



“Laws too gentle are seldom obeyed; too severe, seldom executed.”

– Benjamin Franklin

Cyberlaw refers to the rules and regulations established by Congress, legislatures, courts, and international conventions to govern, prevent and resolve disputes that arise from the use of computers and the Internet.

Privacy of Online Communications

Before the advent of the Internet, there were fairly simple dividing lines between what information was widespread (reported in the media), what information was publicly available, but required effort to obtain (public records) and what information was private (more or less everything else). These dividing lines were presumed when most of our current public-records laws were enacted—before the Internet era.

How has the Internet blurred the dividing lines between public and private information? First, all sorts of “public” information, previously available only in hard copy to those who visited a courthouse file room or a county recorder’s office, is finding its way onto the Web. Social Security numbers, signature specimens, detailed personal financial information, mothers’ maiden names and credit card numbers are now available online to anyone in the world. Currently, there are few restrictions regarding the type of information courts and government agencies can place online. In addition, individuals who previously used letters and telephone calls to communicate now use the Internet for their personal communications. As a result, these private communications have a greater potential to become public even if the individuals who are communicating do not intend to make their communications public.

E-Mail

E-mail communications, like regular mail communications, are meant to be private. There are federal laws that prohibit the interception and disclosure of e-mail communications. For example, the Electronic Communications Privacy Act makes it a federal crime in many cases to intercept electronic communications, including e-mail, voicemail and FAX transmissions that have been sent by other people. However, individuals should not send e-mail messages expecting that they will remain private, nor should they assume that the laws would be enforced against anyone who discloses the messages. A single e-mail message may travel through many computers, even computers outside of the United States, before arriving at an intended recipient’s computer. As the message travels, copies may be made at each of these intermediate computers. An individual’s message may be shared with others accidentally, even with others outside the United States.

To enhance the privacy of e-mail communications, individuals can encrypt messages before sending them. Encryption software used for e-mail messages typically scrambles the message content so that only the intended recipient can read the message. Some e-mail programs include tools to encrypt messages before they are sent. If an individual’s e-mail program does not support encryption, he or she may use a separate program to encrypt messages before sending them.

Another common practice is to add a confidentiality notice to the message. Most confidentiality notices state that the message is intended only for the person to whom it is addressed and may contain confidential information. The notice also prohibits the dissemination or distribution of the message to other parties. Although such a notice does not ensure that a message will remain private, it may stop the recipient from revealing the contents of the message to others.

When an individual deletes an e-mail message appearing on his or her computer screen, typically only the copy of the e-mail being viewed is deleted. The default settings of many e-mail programs do not remove the message from the user's computer even though an individual's e-mail program says the message has been deleted. Many e-mail programs only move the selected message to a "deleted items" or "trash" folder. These folders of deleted messages may be accessed and viewed at any time as though the messages were never deleted. When a message is finally deleted from the Deleted Items or Trash folder, it is no longer accessible through the e-mail program; however, inexpensive "undelete" software and/or more sophisticated forensic analysis software often can recover the deleted message from a user's hard drive.

In addition, copies of the e-mail message may remain at one or more other computers through which the message has traveled on its way to the recipient's computer. Further, the sender and recipient of the e-mail message may have sent a copy of the message to many other recipients. Backup copies of the message also may have been created at each of the computers through which the message traveled. As a result, copies of the deleted e-mail message still may exist on a remote server, tape backup, or someone else's computer years after it was deleted from the user's computer.

So, although a privacy notice may be honored by a recipient, an e-mail sender should be aware that such notices cannot guarantee that an e-mail message will remain private.

Chat Rooms

Individuals participating in chat rooms assume the risk for their activities. It is a common practice for an individual to hide his or her identity while online. Many Internet service providers (ISPs) are willing to maintain the confidentiality of their members' identities. When a person believes his or her real identity is protected, that person may share thoughts and comments more freely, even

thoughts and comments that others find offensive, objectionable, or defamatory.

