota v. Granite Gate Resorts*, 568N.W.2d715 (Minn. Ct. App. 1997), the court determined that Minnesota had jurisdiction over an out-of-state company whose web site solicited gambling by Minnesota residents. In *Granite Gate*, a company opened an Internet on-line gambling service from Belize called “WagerNet.” In order to access “WagerNet,” one first had to pay a \$100 set-up fee to receive certain necessary hardware and software. In addition, members were to place at least \$1,000 into an account to cover their bets. The WagerNet fee for handling bets was 2-1/2%, and, after paying this fee, one could bet on-line. To attract customers, WagerNet advertised its service on the Internet at the Web site: <http://www.vegas.com/wagernet>. The web site included several disclaimers and several telephone numbers that prospective members could call to be placed on a mailing list in order to receive information. The Minnesota Attorney General took the position that on-line betting violated both federal law and Minnesota law and filed suit in Minnesota against Granite Gate.

In *Granite Gate*, the court found that based upon the extent and nature of the Internet advertising, the defendant had sufficient “minimum contacts” with the forum state, and could “reasonably anticipate being hailed into court in Minnesota.” The court further held that “maintenance of the suit in the forum state [would not] offend traditional notions of fair play and substantial justice.” In

reaching its conclusion, the court considered that the Internet advertisement was available “24 hours a day, seven days a week to any Internet user.” In addition, the court also considered WagerNet’s intent to reach potential customers in Minnesota, as well as the inclusion of numerous Minnesota residents on its mailing list.

Ordinarily, a state’s jurisdiction is limited to people, businesses, transactions, events, or other occurrences within the state’s geographical territory. A state may, however, exercise its right to assert jurisdiction over non-residents to the extent such parties transact business within the state, commit illegal acts within the state, own or possess real property within the state, make or perform a contract within or connected to the state, breach a fiduciary duty within the state, or do any other act giving rise to personal jurisdiction in accordance with the state’s laws. Any business conducting activities through the Internet must therefore assume that it may be subject to jurisdiction in another state. To avoid liability, a business might consider specifically identifying on its web site that its offer is limited to specific states. If the web site merely contains information and is not interactive, it may not provide the minimal contacts necessary to trigger jurisdiction. If, however, direct mailings and toll free telephone numbers are combined with promotion over the Internet, courts may assert jurisdiction. Finally, by incorporating the business activities related to the Internet separately from the company’s regular business operations, the business might be able to shield its core assets from liability. Jurisdictional issues related to the Internet are particularly difficult to predict since such cases will depend upon the specific facts and circumstances of each situation. It is fair to say, however, that any company doing business on the Internet should consider that it is now essentially a global business that might be sued in any court and in any territory where its presence becomes known.

The following four themes have emerged from the growing body of case law related to jurisdiction on the Internet:

- **Deriving revenue from forum equals jurisdiction**

Revenue producing activities on the Internet that result in revenue earned in the forum district may result in a finding of personal jurisdiction. See *CompuServe, Inc. v. Patterson*, 89 F.3d 1257 (6th Cir. 1996).

- **Sliding Scale established for Internet sellers**

The more completely the transaction of business can take place on-line, the more likely that the court will assert jurisdiction based on the on-line activities, *Minnesota v. Granite Gate Resorts Inc.*, 568 N.W.2d 715 (Minn. Ct. App. 1997). Passive web sites that only provide information about the defendant are not likely to be a sufficient basis for personal jurisdiction in a forum state where the defendant does not conduct business. See *Cybersell, Inc. v. Cybersell, Inc.*, 44 U.S.P.Q.2d 1928 (9th Cir. 1997). There are, however, several exceptions where passive Internet sites of out-of-state defendants were found sufficient to establish personal jurisdiction. See *Maritz, Inc. v. Cybergold, Inc.*, 947 F.Supp. 1328 . (E.D. Mo. 1996).

