



## Consumer Rights And Protection

©2009 eNotes.com, Inc. or its Licensors. Please see [copyright information](#) at the end of this document.

- [Background](#)
- [Development of the Internet](#)
- [Consumers and Privacy](#)
- [Cybersquatting](#)
- [Electronic Signatures and E-Sign](#)
- [Additional Resources](#)
- [Organizations](#)

### Background

The Internet has raised a variety of legal issues since it first became widely used in the mid-1990s, most in the area of consumer rights and protections. But because the Internet is relatively new, regulations affecting consumer rights have often lagged behind the development of e-commerce as important new revenue source for businesses in the United States.

At the end of the 1990s and beginning of the twenty-first century, legislation affecting consumer and business rights in areas such as privacy, cybersquatting, and electronic signatures was passed. This legislation marked some of the first attempts to regulate the Internet marketplace. Because the Internet is still changing and developing, these new laws will almost certainly not be the last in terms of Internet regulation. It remains to be seen what will develop for this extraordinarily powerful marketing and selling tool.

### Development of the Internet

The Department of Defense first created the Internet in the late 1960s as a way of making sure communications between different facilities could withstand a war. It was originally called ARPANet, and in time this network came to link [CORPORATIONS](#) and educational institutions as well. As this system developed, its aptitude for commercial applications became more and more apparent. The introduction of the first Internet browsers, along with the development of domain names—the names used by their owners to identify specific Internet addresses (e.g. [www.gale.com](http://www.gale.com))—and hypertext transfer protocols (HTTP), hastened this changeover. By 1995, when the National Science Foundation finally stopped supervising the Internet and Netscape introduced the first commercial Internet browser, it was clear that the Internet was going to become something big.

Since that time, companies offering various commercial services have popped up all over the Internet. Amazon, E-Bay, and Yahoo are the most widely known of the thousands of retail companies that have taken advantage of the Internet's lack of overhead and its ease of use. Internet commerce exploded from less than \$100 million in 1995 to \$33 billion in 2001.

But with this tremendous increase in trade has come concern for the rights of consumers who use the Internet to buy everything from soap to cars. Because the Internet has grown so fast in a relatively short while, many unusual consumer issues have arisen that have required both regulatory agencies such as the FTC and the

legislative branches to pass new rules and laws specifically adapted to the situation.

## **Consumers and Privacy**

One of the most controversial issues facing consumers using the Internet has been privacy. Consumers have been concerned not just about having important information such as credit card numbers given out to the wrong people but also other information such as addresses and phone numbers.

One of the biggest controversies over privacy and the Internet has concerned so-called informational databases that companies accumulate when individuals buy something or registers on their sites. These databases contain personal information that can be sold to other corporations wishing to target those consumers. Corporations have traditionally treated these databases as a normal business asset. Recently Congress has stepped in to enact legislation making it more difficult to sell or purchase these databases without the consent of the consumer providing the information. There are questions about the reach of some of this legislation, however.

### ***Computer Fraud and Abuse Act***

The Computer FRAUD and Abuse Act (CFAA), first passed in 1984, was amended in 1996 to punish anyone who "intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains information from any protected computer." Computers used for e-mail communication between states or used for online purchases from online vendors from other states are presumably included under the definition of protected computer that states that it includes any computer "which is used in interstate or foreign commerce or communication."

Thus, any user who covertly collects personal information of web-users engaged in transactions is in violation of this act. However, the CFAA has been used sparingly in prosecutions so far, and there are questions about its reach in regard to Internet privacy issues.

### ***Electronic Communications Privacy Act***

Like the CFAA, the Electronic Communications Privacy Act (ECPA) was originally passed in the 1980s. The ECPA prohibits the intentional interception of electronic communications, the intentional disclosure of electronic communications wrongfully obtained, and the intentional use of electronic communications wrongfully obtained.