Some ISPs have service agreements that attempt to regulate their members' actions in chat rooms, as well as with other electronic communications. However, ISPs are not always willing, or even legally obligated, to resolve a complaint by one member against another member. An individual who believes another Internet user has harmed him or her should consult an Internet law attorney to get help understanding his or her rights.

Web Tracking

Inexpensive telecommunications, such as the Internet, combined with inexpensive computing power, makes it easier to gather detailed information about individuals. On the private side, Web advertisers use *cookies* to track people's Internet use, maintaining data files on millions of consumers with hundreds of data fields per consumer. (Cookies are files stored on a hard drive that a Web site server gives to a browser the first time the user visits the site and that are updated with each return visit.)

Recent federal legislation permits banks and financial institutions to sell to third parties, such as marketing agencies, all the information they have about their customers (on- or off-line), except for customers who specifically opt out. Under the 1999 Gramm-Leach-Bliley Act, financial institutions are required to notify their customers about their privacy policies and practices and to notify them of their right to opt out of the sharing of protected information with non-affiliated entities, except in limited cases. Since the Federal Trade Commission has recommended that no new privacy legislation regarding the Internet be introduced for the time being, it is unlikely that Internet privacy issues will be addressed in the near future. Also, post-September 11 legislation gives law enforcement personnel far more power to monitor and intercept information sent via the Internet.

In the near future, all cell phones should be able to transmit information about the location of cell phone users whenever they are switched on.

(The Federal Communications Commission required this “enhanced 9-1-1” service, but the requirement that mobile phones transmit location information was never limited to 9-1-1 calls.) This location data could allow companies to match the Web-browsing habits of targeted individuals with the driving habits of those same individuals in order to decide where to locate a new bridal shop or toy store. Or, a Web-enabled cell phone might beep with a special offer as a driver nears a certain restaurant. Such uses of location data may be commercially reasonable, but unprotected location data also could be sold to third parties. Therefore, cell phone users should be aware that their movements can be monitored when using a cell phone and may not remain private.

Cyberspace On The Job

Many employers provide employees with the equipment necessary to access the Internet and the Web to fulfill their job responsibilities. Therefore, an employer has the right to monitor and control the use of the equipment and an employee’s activities on the Web. Furthermore, employers must comply with federal and state workplace regulations. Employers have a duty to protect their employees from certain actions and can be liable to their employees for failure to take precautions. For example, employers have a duty to protect employees from sexual harassment. Consequently, they can prohibit an employee’s use of the Internet or Web sites to access or distribute unacceptable content.

Many employers have an Internet-use policy to inform their employees about what activities are permitted and what activities are prohibited. Most employers allow their employees to access the Internet for personal use as long as the use does not affect the employees’ job performance, consume significant resources, or interfere with other employees’ activities. Many employers do not regularly monitor their employees’ Internet use, but will inform their employees that messages and communications may be viewed publicly and inadvertently disclosed. Therefore, employees should not expect privacy when using the Internet

at work. Employees should check with their employers to determine whether an Internet-use policy applies to their activities at work.

Children’s Online Privacy

Congress enacted the Children’s Online Privacy Protection Act (COPPA) in 1998 to regulate the online sharing of information by children. The law requires Web site operators to obtain verifiable parental consent before collecting, using, or disclosing to third parties information from children under 13.

The law covers information such as full names, addresses, telephone numbers, or any other contact or identifying information. Web site operators must provide e-mail notice to parents of their use of such data. Parents may allow operators to use the data, but also can limit a Web site from disclosing the information to third parties. Parents also may review the data submitted by their children and bar further collection and use of the data.

What individuals can do to protect their privacy when using the Internet:

- Don’t click on links in e-mails to log into your bank, credit card, utilities or other important accounts. Instead, independently open your browser to log into these accounts.
- Create a password known only to you and avoid using personal information, such as your address or birthday, when creating it; change your password often and don’t share it.
- If you are not willing to use different passwords for each different Web site, at least use a different password for financially related accounts than you use for general Web sites.