- **Effects test of torts applied**

The “Effects test” is applied where trademark infringement, defamation, or other torts are alleged, to find jurisdiction based on intentional action expressly aimed at the forum state, and causing harm in the forum state. See *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, 952 F.Supp. 1119 (W.D. Pa. 1997).

- **24 hours a day-7 days a week**

The continuous nature of the Internet makes it more substantial than print, radio, or television. As such, Internet commerce or advertising is more likely to increase the amount of contacts with other forums. See *Inset Systems, Inc. v. Instruction Set*, 937 F.Supp. 161 (D. Conn. 1996).

As online business becomes a global enterprise, cases involving foreign parties and jurisdiction are becoming frequent. The *Arista Record Company* sued a Spanish business based on a website *Puretunes.com* that allowed individuals to download copyrighted

works owned by Arista without their permission. This action was filed in Washington, D.C. and the Defendant moved for dismissal arguing that the Spanish company had no business contacts in the District of Columbia. During discovery it was revealed that Defendant had customers in the District of Columbia based on information obtained through computer servers owned by a third party service provider as well as the credit card company that provided payment information on customers of the Spanish business. The Motion to Dismiss for lack of personal jurisdiction was therefore denied. See *Arista Records Inc. v. Sakfield Holding Company*, 314 F.Supp 2nd 27, 71 U.S.P.Q. 2nd 1035 (D.D.C. Apr. 22, 2004).

TAXATION

The increasing amount of commerce conducted through and on the Internet also raises questions of whether and how that commerce should be taxed by the states. With respect to state sales tax laws and the Internet, the closest analogy is the law with respect to mail order (i.e., catalog) sales. In that context, the Supreme Court of the United States has ruled, most recently in *Quill Corporation v. North Dakota*, 504 U.S. 298 (1992), that a use tax imposed on a mail order firm that was not physically present in that state violated the Commerce clause of the U.S. Constitution. Note that the *Quill* decision is only the most recent of many cases dealing with whether and how a state may legally impose sales and use tax laws on businesses without any employees or property located within that state. Also, it should be noted that the majority opinion in the *Quill* case makes it clear that Congress' power to regulate interstate commerce means that Congress is free to pass legislation overruling the *Quill* decision or any others like it.

With respect to state income taxation of Internet commerce, the closest analogy is the Supreme Court of the United States's 1992 decision in *Wisconsin Department of Revenue v. William Wrigley, Jr., Co.*, (505 U.S. 214). In that case, the Supreme Court was asked to interpret 15 U.S.C. § 381, which prohibits a state from taxing the income of a corporation whose only business activities within the

state consist of “solicitation of orders” for tangible goods, provided that the orders are sent outside the state for approval and the goods are delivered from outside that state. At issue in that case were whether the activities in Wisconsin of Wrigley Co.’s sales representatives were so great as to fall outside the protection from tax offered by 15 U.S.C. § 381. The Court found that those representatives’ practices of providing free, replacement gum to retailers, of selling gum to retailers, and of storing gum at home or in rented spaces fell outside the statutory protection.

On October 21, 1998, President Clinton signed into law the Internet Tax Freedom Act (ITFA). In November 2001, the ITFA was extended for two years. The ITFA, which expired in 2003, was an effort to preempt state and local taxes that are viewed by some as a potential threat to the growth of commerce on the Internet. The purpose of ITFA was to establish a national policy against state and local government interference with interstate commerce on the Internet by establishing a moratorium on the imposition of taxes that interfere with the free flow of commerce on the Internet. On December 3, 2004 President Bush signed the Internet Tax Nondiscrimination Act into law reinstating the ban on Internet access taxes for an additional three years.