Observers have suggested that the ECPA could limit the use of "online profiling." Profiles are compiled by tracking users' movements online, usually by the use of cookies (pieces of code that are placed on users' computers when they visit a website that compiles information about users the websites use when the users make return visits). These cookies are often traded between sites so that online profiles of Internet users can be built, and marketing information can be targeted as specific users.

The ECPA contains an exception to its general rules about electronic communications that allows the interception and dissemination of electronic communications when one party to the communication has given consent. This would limit the use of ECPA in terms of online profiling since the site the user is in direct contact with would be allowed to use the consumer's information under this exception.

### ***Children's Online Privacy Protection Act***

The Children's Online Privacy Protection Act (COPPA), passed in 1998, marks the first action by the government specifically limiting companies' dissemination of private information over the Internet. COPPA prohibits an operator of a website or online service directed at children or any operator that has actual knowledge that children are using its website, from collecting personal information from a child, unless the operator meets certain regulatory requirements.

These regulatory requirements include providing notice on the website as to what information is collected from the children and how the operator plans to use the information. In addition, the operator must obtain verifiable parental consent for the collection, use, or disclosure of personal information from children. Finally, operators are required, upon the request of a parent, to provide a description of the specific types of personal information collected from the child by that operator and an opportunity to prevent further collection or use of such information.

COPPA applies to websites and online services that are specifically directed at children under the age of thirteen and to operators of websites where the operators have actual knowledge they are collecting information from children under the age of thirteen. In 2000, the Federal Trade Commission filed its first action under COPPA, against a website called Toysmart. After it declared [BANKRUPTCY](#), Toysmart had attempted to sell the data it had collected selling toys. The FTC and Toysmart eventually agreed to a consent degree which allowed Toysmart to sell its database but only to a qualified buyer who focused its business in the same area that Toysmart did and agreed to the same limitations on that information that Toysmart had to follow under COPPA.

### ***FTC Actions***

Beyond the above-mentioned acts, the FTC has made clear to Internet service providers they are expected to abide by the privacy policies posted on their websites. Recently, the FTC took action against at least one "virtual community website"—consisting of the home pages of millions of members—which was providing information to third parties compiled from members in violation of its own privacy policies. The FTC suggested in a release after the case was settled that "statements about information practices must be accurate and complete." If a retailer or other service provider states in a privacy policy it will not disseminate information, the FTC will step in if that policy is violated.

### **Cybersquatting**

Cybersquatting refers to the registration of a domain name in which the person has no legitimate interest. Cybersquatting is the attempt to profit by reserving and later reselling the domain name to the companies or individuals that have the trademarked right to the domain name. This can happen because domain names are registered on a first come, first serve basis. As an example, a cybersquatter may register the name "[Exxon.com](#)" and attempt to sell this name back to the Exxon corporation, or alternatively, may attempt to block Exxon from using [Exxon.com](#) as an address to conduct business on the Internet. The cybersquatter may use the [Exxon.com](#) address to post disparaging information about Exxon or to try to [DEFRAUD](#) consumers wishing to do business with Exxon into thinking they have accessed the official Exxon site.

In response to the tremendous amount of [LITIGATION](#) that occurred as a result of cybersquatting, the Anticybersquatting CONSUMER PROTECTION Act (ACPA) was passed in 1999. This law provides that persons are liable for civil damages if they register, use, or traffic in domain names that are identical or confusingly similar to a distinctive or famous mark owned by the plaintiff and the person has a [BAD FAITH](#)

intent to profit from such activity.

The ACPA is a fairly broad act that prevents many of the actions of cybersquatters discussed above. To assist in the bad faith determination, the court provides a non-exhaustive list of factors the court may examine in looking at a person's registration of a domain name. These include:

- The trademark or other intellectual property rights of the person in the domain name
- The extent to which the domain name consists of the legal name of the person or a name that is commonly used to identify that person
- The person's prior use of the domain name for a commercial purpose
- The person's prior use of the domain name for noncommercial purposes
- The person's intent to divert consumers from the mark owner's online location to a site that could harm the good will represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark
- 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
- The person's provision of material and misleading false contact information when applying for the registration of the domain name
- The person's registration or acquisitions of multiple domain names that the person knows are identical or confusingly similar to the marks of others
- The extent to which the mark incorporated in the person's domain name registration is or is not distinctive and famous.