Continued on page 189

What individuals can do to protect their privacy when using the Internet: (continued)

- If you cannot memorize all of your different passwords, at least store any written lists of passwords in a secure location.
- If you store lists of all your on-line accounts and passwords in a computer file such as a Word document, make sure this file is password protected.
- Unless you are using an encryption program with e-mail, be mindful that your e-mail messages could be intercepted and exploited by a third party without your knowledge.
- Whenever a financial institution sends you a disclosure document, read the fine print, find out how to opt out of information sharing, and opt out.
- Install an Internet firewall program and/or a firewall router to prevent unauthorized access to your computer and unauthorized transmissions from your computer.
- Use updated anti-virus software.
- Use updated spyware detection software.
- Use a browser that allows you to turn off cookies except for specific Web sites of your choosing.
- When giving information that will end up in a public record, provide only the minimum necessary, and if the information is for a court proceeding, consider asking for a protective order to restrict the scope of the disclosure.
- Review your credit reports once a year. You are entitled to receive one free credit file disclosure every 12 months from Equifax, Experian and TransUnion. (see AnnualCreditReport.com for details).
- Write to your legislators and express your opinion regarding what types of privacy should be protected by new legislation.

Using Online Information

Intellectual property laws protect those who create property that comes from the work of the mind, such as an invention, a program, a method, a painting, or a trade secret. Creators of certain types of intellectual property may protect their interests, for example, by registering a copyright or trademark, or by applying for a patent.

When using online information, it is important to understand that certain material is protected by intellectual property laws just as any hardcopy book or recording is protected. Therefore, it is important for those who use online information to understand how to appropriately use this information.

Intellectual Property and “Fair Use”

Individuals are free to view online content made available on an Internet Web page, although they may not be free to download, copy, print, or save this information. Some Web site operators will tell individuals what they can and cannot do with the information that is available from a particular site. In some cases, individuals may be asked to review a document while online and agree to the terms of use before viewing the information. In general, individuals must obtain permission from the copyright owner to use this information. If, however, an individual intends to use the information in a way that falls within a *fair use* exception, then that individual is not required to get the copyright owner’s permission. Courts consider the following factors in determining whether a use is a fair use:

- the purpose and character of the use;
- the nature of the work;
- the amount of the work involved; and
- the effect of the activity on the market for the original work.

The doctrine of fair use typically permits reproduction for scholarship and research (among other certain restricted uses), i.e., where society believes making information publicly available and useable increases its general welfare. For example, copying a page from an encyclopedia at the public library for personal use is probably a fair use. However, an individual is likely to run into trouble if he or she makes multiple copies and uses those copies for trade or business. This is why it is prudent to ask permission before using such information in any commercial setting. Unfortunately, deciding what is a fair use is often difficult, and may require the advice of an *intellectual property* (“copyright”) lawyer.

Authors are free to upload their original material (add it to an existing Web site). For example, an individual who has snapped some family photographs is free to post those photographs at his or her own Web site. An individual who does not know or is uncertain who owns the material to be uploaded, or whether the proposed use of the material falls within a fair use exception, should contact an intellectual property law attorney. The attorney can advise that individual about his or her rights to upload the material in question.

Cybersquatting

Cybersquatters, also known as *cyberpirates*, are people or companies that register trademarks as Internet addresses in bad faith for an improper purpose. Cybersquatters generally register Internet addresses so they can sell them back to a “squatted” company or business at excessive prices (sort of an Internet blackmail) or to tarnish or disparage another company’s brand. Cyberpirates also do the same thing with names of sports and entertainment celebrities.

According to Congress, the unauthorized registration and use of trademarks as Internet addresses have:

- resulted in consumer fraud and confusion;
- impaired electronic commerce; and
- deprived trademark owners of goodwill and revenues.

To remedy these problems, Congress enacted the Anti-Cybersquatting Consumer Protection Act.

The Act allows trademark owners to file a civil action against a person who had bad faith intent to profit from registering the trademark as an Internet address. Additionally, trademark owners can sue for statutory damages in the amount of \$1,000 to \$100,000 per Internet address and have the Internet address canceled or transferred to them if bad faith intent is proven.

