



ONLINE LAW

Does free speech apply to the Internet?

Yes. The First Amendment applies to the Internet, and you may express your views through the Internet in any way you choose. However, established legal principles regarding defamation, invasion of privacy, stalking, harassment, etc., also apply on the Internet. Also, once you make a statement on the Internet, be aware that it is difficult to retract or remove it later.

What is the law regarding my use of the Internet at work?

Employers have the right to monitor and control an employee's Internet use while at work because an employee's uncontrolled Internet use could get a business in trouble. A business may monitor employees to prevent them from leaking confidential information, downloading files that infringe copyright law, or simply goof off. Also, businesses must prevent a "sexually hostile" work environment—something that could result from online access to inappropriate material. Your employer may allow you to access the Internet for personal use as long as the use does not interfere with the employer's interests, but do not expect privacy when accessing the Internet at work.

Can I expect privacy when using the Internet at home?

Despite some laws protecting Internet privacy, it is safe to assume that everything you do on the Internet is being monitored, tracked, logged, archived and aggregated with other information about you in various databases. Generally, this is done for commercial reasons. Online companies track and analyze consumer Web use to do targeted advertising and to determine what types of Web sites and selling techniques work best. Unless you specifically opt out, banks and financial institutions can share, sell or exchange your customer information.

A federal law protects the privacy of e-mail communications. However, it includes a provision that gives Internet service providers the right to monitor the contents of the e-mail sent or received by their customers. Post September 11, law enforcement personnel have increased powers to monitor and intercept information.

The Internet also affects the privacy of people who do not use it. Information previously available only to those who showed up at places like a county recorder's office is finding its way onto the Web. Social Security numbers, signature specimens, personal financial information and even credit card numbers are sometimes accessible through the Web. Legislatures and courts are grappling with the difficult issues of public access versus privacy interests.

Is there any way I can protect my privacy when using the Internet?

- Use a combination of protections, including an Internet security or "firewall" program, anti-spyware program and anti-virus program to prevent unauthorized access to, transmissions from and tracking of your computer.
- Use the security settings on your browser to allow "cookies" (codes that track your Internet use, stored on your computer by the sites you visit) only when you permit them. Don't type in sensitive



AFIT JA FACT SHEET

personal information such as your Social Security number or credit card number unless the merchant is reputable and the information is encrypted.

- When disclosing information that may end up in a public record, disclose only the minimum necessary information, and if the disclosure is for a court proceeding, consider asking your attorney to request a protective order to restrict the scope of the disclosure.
- Be careful when responding to e-mails requesting information. A "phishing" scam may appear to be a reputable company contacting you through e-mail, but could be a predator attempting to obtain personal information. If there is any doubt, make an independent confirmation before disclosing information.
- Deal only with merchants that have good privacy policies. Merchants must comply with any privacy policy they post.
- If you must ensure privacy when transmitting information, consider using an encryption program to prevent unwanted review of your data.

What should I know about online transactions?

Online transactions are safe if you use common sense. Federal and state governments have enacted laws designed to promote electronic commerce. In general, it is safe to give a credit card number to an online merchant, but some credit card companies may restrict your right to dispute online transactions involving out-of-state companies. Avoid dealing with a company that does not list a verifiable street address and phone number on its Web site. When providing credit card information online, make sure the site is secure ("https://" plus a "closed lock" symbol on your browser), and make sure you have an up-to-date browser with good encryption. It is safe to provide the "validation code" on the back of your credit card, but do not provide a Social Security number. Under federal and state law, you no longer need to physically sign your name to enter into a contract—almost anything can serve as a signature in an online transaction: clicking a button, typing "accept" or a password, etc. Print out a copy of the online order confirmation screen, and review your credit card records to make sure only legitimate charges appear. Credit card companies cover losses of more than \$50 from lost or stolen credit cards. Debit cards pose additional risks, as they are much less protected than credit cards from loss, theft or improper use, and remove money from your bank account almost immediately.

Is there is a special law prohibiting taxes on the Internet?

No. You pay sales tax on the Internet just as you would for mail-order goods. If you buy goods from a merchant who has a store in Ohio, you must pay sales tax even if you are ordering from the online affiliate of the merchant in some other state. The "Internet Tax Freedom Act" does not affect taxes of online sales of goods and services, but only prohibits new taxes on the Internet connection itself.

What should I know about my children's Internet use?

- Under federal law, operators of Web sites directed at children must obtain parental consent before collecting and sharing any personal data about children younger than 13. For more information go to www.ftc.gov (keyword "children").



AFIT JA FACT SHEET

- Courts have consistently held that the Internet is a medium for adults and cannot be restricted to suitable-for-children standards. However, technical and practical ways to prevent minors from viewing inappropriate content include: using a browser or a firewall to prevent pop-up advertising; setting spam filters to reject e-mail from unknown senders; subscribing to a content-blocking service; and discussing “inappropriate content” with your children.
- Increasingly, children have been illegally downloading electronic content such as music, video and computer software. Violators of copyright law can be subject to paying damages up to \$150,000 per violation. Be aware of what your child downloads and its origin, and encourage your child to download only legal copies.

What is being done about spam, viruses and spyware?

Federal law now regulates the sending of commercial e-mail messages, but it is difficult to make such laws effective since the Internet has no borders. Similarly, there are already numerous laws making it a crime to interfere with the operation of a computer by knowingly producing or transmitting a virus, but these laws have not successfully stopped viruses.

However, there are technical and practical solutions for spam and virus problems. Most Internet providers now offer spam-filtering capability. Also, Internet users can use “disposable” e-mail addresses when corresponding with merchants and others, and use long-term e-mail addresses for friends and family. To address virus and spyware problems, anti-virus, spyware removal and Internet security software is widely available.

What should I know about the “back alleys” of the Internet?

Questions about the legality of the following online activities arise frequently:

- *Gambling*. Internet gambling is illegal throughout the United States. The major credit card companies no longer will process credit card transactions with offshore casinos. If you gamble online, you have no legal remedies if the casino cheats you.
- *Alcohol and cigarettes*. It is legal to buy alcohol and cigarettes online. State laws banning such sales have been held unconstitutional.
- *Pharmaceuticals*. Generally, pharmaceuticals may be purchased online, even from out-of-state or foreign vendors. However, pharmacists are restricted as to when they may dispense prescription drugs to patients who have not been physically examined by a doctor. For more information, see www.fda.gov.
- *Pornography*. It is *legal* to download or view “non-obscene” adult material on the Internet. It is *illegal* to download or view “obscene material.” A definition of what is “obscene” cannot easily be applied to the Internet, but pornography involving minors is generally considered “obscene.” Again, the best preventions are technical rather than legal.
- *Online scams*. If you become the victim of an Internet-based scam, contact the government agency with jurisdiction over the type of scam involved. For investment scams:



AFIT JA FACT SHEET

www.sec.gov/investor/pubs/cyberfraud.htm. For consumer ripoffs: www.ftc.gov. For consumer complaints involving Ohio companies: www.ag.state.oh.us.

Is it illegal to download from the Internet?

Consumers now can access music, video, computer software and other electronic content through the Internet. Many specially licensed Web sites allow you to download electronic content for free or for a small fee through the Internet. File swapping over "peer-to-peer" (P2P) networks, however, can be illegal and may subject an individual to enforcement of copyright infringement by the copyright owner, such as the Record Industry Association of America (RIAA). Damage awards can be up to \$150,000 per violation (song/download). If you decide to download, be sure to download from licensed sites. The RIAA does, however, offer a "Clean Slate Program" to provide amnesty for individuals who have illegally downloaded.