## Electronic Signatures and E-Sign

One of the most difficult issues to resolve in the area of consumer rights and the Internet is the role of "electronic signatures." Traditionally, signatures have had a hallowed place in the arena of contract law, where they have been seen as crucial to making a valid contract between parties. But on a computer, it is impossible to sign a name; at least in the traditional way it has been done. Yet consumer transactions between parties require some sort of indication of agreement even over the Internet, some sort of indication there has been a "meeting of the minds."

On Oct. 1, 2000, in answer to these concerns, the E-Sign Act took effect. E-Sign established a uniform federal framework for validating electronic commerce transactions. E-Sign allows electronic signatures for two scenarios: a transaction that occurs in "electronic form," and a transaction that utilizes an electronic signature or electronic record. In both of these scenarios, E-sign upholds the effects of electronic transactions regardless of the type of method of electronic record or signature employed by the transacting parties.

E-Sign applies only to transactions where parties have agreed to do business electronically—through the Internet or other electronic methods. In addition, where an existing law requires that information relating to a transaction be made available to a consumer in writing, a consumer must affirmatively consent to an electronic record in place of the written record, and must be provided with an easy to understand way to withdraw such consent.

E-Sign does not change existing state law regarding the necessity or effect of signatures. It merely provides one more way for such signatures to be recorded.

## Additional Resources

*"Consumer Protection and Antitrust Enforcement at the Speed of Light: The FTC Meets the Internet."* Graubert, John, Jill Coleman, Canada-United States Law Journal, 1999.

*"Fighting Back on the Internet: A Primer on the Anticybersquatting Consumer Protection Act."* Toth, Justin T., Utah Bar Journal, November, 2001.

*"From Wax Seals to Hypertext: Electronic Signatures, Contract Formation and a New Model for Consumer Protection in Internet Transactions."* Balloon, Anthony M., Emory Law Journal, Summer 2001.

*"The New Ecomania: Consumer Privacy, Bankruptcy, and Venture Capital at Odds in the Internet Marketplace."* Wingate, John M., George Mason Law Review, Spring 2001.

*"The Rise and Fall of Internet Fences: The Overbroad Protection of the Anticybersquatting Consumer Protection Act."* Ward, Jonathon M., Marquette Intellectual Property Law Review, 2001.

## Organizations

### *Electronic Frontier Foundation (EFF)*

454 Shotwell Street  
San Francisco, CA 94110-1914 USA  
Phone: (415) 436-9333  
Fax: (415) 436-9993  
URL: <http://www.eff.org/>  
Primary Contact: Brad Templeton, Chairman of the Board

### *Federal Trade Commission (FTC)*

600 Pennsylvania Avenue, N.W.  
Washington, DC 20580 USA  
Phone: (202) 326-2222  
URL: <http://www.ftc.gov>  
Primary Contact: Timothy J. Muris, Chairman

### *National Consumer Law Center*

77 Summer Street, 10th Floor  
Boston, MA 02110-1006 USA  
Phone: (617) 542-8010  
Fax: (617) 542-8028  
URL: <http://www.consumerlaw.org/>  
Primary Contact: Willard P. Ogburn, Executive Director

**Copyright Notice**

©2009 eNotes.com, Inc.

ALL RIGHTS RESERVED.

No part of this work covered by the copyright hereon may be reproduced or used in any form or by any means graphic, electronic, or mechanical, including photocopying, recording, taping, Web distribution or information storage retrieval systems without the written permission of the publisher.

For complete copyright information, please see the online version of this work:  
<http://www.enotes.com/everyday-law-encyclopedia>