In addition to the Act, trademark owners may use the Uniform Domain-Name Dispute Resolution Policy (UDRP) adopted in 1999 by the Internet Corporation for Assigned Names and Numbers (ICANN). According to the UDRP, an administrative panel must resolve Internet address disputes. Panel members consider factors such as whether the Internet address is confusingly similar or identical to the trademark, and if the Internet address was registered in bad faith. Unlike the Act, legal remedies under the UDRP do not include allowing trademark owners to sue for damages, though they do include canceling or transferring the Internet address.

Online Transactions

Increasingly, consumers are using the Internet for their personal transactions. They may buy gifts, clothes, books, insurance policies, or even cars online. Online transactions differ from “in person” transactions in several respects. For example, online transactions are commonly made between people who live in different states, or even different countries. Also, the customary signature used for face-to-face transactions has given way to other methods of “sealing the deal.” Consequently, it has been necessary for states and the federal government to develop new laws to govern online transactions.

State and federal laws govern online transactions in Ohio and elsewhere in the United States. Usually, the vendor defines the terms of the contract. The terms may be in a written agreement or implied by conduct such as exchanging

e-mail messages. Simple actions such as completing an online order form at a Web site and providing a credit card number to pay for an item may result in the formation of a contract. The contract is formed when the Web site accepts the order. Many Web vendors use *clickwrap* agreements that require a customer to review the terms of the agreement and select an option to agree or disagree before proceeding with the transaction.

Sales transactions, even those transactions completed online, are usually governed by state law. If two parties to a transaction are from different states, the question arises as to which state's law should apply to the transaction. Many clickwrap agreements include "choice of law" provisions that determine which state's law applies to the transaction. Usually, the vendor's state law applies because the vendor is providing the clickwrap agreement. If the parties in a dispute have not agreed on a choice of law, the court will review the facts and circumstances of the transaction and select which state's law to apply before proceeding with the dispute.

Federal laws also may apply to certain online transactions. Some online vendors, such as banks, are subject to federal as well as state regulations. The court will determine whether state or federal law applies to a certain issue in a dispute that involves an online transaction. (*For a discussion of court jurisdiction as it relates to online activity, see "Personal Jurisdiction in Cyberspace" below.*)

Digital Signatures

It is no longer necessary for an individual to physically place a signature on a piece of paper in order to enter into a contract. Instead, an individual may agree to buy insurance, sign a lease, arrange for utility service, or take out a loan by providing a digital, or electronic, signature online.

Digital signature laws are now in effect at both the state and federal levels. On the federal level, the Electronic Signatures in Global and

National Commerce Act (E-SIGN), enacted in October 2001, is significant because it means that digital signatures are now valid for commercial transactions throughout the United States and for all international commercial transactions based on U.S. law. Although E-SIGN does not mandate the use of digital signatures, it does give them the same legal effect as manual signatures. Further, it specifically invalidates state laws requiring paper signatures, as well as state-level digital signature laws and court decisions with conflicting provisions. It also permits businesses to require digital signatures of their customers as a condition of doing business.

E-SIGN does have some limits. It applies only to commercial transactions. It does not apply to:

- wills and trusts;
- family law matters such as marriages, adoptions or divorces;
- court documents; or
- notices of termination of various sorts such as evictions, utility cutoffs, product recalls and insurance cancellations.

Although E-SIGN applies to the *Uniform Commercial Code* provisions for contracts and sales and written waivers, it does not apply to commercial paper, bank deposits and collections, letters of credit, warehouse receipts, investment securities, or transactions involving a security interest.

E-SIGN also provides a way for parties to choose not to use electronic contracts. Online companies must indicate whether paper contracts are available. They also must inform customers that, even if they have given their consent to use electronic documents, they can change their minds and request paper agreements instead. The notice must explain what fees or penalties might apply, if the company has to use paper agreements for transactions. The notice also must indicate whether the consumer's consent applies only to the particular transaction at hand or whether the business has to get consent to use e-signatures for each transaction.