As more and more businesses are looking at the Internet as a vehicle for selling products, there will be continued discussion as to whether the imposition of new efforts to collect government taxes will hinder electronic commerce. In the meantime, according to Forrester Research, Inc., on-line retail sales have exploded past \$100 billion in 2003. This represents an increase from \$500 million in 1995, \$1.1 billion in 1996, and \$6 billion in 1997 and \$14.8 billion in 2000. On-line retail sales are expected to reach \$269 billion in 2005. It should be noted, however, that Internet sales still represent only a small fraction of retail sales (less 6%). Whether or not the freedom from taxation for on-line commerce is justified or poses a significant threat to traditional retail businesses remains a significant issue.

ELECTRONIC PAYMENT SYSTEMS

While the conventional form of payment for retail products and services includes coins and currency, checks, money orders, and credit cards, there are also electronic fund transfer systems that have been used for over a decade including automated teller machines, debit cards used to automatically pay merchants by debiting customer's accounts, and point of sale systems which debit or credit customer accounts. There are a number of federal laws which apply to any entity providing such services including the Truth in Lending Act ("TILA") and the Electronic Fund Transfer Act ("EFTA"). The TILA and the EFTA protect consumers with paper-less transactions involving telephones, electronics, and computers. Other federal laws address financial privacy issues related to electronic cash payment systems including the Right to Financial Privacy Act of 1978.

Rapidly developing electronic cash technologies may challenge the traditional banking rules and regulations. It is not yet clear how these new technologies might mesh with existing payment systems and what laws will control. Legal issues concerning bank regulations, consumer protection, financial privacy and risk allocation all must be considered by any business that is considering utilizing some form of electronic cash payment technology.

The newer electronic cash payment systems store monetary value in the form of electronic signals on a plastic card, on a computer drive or on a disk. There are also digital cash systems which allow electronic cash to be used over computer networks without use of a plastic card - sometimes called "digital cash." An example of a digital cash transaction would be as follows:

1. A digital cash account is opened by a customer by depositing funds in a "Cyberbank."
2. The customer's funds are held in trust by the Cyberbank.
3. When the customer purchases a product or service over the

Internet, the customer transmits an encrypted electronic e-mail message with the customer's unique digital signature to the Cyberbank requesting release of customer's funds.

4. The customer's account is debited and the digital cash is transmitted via phone lines to the customer's computer.
5. The customer then transmits the digital cash to the merchant who can verify authenticity of the customer's digital signature, credit the digital cash amount to merchant's account with the Cyberbank, or transmit the digital cash to another party.
6. The Cyberbank may charge the customer or merchant a fee to participate in such an electronic payment system.

The Federal Reserve Board's Regulation "E" governs on-line payment systems which provide digital substitutes for cash and electronic funds transfers. This federal law defines electronic funds transfers as any transfer of funds initiated through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit an account. A business contemplating use of such an online payment system should verify that it complies with the requirements of Regulation "E."

SELLING PRODUCTS ON AUCTION SITES

Businesses of all sizes are finding avenues to use the Internet to market their products. One of the more recent trends, especially for smaller businesses, is the use of Internet auction sites for both sale and purchase of products. There are two main types of Internet auctions. In an ascending price auction (often referred to as a "forward" or "English" auction); a seller puts up product for sale on the seller's own site or an Internet "marketplace" site, and bidders place bids in ascending amounts. After a pre-determined time, the top bidder pays the seller, completes the transaction and the product is shipped. In a descending price auction (often referred to as a "reverse" or "Dutch" auction), a buyer announces

its product needs on its own or an Internet “marketplace” site and sellers submit their lowest price. After a pre-determined time, the seller selects the lowest bid, completes the transaction and the product is shipped.

Most auction sites have a method whereby buyers can rate sellers and sellers can rate buyers. Sellers are prohibited from placing false testimonials in their auctions. Sellers must also refrain from placing bids on their own products to increase the price. As reported on the Federal Trade Commission’s web site, “(t)hese practices are not only unethical, they’re also fraudulent.” Sellers also may not offer illegal items through Internet Auctions. The Federal Trade Commission provides additional details to protect sellers and buyers at www.ftc.gov/bcp/conline/pubs/onlin/auctions.htm.