Ohio's Electronic Transactions Law

Ohio enacted the Uniform Electronic Transactions Act in 2000. The law is similar to E-SIGN and supports the use of electronic commerce. It makes the electronic record of a transaction equivalent to a paper record and gives electronic signatures the same legal effect as manual signatures. This means that a contract formed through the use of an electronic record can be enforced. However, electronic records and signatures cannot be used when creating or executing wills and trusts.

The law applies only to transactions parties have agreed to conduct by electronic means. No one is forced to conduct electronic transactions; parties to a transaction must be given the opportunity to opt out.

The law also permits state agencies to use electronic records and signatures in performing their duties, but bars their use by the General Assembly, legislative agencies, and the Supreme Court of Ohio and other Ohio courts.

Personal Jurisdiction in Cyberspace

Jurisdiction refers to the court that will hear a dispute arising in the online environment. Jurisdiction in Cyberspace has become an increasingly important subject for both businesses and consumers. Businesses need to know what laws to obey, while consumers who make online purchases may not have an adequate remedy if they must pursue claims in foreign jurisdiction.

By its very nature, the Internet permeates the world. It has been observed that events on the 'Net happen everywhere, but nowhere in particular. Local activity such as typing on a computer keyboard, then clicking a mouse, can literally have global effects. When disputes arise, where should Internet-related litigation between residents of different states and countries be heard?

Some jurisdictional disputes involve Web sites. A claim might arise in connection with the content of a particular Web site operated by an owner in one state that infringes on the protected rights—such as trademarks or trade names—

of someone in another state. For example, let's say a California company starts a new business and registers a domain name, such as "PAYMYBILLS," that is similar to an existing Ohio company's name, "PAYMYBILL." If confusion arises among Internet users, causing the Ohio company to sustain damages, should the dispute be resolved in Ohio or California?

Another interesting example of a challenging factual scenario would be one of an Ohio resident who uses a computer system in California to post content on a Web site that a North Carolina resident claims is defamatory. Should the dispute be resolved in Ohio, California or North Carolina?

Or, what if you purchase over the Internet defective goods or products supplied by a company located in the United Kingdom? Where should that dispute be heard? Can you sue here, or must you travel to the foreign country? If the latter, you may not have meaningful recourse due to time and expense considerations.

There are no clear and easy answers to these questions. These are the types of issues that courts have grappled with recently with the increasing popularity of the Internet.

While early court decisions were inconsistent, the recent trend has been to return to the traditional tests for the assertion of personal jurisdiction that require a defendant to purposefully avail himself of the benefits of the foreign state before he can be subjected to suit there. So, it would be proper for a state to exercise jurisdiction over a non-resident if that person is "doing business" there, and deriving revenues and profits as a benefit.

Another trend in U.S. courts is that Internet usage is viewed on a sliding scale. If you merely advertise products or events to consumers in other states on a *passive* Web site, you will likely not be subjected to a lawsuit in the other states if there is a problem. For example, if a jazz club advertises on the Web its upcoming schedule of events, but the site does not permit you to order tickets, it would fall into the "passive" category.

On the other hand, if you advertise a product on a Web site that is *active*, permitting customers

in other states to order products, those states likely possess jurisdiction. A good example of an active site might be Amazon.com®, where you can shop online and make purchases using a credit card.

If the Web site falls somewhere between the two extremes, it is anyone's guess as to the appropriate court for the dispute resolution. In such cases, courts will often look at whether or not the defendant targeted the impact in the other state, as opposed to unintended consequences that might occur there.

In all jurisdictional disputes, facts are very important and will be carefully examined by the court to insure that fair play and substantial justice are being observed. If that is the case, then the out-of-state defendant's constitutional rights are protected, and subjecting that defendant to the jurisdiction of a foreign state is both fair and foreseeable.

Liability for Online Conduct

The Internet has greatly increased the amount of information, even seemingly private information, that is available to the average person. This easy access to information solves some problems and creates others. Gossip you pass to a neighbor might be considered libelous or even slanderous if shared in a chat room. Persons intent on causing trouble for a company can do so through the Internet with relative anonymity. The potential for copyright infringement is significant. While existing laws generally can be applied to these Internet-related situations, legal issues arise that are unique to online conduct. Therefore, laws governing online conduct are developing as use of the Internet grows.

Defamation

An individual's communications in chat rooms and elsewhere on the Internet are subject to the laws of defamation. The laws of defamation include the law of libel, which applies to written

statements, and the law of slander, which applies to spoken statements. A defamatory statement is a substantially false statement that causes damage to the reputation of another person or entity such as a corporation. (*See Part V, "Torts," for more information.*)

Ordinarily, the law of libel rather than the law of slander governs defamatory statements transmitted through the Internet because the statements are written. Although statements made in a chat room are written and, therefore, subject to the law of libel, they are transitory and spontaneous and, therefore, very similar to spoken words. Consequently, the law of slander also may apply. In a defamation lawsuit, the court will decide which laws apply.

Regardless of whether the law of libel or slander applies, these laws have not been changed for electronic communications. Therefore, if an electronic communication includes a defamatory statement about another individual, the writer may be held liable for defamation.

Electronic communications are subject to other laws as well. For example, individuals may be liable for violating trade secret laws if they communicate their employer's proprietary information to others outside of the company without permission. They also may be liable for violation of state and federal laws if their electronic communications relate to or support illegal activities.

"Cybersmear" Attacks

The Internet epitomizes the notion of a double-edged sword: it enables businesses to reach prospective customers and investors around the world, while at the same time equipping disgruntled employees, underhanded competitors and others with a convenient medium for airing venomous complaints that sometimes warrant retaliation. While it is fairly simple for companies to choose a legal response to such *cybersmear* attacks (such as defamation, interference with business relations, and misappropriation of trade secrets), the task of tracking down the often-faceless defendants can prove daunting. What,

then, is the best tactic for identifying anonymous online critics?

Although a cybersmear on any company's reputation can be made with relative or total anonymity, victims need not despair. A number of companies have succeeded in identifying anonymous culprits in "John Doe" suits designed expressly for that purpose.

Before filing suit on any substantive claims, the plaintiff must file a John Doe suit, naming the unknown poster as a "John Doe" defendant, and then subpoena the Doe's identification from ISPs suspected of hosting the Doe's postings. In some cases, John Doe subpoenas yield swift results. In others, however, the unmasking is not so easy. The vast majority of ISPs do not review their bulletin boards for obscene or profane material because federal law generally protects ISPs from content liability (*see below*). In addition, they are sometimes reluctant to play the "middle man" in John Doe suits.

The occasional reluctance of ISPs in responding to subpoenas is not the only bump in the John Doe road, however, as defendants frequently assert a right of privacy in their online anonymity. Ever-advancing technology is helping cybersmearers achieve almost indecipherable anonymity as the number of online encryption-for-hire services continues to grow.

The law in this area is evolving. Inevitably, the courts will be obliged to decide whether to establish new rules to streamline the now arduous John Doe identification process.

Internet Service Provider Liability for Online Conduct

If a subscriber to a particular Internet Service Provider (ISP) disseminates another's copyrighted material or posts a defamatory statement, should that individual's ISP be liable for the online conduct of its customer? Internet Service Providers argue that, because they are channels for sending information (like telephone companies), they should not be held liable for a subscriber's online conduct.

Under the Digital Millennium Copyright Act (DMCA), ISPs can avoid liability for their subscribers' posting of another's copyrighted material if:

- they did not obtain any financial benefit from the copyright infringement;
- they did not have actual knowledge that the subscriber was transmitting copyrighted material; and
- after learning of the infringement, they acted quickly to remove the copyrighted material or disable access to it.

Under the law, ISPs must designate an agent to receive notices from wronged copyright holders and register the agent's name and address with the U.S. Copyright Office. They also must develop a policy of terminating subscribers who repeatedly infringe others' copyrights.

Under the Communications Decency Act (CDA), ISPs cannot be held responsible for the statements or comments of their subscribers. Under the CDA, it is the subscribers who are considered the "publishers" or "speakers" of any statements or comments they may post on the Internet through an ISP, so it is only the subscribers who can be held liable for any improper conduct.