SECURITY ON-LINE AND DIGITAL SIGNATURES

A major concern of buyers and sellers over the Internet involves the security and authenticity of transactions conducted on-line. How can the seller be assured of the integrity of the orders and payments for its products and services? How can the buyer be assured it will be provided the quality product or service purchased on-line?

Digital signatures and third party certification are methods used by vendors to authenticate the buyer. A “digital signature” is the electronic substitute for a handwritten signature. The Minnesota Electronic Authentication Act, Minn. Stat. §325K.01 et. seq., defines digital signatures as “a transformation of a message using an asymmetric cryptosystem such that a person having the initial messages and the signer’s public key can accurately determine: (1) whether the transformation was created using the private key that corresponds to the signer’s public key; and (2) whether the initial message has been altered since the transformation was made.” An asymmetric cryptosystem is “an algorithm or series of algorithms that provide a secure key pair.”

In addition, Minnesota has enacted the Uniform Electronic Transactions Act (Minnesota Statutes Chapter 325L, as added by

Chapter 371 of the 2000 Laws of Minnesota) (UETA). Under Chapter 325L, parties may choose (but are not required) to use electronic records or signatures in place of written ones. (Note that the UETA does not apply, among other instances, to transactions governed by certain sections of the Uniform Commercial Code). The UETA provides that electronic records or signatures may not be denied validity or legal effect solely because they are in electronic form, and that such records or signatures satisfy laws that require records or signatures to be in writing. The UETA also contains provisions:

- setting out requirements for accessing, reading and retaining electronic records and signatures;
- allowing for the notarization of electronic records and signatures, and the transferability of electronic records;
- addressing when electronic records are considered to be received and sent; and
- allowing for making changes to already-transmitted electronic records (including but not limited to when those records contain errors).

Digital signatures should become a viable means of creating legally binding contracts for products and services on-line. Utah and Minnesota are among the first states to enact a digital signature act, and other states are likely to follow. A key element in the use of digital signatures involves a form of encryption. An individual is given two encryption keys - a private key known only to the individual and a public key made available to other Internet users. The sender of a message on-line uses his or her unique private key as well as the public key of the intended recipient of the on-line message. The recipient of the on-line message must use the public key of the sender and the unique private key of the recipient to receive the on-line message. For many transactions on the Internet, the digital signatures resulting from this public key encryption system will provide adequate security. There is also an encryption system involving a third party

which can certify the identity of the seller or recipient for purposes of authenticating the message or payment. The use of such third party digital certification systems may help further address some of the legal concerns relative to authentication of electronic transactions. Rules and standards for such third party certification are still evolving and some uncertainty remains regarding liability of such third parties for non-payment or errors in the certification process. Courts are likely to look at existing laws covering liability for credit card transactions when considering liability of third parties providing digital certification.

UNSOLICITED E-MAIL

Bulk e-mail has become a popular way to market products or services on-line. With minimal cost and quick delivery, e-mail has been adopted as a cheap and effective direct marketing tool. However, the use of bulk e-mail has also become an annoyance and hindrance to many users of the Internet and has led to proposed federal legislation to try to curb such practices. Of particular concern is what is known as "spamming." This is the Internet equivalent of junk mail and consists of a wide distribution of unsolicited e-mail messages usually promoting a product or service. In one case, *Cyber Promotions, Inc. v. America On-Line, Inc.*, C.A. No. 96-2486 (E.D. Pa. Nov. 4, 1996), the Court found that Cyber Promotions, which had been sending bulk e-mail messages to AOL subscribers, did not have a First Amendment right of free speech to deliver unsolicited e-mail through a privately owned computer services network such as AOL and that AOL was entitled to restrict the transmission of bulk e-mail messages to its customers. The AOL electronic community was not deemed a public forum that would allow the exercise of such First Amendment rights. In a related case, *CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015 (S.D. Ohio 1997), the Court found that the disseminator of bulk e-mail may be liable for damages as a result of trespass on the computer system of the Internet service provider if such e-mail transmissions are received without the consent of the Internet service provider.

THE CAN-SPAM ACT

The CAN-SPAM Act (acronym for “Controlling the Assault of Non-solicited Pornography and Marketing”) (P.L. 108-187, 117 Stat. 2719) became effective January 1, 2004. This new federal law preempts over 30 state laws (including the Minnesota law) that had been enacted to control the proliferation of unsolicited commercial e-mail. CAN-SPAM does not ban unsolicited commercial e-mail but may have a significant impact on all businesses who use e-mail to communicate with or advertise to customers. The federal law leaves intact those portions of state laws that cover falsified information and other fraudulent activity. CAN-SPAM applies to all commercial electronic mail, defined as any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service. So called “transaction and relationship” messages are specifically excluded and include e-mail sent with billing statements, emails necessary to complete a transaction, warranty information, account balance, and similar type information. The law requires that all commercial e-mail messages include 1) text that describes how the recipient can “opt out” of receiving future e-mails; 2) the senders physical address; and 3) an indication that the e-mail is a solicitation. The law also bans the use of a false or misleading header, sender or subject line information or the use of deceptive subject headings.

Any business that is contemplating sending bulk e-mail must consider all federal and state laws which may apply. This legal landscape is likely to change at any time. Permission should be obtained from any Internet service provider that would be the recipient of such bulk e-mail messages. Permission should also be requested from the ultimate recipient of such bulk e-mail with an opportunity to opt out of receiving such messages. Under no circumstances should any false or misleading information be transmitted on-line. The volume of e-mail messages should be reasonable so as not to become an annoyance or hindrance to the recipients. Finally, the terms of an agreement with an Internet service provider may specifically restrict the use of bulk e-mail.

PRIVACY

Since the Internet involves the transmission of large amounts of data among and between a large number of people and organizations, privacy of such data is of great concern. This problem has been widely discussed and debated and is likely going to grow in intensity as the collection and communication of personal data continues to increase. However, this is not an entirely new phenomenon.

Even before the Internet existed, laws were enacted to protect individuals from the use and disclosure of personal information. The Electronic Fund Transfer Act passed in 1978 required financial institutions to disclose the circumstances under which they would provide account information on individuals to third parties. The Cable Privacy Act, Electronic Communications Privacy Act (ECPA), and the Telephone Consumer Protection Act were all designed to protect individuals from unreasonable intrusions on the personal privacy of individuals.

Because privacy flows from constitutional, tort, legislative, and public perceptions, it is difficult to provide general legal guidance as to how such issues might be handled by the courts. It should be noted, however, that corporations do not have a right to privacy. A corporation must therefore rely upon the intellectual property and unfair competition laws.

The United States Constitution limits the ability of the government to obtain private information about individuals. These constitutional protections are, however, limited to government intrusion into personal privacy and do not cover circumstances where an individual voluntarily places personal information into commercial use or makes such information accessible to another party.

The ECPA covers some of the basic privacy issues surrounding the use of e-mail, including the procedural steps necessary to search and retrieve such information.

Privacy issues on the Internet may differ depending upon the

product, parties, method of collecting information, use of the information, and storage medium involved in the collection and use of information.

For example, there are federal privacy laws which cover government record keeping (5 U.S.C. § 552); videotape rental records (18 U.S.C. § 2710); credit reports (15 U.S.C. § 1681); political contributors (2 U.S.C. § 438); tax records (26 U.S.C. § 6103); cable TV viewing habits (47 U.S.C. § 551); and delivery of pornography through the mail (39 U.S.C. § 3008).

The ECPA regulates the privacy of e-mail messages in public e-mail systems by prohibiting the interception, use, or disclosure of e-mail by third parties. The ECPA also sets forth procedural safeguards and standards that law enforcement agencies must follow when seeking access to e-mail. The ECPA does not apply if a party has consented to such monitoring, and it may not apply to private e-mail systems such as those operated by employers. Most businesses and organizations that have implemented e-mail systems have also developed corporate policies which specifically clarify the scope of privacy, if any, employees are entitled to within the employer's system. (See the section of this Guide entitled Employment Law - Privacy of Employee E-mail).