For example, America Online® (AOL®) avoided liability under the CDA after it posted a defamatory story about Sidney Blumenthal, an assistant to former President Clinton. Matt Drudge, the online gossip columnist who writes the Drudge Report, posted a story alleging that Blumenthal had a history of spousal abuse. America Online ran the story after paying Drudge \$3,000 per month for the right to post his column. After having received a letter from Blumenthal, Drudge and AOL retracted the story and issued a correction; however, Blumenthal sued Drudge and AOL for defamation. The court dismissed AOL from the lawsuit, ruling that the CDA shielded AOL from liability, even though AOL had paid Drudge for the right to post the story.

Chapter Summary

- Cyberlaw relies on common law and case law principles to resolve controversies that arise from computer activities. However, new laws are enacted when established law cannot provide a general solution.
- Contract law governs online transactions. Usually, the vendor defines the terms of the contract. The terms may be in a written agreement or implied by conduct such as exchanging e-mail messages.
- Sales transactions, even those transactions completed online, are usually governed by state law.
- Digital signature laws are now in effect at both the state and federal levels. The federal version, the Electronic Signatures in Global and National Commerce Act (E-SIGN), took effect October 2001.
- Individuals are always free to view online content, although they may not be free to download, copy, print, or save this information. Some Web site operators will tell an individual what he or she can do and cannot do with the information that is available from a particular site.
- *Cybersquatters*, also known as *cyberpirates*, are people who or companies that register trademarks as domain names in bad faith for an improper purpose.
- The advent of the Internet has blurred the lines between what is public and private information. Currently, there are few restrictions regarding the type of information courts and government agencies can place online.
- E-mail communications, like regular mail communications, are meant to be private. There are federal laws that prohibit the interception and disclosure of e-mail communications.
- Individuals participating in chat rooms assume the risk for their activities.
- Inexpensive telecommunications, such as the Internet, combined with inexpensive computing power, makes it relatively easy to gather detailed information about individuals. Web advertisers use *cookies* to track people's Internet use, maintaining data files on millions of consumers with hundreds of data fields per consumer.
- Congress enacted the Children's Online Privacy Protection Act (COPPA) in 1998 to regulate the online sharing of information by children.
- Many employers provide employees with the equipment necessary to access the Internet and the Web to fulfill their job responsibilities. Therefore, an employer has the right to monitor and control the use of the equipment and an employee's activities on the Web.
- An individual's communications in chat rooms and elsewhere on the Internet are subject to the laws of defamation.
- The Internet enables businesses to reach prospective customers and investors around the world, while equipping disgruntled employees, underhanded competitors and others with a convenient medium for airing complaints that sometimes warrant retaliation.
- Laws governing online conduct are developing as use of the Internet grows.

Web Links:

From the OSBA:

OSBA's "LawFacts" pamphlets:

(go to <http://www.ohiobar.org/pub/lawfacts/> and search by topic)
"Online Law"

OSBA's "Law You Can Use" articles:

(go to <http://www.ohiobar.org/pub/lycu> and search for article by title or by topic)

"Consumers Should Exercise Care When Purchasing Health Products Online"

"Digital Signatures: Might You Sign a Contract without Realizing It?"

"'Fair Use' Doctrine Permits Limited Copying of Copyrighted Material"

"FTC Enforces 'Consumer Protection' Laws"

"Prepare to 'Face the Music' When Downloading from Internet"

"What You Should Know about On-line Shopping"

From other sources:

<http://www.ftc.gov/bcp/online/edcams/kidzprivacy/>
Children's privacy and the Internet

<http://www.copyright.gov/legislation/dmca.pdf>
Digital Millennium Copyright Act

<http://www.copyright.gov/>
U.S. Copyright Office

<http://www.gseis.ucla.edu/iclp/bib.html>
UCLA Online Institute for Cyberspace Law and Policy

<http://www.ag.state.oh.us/>
Search: Computer Crimes Task Force