In *USA vs. Bradford Councilman*, 373 F.3d 197 (1st Cir. 2004); 2004 WL 1453032, the First Circuit United States Court of Appeals determined that there was no violation of the Wire Tap Act as amended by the Electronic Communications Privacy Act (ECPA) when stored e-mail was accessed, because, since it was in storage, no "interception" occurred within the meaning of the federal laws. The defendant was an officer of a business that operated an online listing service for rare and out of print books. The business also provided e-mail service to some of its customers who were book dealers. The government claimed that the business developed and used computer code that enabled them to intercept, copy and store e-mail messages that were being transmitted from Amazon.com to their book dealer customers and to obtain commercial advantage by reading these messages prior

to them being received by the intended recipients. Defendants argued successfully that since the definition “electronic communication” in the statute makes no reference to stored communications no “interception” can occur while the e-mails are in electronic storage. Since there is no illegal interception as defined by the law the defendant argued there was no violation of the federal law. The case demonstrates the difficulty in application of these older federal wiretap laws to more recent Internet based technology as the court states “the language [of the statute] may be out of step with the technological realities of computer crimes. However, it is not the province of this court to graft meaning onto the statute where Congress has spoken plainly.” A strongly worded dissent suggests that the narrow approach of this court renders the Wiretap Act irrelevant.

It is important for businesses to notify their employees that their e-mails may be monitored and the employees have no right to privacy to such communications. Employers might even request that their employees sign a statement acknowledging that the employer has the right to monitor, access, and disclose any e-mail messages received or transmitted on their system. Such policy should be clear and unambiguous and, once implemented, applied by the employer consistently and fairly.

The Federal Trade Commission (FTC) brought an enforcement action targeted at the privacy practices of a web site operated by Geocities. The FTC accused Geocities of deceptive trade practices in its collection and use of personal information obtained from web site visitors. Geocities used an on-line application for new members and sold the collected information to third-party marketers. The FTC claimed that Geocities misrepresented that the collected information was used only for specific advertising offers requested by members. In a consent order, Geocities agreed to post a clear and prominent “Privacy Notice” which would disclose what information is being collected, for what purposes, to whom the information will be disclosed, and how consumers can access the information. Parental consent is necessary before collecting information from children under 13 years old and

Geocities must give members the opportunity to have their information deleted from Geocities' and third party's databases, In The Matter Of Geocities, Federal Trade Commission File No. 9823015, August 13, 1998 (consent order is available at <http://www.ftc.gov/os/1998/08/goe-ord.htm>).

PRIVACY ISSUES IN EUROPE

The European Community has gone far beyond the United States in its efforts to protect privacy rights. A Directive passed by the European Parliament in November 1995 requires that, among other things, personal data can only be processed if the subject has granted "unambiguous consent" to the collection and disclosure and use of the information. Article 25 of the Directive specifically covers the transfer of personal data from European Union countries to countries outside of the European Union and only allows transfers of personal data to those countries which afford an adequate level of protection for privacy of data or if adequate safeguards are implemented, i.e. contracts to specifically protect and preserve the data. It is still not clear whether the United States will be deemed adequate for purposes of the transfer of personal data from European Union countries in accordance with Article 25. The transfer of personal data to the United States from Europe will likely be evaluated based upon the federal, state, and local privacy laws in effect as well as any specific contractual arrangements that are in place to protect and preserve the specific data at issue.

Any business, large or small, doing business on the Internet must consider itself a global business, and the impact of the European privacy initiative may have an effect on their operations. The collection of data on-line to enhance marketing or advertising may be an acceptable practice in the United States but falls under the more severe restrictions that protect such personal data in Europe.